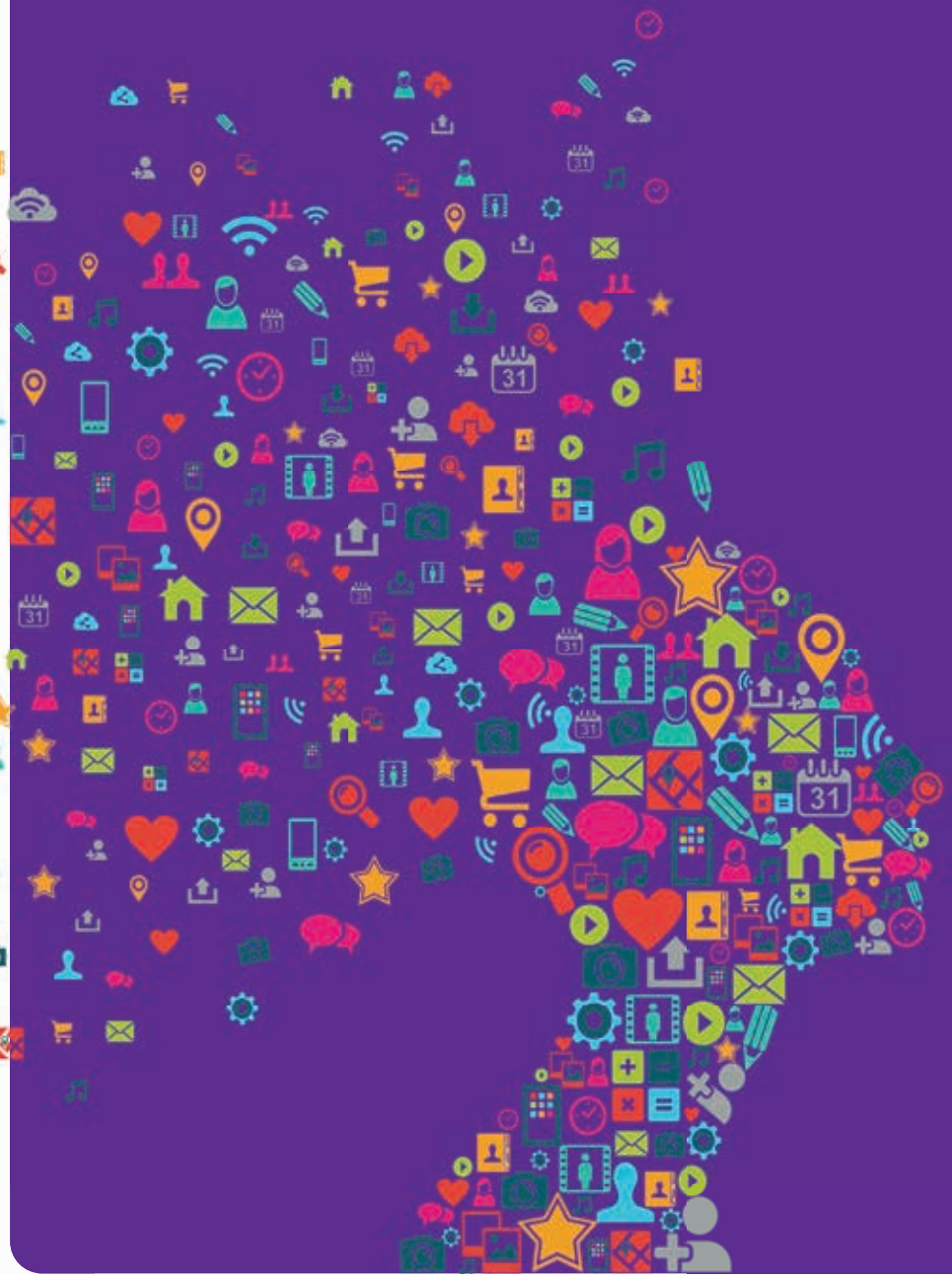


Materiales didácticos

Confianza y seguridad de las mujeres en la Red

2014

MINISTERIO
DE SANIDAD, SERVICIOS SOCIALES
E IGUALDAD

SECRETARÍA
DE ESTADO DE SERVICIOS SOCIALES
E IGUALDAD

INSTITUTO DE LA MUJER
Y PARA LA IGUALDAD DE OPORTUNIDADES

Unión Europea
Fondo Social Europeo

Presentación

Este material que presentamos sobre confianza y seguridad de las mujeres en la Red, tiene como finalidad última, mejorar el manejo y las habilidades de las mujeres para usar los servicios que ofrecen las nuevas tecnologías con confianza y de forma segura. El material, dirigido al personal facilitador que trabaja con mujeres en espacios TIC, trata sobre algunos de los posibles riesgos que pueden encontrarse en Internet. Incluye dinámicas para trabajar de forma participativa con grupos de mujeres, así como, recomendaciones y consejos para prevenirlos. Contempla también algunas reflexiones sobre la situación de las mujeres en relación a las nuevas tecnologías, un breve glosario de términos y un listado de recursos en la Red que pensamos pueden ser de utilidad para el trabajo con las mujeres, independientemente del ámbito en que lo hagan.

Las nuevas tecnologías pueden aportar a la sociedad en su conjunto, a la población en general, y a las mujeres en particular, múltiples oportunidades y beneficios, sin embargo, también surgen nuevos riesgos. Como en muchos otros ámbitos, las mujeres presentan mayor vulnerabilidad a algunos de estos riesgos: las brechas digitales de género pueden dificultar el acceso al empleo, a la formación o a la información en general, pero además surgen nuevos riesgos de sufrir violencia de género. La Red reproduce los roles y estereotipos de género y posibilita nuevas formas de agresión a las mujeres. Es por ello, que en este material, además de abordarse riesgos generales como por ejemplo, estafas o robo de contraseñas, se tratarán aquellos relacionados con la violencia de género. También, dado que las mujeres, aún con mucha frecuencia, son las responsables de los cuidados en la familia, abordaremos algunas temáticas relacionadas con menores e Internet.

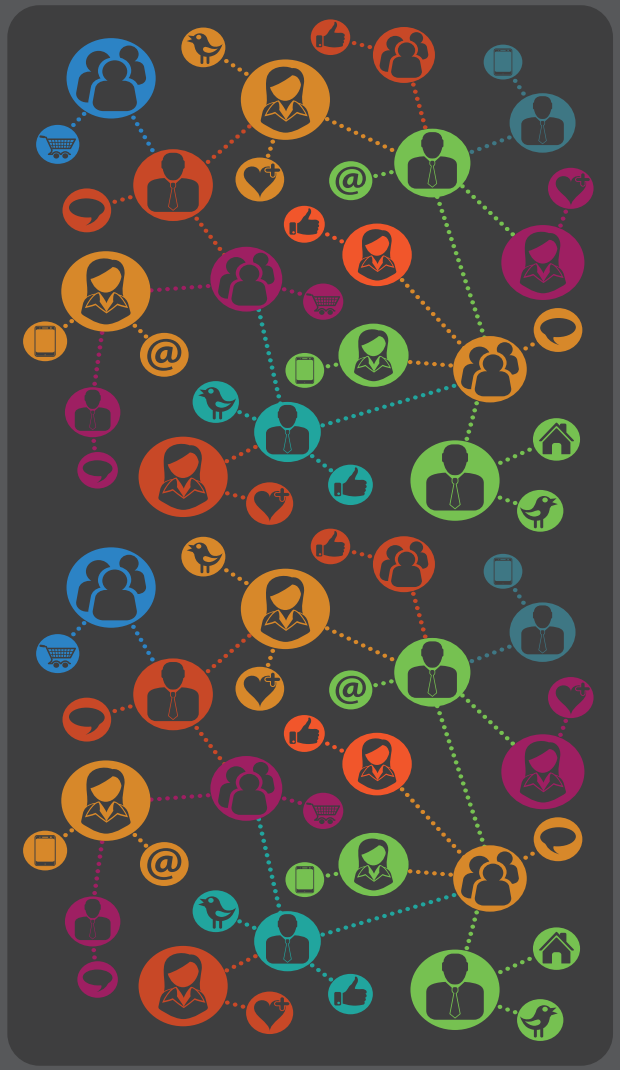
En definitiva, esperamos que el material sea de utilidad para el empoderamiento de las mujeres, contribuyendo a mejorar su confianza y seguridad en la Red.

Instituto de la Mujer y para la Igualdad de Oportunidades

Introducción al material "Confianza y seguridad de las mujeres en la Red"

Objetivo general

Este material ha sido creado con el fin de promover la participación de las mujeres en la Sociedad de la Información, aumentando su confianza y seguridad en el uso de las nuevas tecnologías de la información y comunicación.



MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD

SECRETARÍA DE ESTADO DE SERVICIOS SOCIALES E IGUALDAD

INSTITUTO DE LA MUJER Y PARA LA IGUALDAD DE OPORTUNIDADES

Unión Europea
Fondo Social Europeo

1. Introducción

Para la elaboración de este material, se parte de la premisa de que las participantes relacionarán sus conocimientos previos con la reconstrucción de nuevos saberes y experiencias vinculadas al uso de las nuevas tecnologías. Este enfoque del proceso de aprendizaje, se centra no tanto en la adquisición de conceptos, sino en la compresión de los mismos basada en la experiencia, trabajando así, los niveles cognitivos, actitudinales y emocionales, teniendo en cuenta, por tanto, la realidad de las participantes.

El material está diseñado para que las mujeres sean protagonistas del proceso de aprendizaje, a través del diálogo, la creatividad, la flexibilidad y la toma de conciencia. Los nuevos conocimientos se construyen grupalmente actuando el personal dinamizador como facilitador del proceso.

Uso del material didáctico

Este material permite el trabajo de las distintas temáticas sin necesidad de seguir un orden lineal determinado. Los colores de fondo y los íconos facilitan caminos alternativos en su organización y preparación. Cada temática está agrupada en un pequeño cuadernillo en el que se incluyen una serie de actividades, que se pueden seleccionar según los objetivos que se pretendan conseguir. Está pensada para trabajar la confianza y seguridad en la Red con mujeres que tengan conocimientos de informática a nivel de usuaria.

Este material se compone, además de éste, de doce cuadernillos temáticos con actividades didácticas.

- Identidad digital, reputación y privacidad on-line
- Contraseñas

1. Introducción

- Ciberacoso
- Sexting
- Extorsión sexual - Sextorsión
- Acoso sexual a menores en Internet - Grooming
- Ciberacoso escolar - Cyberbullying
- Tecnoadicciones
- Fraude en la Red - Phishing
- Correo basura - Spam
- Bulo - Hoax
- Virus y malware

Para cada una de las temáticas, se definen como objetivos generales las capacidades que las participantes tendrán al finalizar las actividades propuestas. Igualmente, para facilitar su uso y hacer más funcional el material, se identifican los soportes digitales donde se puede producir el riesgo o amenaza.

Así mismo, cada cuadernillo temático incluye una serie de actividades, definiéndose los objetivos a conseguir con cada una, es decir, las capacidades adquiridas por las participantes al finalizar la actividad y especificando los recursos y el tiempo necesario para llevarla a cabo. El tipo de actividades que se proponen es variado: lluvia de ideas, reflexión personal, debate grupal, dramatizaciones y juego de roles, proyección de cortos o videos, etc.

1. Introducción

Por tanto, para algunas de las actividades, será necesario el uso de ordenador y la conexión a Internet; para otras no será necesario contar con ordenadores u otros equipos. El personal facilitador podrá adaptarlas en función del contexto, de la realidad de cada grupo y de la profundidad con que se quiera trabajar las distintas temáticas.

En gran parte de las actividades, se han incluido casos redactados a partir de noticias de prensa, blog y webs oficiales, a modo de ejemplos con los que las participantes puedan relacionar sus conocimientos y su experiencia y visualizar mejor los conceptos a trabajar. En algunos casos, se incluyen errores gramaticales, ortográficos y de sintaxis, elementos clave para trabajar problemáticas concretas.

Todas las actividades propuestas pretenden sugerir, despertar la creatividad y la elaboración de propuestas adecuadas para cada momento y lugar, y por tanto, no deben utilizarse como un recetario sino de forma abierta, flexible y contextualizada. En definitiva, se trata de recrear las actividades adaptándolas a cada caso.

Por otra parte, cada una de las actividades va acompañada de un apartado denominado "Recuerda que" en donde se recogen las ideas fundamentales que se quieren trabajar, y que sirve como guía para el personal facilitador y para reforzar y sistematizar lo trabajado en cada actividad. Igualmente cada cuadernillo contiene un apartado de consejos y buenas prácticas en relación a la temática tratada en el mismo. Asimismo, se aporta información de interés y palabras clave que facilitarán la búsqueda en Internet y que servirán al personal facilitador para la preparación del taller y para complementar, fomentar o reforzar el debate y los aportes de las participantes.

Por último, y con el fin de reforzar las capacidades adquiridas, cada cuadernillo consta de un test (verdadero o falso) que se puede realizar colectiva o individualmente al finalizar las actividades.

2. Acceso y uso de las tecnologías de la información

En el acceso y uso de las TIC[1] intervienen múltiples variables como por ejemplo, el sexo, la edad, el nivel de estudios, el lugar de residencia y procedencia, la situación laboral, la situación de discapacidad o el nivel económico, y la interacción de éstas, puede producir discriminaciones múltiples que habrá que tener en cuenta en la planificación de las actividades que se vayan a desarrollar.

En relación a la situación de mujeres y hombres en la sociedad de la información, en los últimos años tiende a cerrarse la brecha de género entre quienes han utilizado el ordenador o Internet. Sin embargo, si tenemos en cuenta la edad, aquella se incrementa entre mayores de 65 años, donde se da mayor brecha a favor de los hombres. El nivel de estudios también determina el acceso y uso que se hace de las TIC, siendo mayor, en general, la brecha de género cuanto menor es el nivel educativo. En cuanto a los usos de dispositivos móviles que utilizan mujeres y hombres para acceder a Internet, ellos acceden en mayor medida a los más avanzados (ordenadores y de PDAs, iPod, videoconsolas, etc).

Se encuentran también diferencias en los servicios utilizados a través de internet, las mujeres refieren en mayor porcentaje que los hombres, el concertar citas médicas o participar en redes sociales, excepto en las redes profesionales donde es mayor la presencia masculina. Por su parte, ellos hacen un mayor uso de la venta directa, las subastas o la banca electrónica.

Por otra parte, persiste una brecha de género a favor de los hombres entre quienes han comprado por Internet en los últimos doce meses, encontrándose diferencias en cuanto al tipo de productos que compran por Internet, ellas refieren mayor consumo de ropa, productos de alimentación, y entradas para espectáculos. Por su parte, ellos hacen un mayor consumo de equipos electrónicos, equipos informáticos, juegos de ordenador, videoconso-

2. Acceso y uso de las tecnologías de la información

las y software y actualizaciones. En lo que respecta a las formas de pago: los hombres utilizan en mayor medida tarjetas prepago, plataformas de pago a través de internet, o el pago por transferencia bancaria a través de Internet.

Por otro lado, los hombres muestran mayores habilidades que las mujeres para las tareas relacionadas con la informática como por ejemplo, instalar un nuevo sistema operativo o sustituir uno antiguo. También para el uso de algunos servicios que ofrece Internet, como los programas de Internet para editar documentos o presentaciones, o para la reproducción de archivos de música o vídeo. Igualmente las mujeres hacen un menor uso de las vías telemáticas para comunicarse con las administraciones públicas o realizar trámites disponiendo en menor medida de DNI electrónico. Señalar que las mujeres aventajan a los hombres a la hora de compartir archivos, imágenes u otros ficheros en páginas personales (blogs o redes sociales).

Respecto a la confianza en Internet entre quienes lo han utilizado en el último año, es mayor el porcentaje de hombres que manifiestan tener "mucho grado de confianza".

Por otra parte, si tenemos en cuenta el lugar de residencia encontramos que la brecha de género aún persiste en cuanto al acceso y uso (utilización de ordenador e Internet en los últimos tres meses) en algunas comunidades, como, la ciudad autónoma de Melilla, la Región de Murcia o la Comunidad Valenciana.

Sin embargo, en relación a las compras realizadas a través de Internet, la brecha encontrada a nivel nacional desaparece en La Rioja y Castilla y León, donde apenas se encuentra diferencia entre hombres y mujeres.

En definitiva, aun cuando las brechas de género relacionadas con el acceso y uso en general tienden a cerrarse, éstas persisten en relación al grado de habilidades y en el uso de los dispositivos más avanzados.

2. Acceso y uso de las tecnologías de la información

Además se encuentran diferencias por sexo en función del tipo de usos que hacen mujeres y hombres de las TIC, reproduciéndose también en este ámbito, los papeles asignados socialmente a unas y otros.

En relación a la presencia de mujeres en el sector TIC, solo señalar que es escasa su presencia en las ramas de estudios de ingeniería y arquitectura, sin embargo, el porcentaje de mujeres en puestos directivos en el sector, es superior a la media de todos los sectores, aunque sigue estando lejos de la paridad.

Por último, y en cuanto a la violencia de género en la red, los últimos informes de la Delegación del Gobierno para la Violencia de Género[2], alertan sobre ésta entre la juventud, siendo en un elevado número de casos, escasa la percepción del riesgo frente a conductas tales, como responder a un mensaje en el que les insultan, quedar con alguien que han conocido por Internet o aceptar como amistad en la red a una persona desconocida.

En concreto, más de una cuarta parte de jóvenes han colgado una foto suya que su padre o su madre no autorizarían. Pero además, un 16% de las chicas no consideran muy peligroso poner en la red una foto suya de carácter sexual. No tienen, por tanto, percepción del riesgo frente a este tipo de conductas, habiendo compartido imágenes privadas como una prueba de confianza o acto de intimidad con la pareja ("prueba de amor") el 2% de ellas, lo que las expone a situaciones de vulnerabilidad o violencia a través de la red. También, más de la mitad de ellas, se exponen usando la webcam, cuando se comunican con las amistades.

Por otra parte, una cuarta parte de las adolescentes reconocen haber sido controladas de forma abusiva por su pareja a través del móvil.

3. Glosario*

Abuso sexual

Comete delito de abuso sexual, quien sin usar violencia o intimidación y sin que medie consentimiento, atenta contra la libertad o indemnidad sexual de otra persona. Si el consentimiento se obtiene prevaliéndose de una situación de superioridad manifiesta que coarte la libertad de la víctima se considera igualmente abuso sexual.

Se consideran abusos sexuales no consentidos, los que se ejecuten sobre menores de trece años, personas que se hallen privadas de sentido, personas de cuyo trastorno mental se abusare, personas sobre las que se ha obtenido el consentimiento sirviéndose de una situación de superioridad manifiesta por parte del autor que limite la libertad de la víctima.

Acoso sexual[3]

Lo constituye cualquier comportamiento, verbal o físico, de naturaleza sexual que tenga el propósito o produzca el efecto de atentar contra la dignidad de una persona, en particular cuando se crea un entorno intimidatorio, degradante u ofensivo.

Acoso sexual a menores en Internet (Grooming)

Conductas de personas adultas dirigidas contra menores para ganarse su confianza y con finalidad sexual realizadas a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación, constitutivas de delito (abusos o agresiones sexuales, prostitución y corrupción de menores, etc.).

Agresión sexual

Comete delito de agresión sexual quien, mediante violencia o intimidación, realice actos que atenten contra la libertad sexual de otra persona.

* Las definiciones que figuran en este glosario no siempre se corresponden con las definiciones legales desde el punto de vista del Código Penal.

3. Glosario

Alias (Nick)

Seudónimo usualmente corto y fácil de recordar que se utiliza en Internet para representar a una persona usuaria sin necesidad de utilizar su nombre real.

Ancho de banda

Término técnico que determina el volumen de información que puede circular por un medio físico de comunicación de datos, es decir, la capacidad de una conexión. A mayor ancho de banda, mejor velocidad de acceso y más personas pueden utilizar el mismo medio simultáneamente. Se mide en bps (bits por segundo).

Antivirus y antimalware[4]

Programa cuya finalidad es prevenir las infecciones producidas por los virus informáticos, así como erradicar las ya producidas. Para que sean realmente efectivos, dada la gran cantidad de virus y malware que se crean continuamente en la Red, estos programas deben actualizarse a menudo.

Archivo ejecutable

En informática, un ejecutable o archivo ejecutable, es un archivo binario cuyo contenido se interpreta por el ordenador como un programa que ejecuta acciones en el ordenador. En los sistemas Windows suelen tener extensión ".exe".

Barra de navegación

Conjunto de elementos que se utilizan como opciones de menú para navegar dentro de una Web. Una página web suele contener una única barra de navegación.

3. Glosario

Bulo (Hoax)[5]

Término utilizado para denominar a rumores falsos que se difunden por la Red, especialmente sobre virus inexistentes. En ocasiones tienen tanto éxito que pueden causar casi tanto daño como un virus real.

Ciberacoso

Acto por el cual se amenaza, hostiga y humilla a una persona a través de diferentes medios de comunicación digital -como el correo electrónico, mensajería instantánea, redes sociales, blogs- de forma repetitiva y recurrente con la finalidad de dañar su dignidad y autoestima.

En España dichas conductas pueden ser constitutivas de distintas formas delictivas: delitos contra la intimidad (descubrimiento y revelación de secretos), de amenazas, de pornografía infantil, contra el honor (injurias y calumnias), etc.

Ciberacoso escolar (Cyberbullying)

Tipo de ciberacoso realizado entre menores en el entorno escolar por medios tecnológicos.

Cibersexo o sexo virtual

Relación sexual en la que dos o más personas de forma voluntaria intercambian mensajes, fotografías o vídeos sexualmente explícitos a través de la Red.

Cifrado[6]

Método de seguridad que vuelve la información ilegible a quien no tenga la clave para descifrarla. Se utiliza generalmente para proteger las compras y otras transacciones de Internet. Cuando un sitio web indica que es "seguro", generalmente se refiere a que los datos que se envían y se reciben están cifrados.

3. Glosario

Contraseña (password)

Código que te permite acceder a diferentes servicios y dispositivos como la cuenta de correo o el teléfono móvil. Se dice que es robusta cuando es secreta, tiene como mínimo ocho caracteres (incluyendo letras mayúsculas, minúsculas, número y símbolos), no está repetida en múltiples dispositivos y se cambia cada cierto tiempo.

Cookies[7]

Pequeños archivos con datos que algunos sitios web depositan de forma automática en los ordenadores de las personas usuarias con el objetivo de almacenar información sobre sus preferencias.

Copia oculta (CCO)[8]

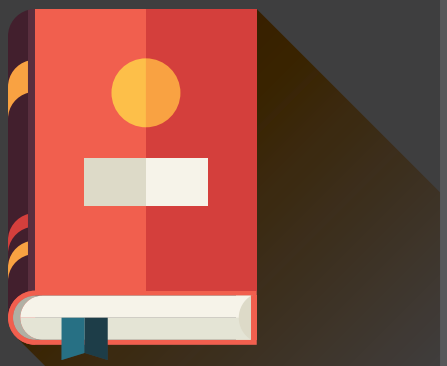
Correo electrónico remitido sin que se identifique a la persona o personas destinatarias. Se recomienda su uso cuando hay que enviar un mensaje a un gran número de personas. En inglés se define como BCC, acrónimo de: Blind Carbon Copy (copia ciega en papel carbón).

Copias de seguridad[9]

Copia de ficheros o datos para que estén disponibles en caso de que un fallo produzca la pérdida de los originales. Esta sencilla acción evita numerosos, y a veces irremediables problemas, siempre y cuando se realice de forma habitual y periódica.

Cortafuegos (firewall)

Sistema para prevenir que personas usuarias de Internet, tengan acceso a una red o a un servidor privado sin autorización. Todos los mensajes recibidos y enviados en una intranet protegida, pasan a través del cortafuegos, que examina cada mensaje y bloquea los que no tengan criterio o código de seguridad especificado.



3. Glosario

Correo no deseado (Spam)

Mensajes de correo electrónico no deseados, ni solicitados, que con frecuencia tienen fines publicitarios y comerciales.

Delitos informáticos o telemáticos

Se aplica a los delitos que se comenten a través de Internet o que utilizan la Red para cometer la actividad delictiva. España ratificó el "Convenio sobre Ciberdelincuencia" en el año 2010, trasponiendo a su ordenamiento jurídico las conductas delictivas que define el Convenio.

Derecho al olvido

Derecho de cualquier persona a exigir la cancelación de los datos personales propios que aparecen en buscadores de Internet. Derecho reconocido recientemente en una Sentencia del Tribunal de Justicia de la Unión Europea.

Enlace (Link)

Se trata un elemento en un documento digital que hace referencia a otro recurso, por ejemplo, otro documento o un punto específico del mismo o de otro documento. Haciendo clic en él se visualiza ese nuevo recurso.

Memoria USB

La memoria USB (Universal Serial Bus) es un tipo de dispositivo de almacenamiento de datos muy utilizado para guardar y transportar información personal creado en 1996. Es también conocido como: pendrive, memoria externa o lápiz de memoria, aunque técnicamente, USB se refiere sólo al puerto de conexión.

3. Glosario

Dominio

Nombre que identifica un sitio en la Red accesible vía web. Por ejemplo, el nombre de dominio http://www.inmujer.gob.es/ identifica la dirección de la web del Instituto de la Mujer y para la Igualdad de Oportunidades.

Encriptación[10]

Procedimiento que permite ocultar el contenido de un mensaje para que sólo las personas en posesión de la clave puedan leerlo tras haberlo descifrado o desencriptado. Encriptar un dato es ocultarlo.

Filtro antispam[11]

Opción que suelen ofrecer las aplicaciones de correo electrónico para realizar de forma automática determinadas acciones de selección sobre los mensajes de entrada y salida en función del contenido de uno o más campos del mensaje. Es muy útil para dejar de ver mensajes no solicitados o que no nos interesan.

Fomo

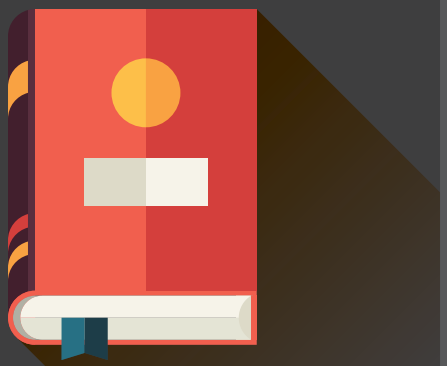
Del inglés Fear of Missing Out – miedo a perderse algo-. Se refiere al sentimiento de exclusión social en el ámbito de las nuevas tecnologías, sobre todo de las redes sociales, y se da cuando la persona necesita estar conectada constantemente con el fin de no sentirse excluida.

Formateo de equipos

Operación necesaria para preparar un disco y poder escribir en él bajo un sistema operativo determinado. Al formatear un disco con información grabada, ésta se pierde.

Fraude en la Red (Phishing)

Consiste en el envío por parte de la ciberdelincuencia una comunicación digital a un usuario simulando ser una



3. Glosario

entidad legítima -banco, institución pública, otro usuario. -con el objetivo de apropiarse de información privada. Los mensajes de tipo phishing usualmente contienen algún enlace a una página falsa que suplanta la identidad de una empresa o servicio en la que, si introducimos nuestros datos, éstos pasarán directamente a manos de quienes estafan.

Geolocalizador (Sistemas de localización)

Dispositivos que permiten determinar la situación exacta de personas, animales u objetos en tiempo real. Tienen múltiples aplicaciones como controlar el stock de una empresa, localizar objetos perdidos (teléfonos, vehiculos, embarcaciones, etc), personas extraviadas (deportistas de alto riesgo) o, contar en la Red dónde nos encontramos.

Gestor de contraseñas

Aplicación que te permite gestionar un gran número de contraseñas complejas, diferentes y seguras. Muchas de las empresas que comercializan antivirus cuentan con estas aplicaciones.

Hackers

Son personas que disfrutan alcanzando un alto grado de conocimiento sobre el funcionamiento interno de un sistema, ordenador o red de ordenadores, y se dedican a demostrar fallos en los sistemas de protección de una red de ordenadores. Cuentan con el respeto de la comunidad técnica de Internet[12]. Las personas que intentan acceder a un sistema informático sin autorización y con malas intenciones son denominadas crackers[13].

Historial del navegador o caché

Es la copia de las páginas web visitadas mantenida por un navegador, de manera que si vuelves a solicitarlas, son leídas desde el disco duro sin necesidad de tener que conectarte de nuevo a la Red, consiguiendo así una mejora

3. Glosario

apreciable del tiempo de respuesta[14]. El caché conserva no sólo el historial, sino también las cookies, la auto cumplimentación de formularios y las contraseñas, por lo que es recomendable borrarlo si consideramos que supone un riesgo para la privacidad o seguridad de los datos.

HTTPS

Protocolo que permiten la transmisión de información a direcciones protegidas con sistemas de cifrado. Este tipo de cifrado evita que la información enviada a través de la red pueda ser interceptada.

Identidad digital

Es el rastro que cada persona va dejando en Internet y a través del cual se le identifica. La identidad digital no existe a priori, sino que se va construyendo a medida que vamos participando en diferentes comunidades al generar contenidos personales: datos personales, imágenes, videos, opiniones y comentarios en las redes.

Identificación (Login)[15]

Proceso de seguridad que exige que una persona usuaria se identifique con un nombre (user-ID) y una contraseña para poder acceder a un ordenador o a un recurso.

Mailing o lista de correo

Lista de direcciones de correos electrónicos que se utiliza para distribuir mensajes a un grupo de personas.

Memoria RAM

Del inglés Radom Access Memory (Memoria de acceso aleatorio o directo). Se refiere a la memoria principal del ordenador donde se almacenan datos y programas.

3. Glosario

Navegador web o browser[16]

Programa que permite el acceso a Internet, interpretando la información de archivos y sitios web para que éstos puedan ser leídos.

Newsletter

Boletín informativo digital, que habitualmente se distribuye a través de listas de correos.

Nomofobia

Del inglés "No Mobile Phobia", se refiere al miedo irracional a salir sin el móvil o no tener conexión.

Pederastia[17]

Conducta delictiva de abuso o agresión sexual cometida contra menores.

Perfil

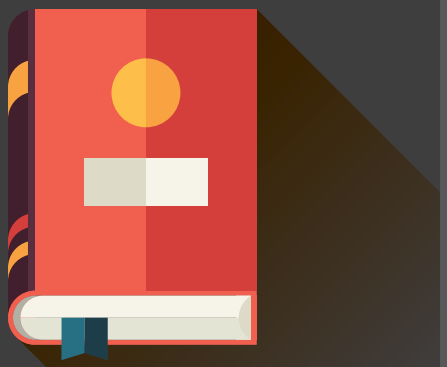
Es tu página personal de usuaria de un servicio y contiene información personal y/o profesional que deseas compartir con otras personas en las Redes Sociales. Dependiendo del servicio, puedes incluir sólo texto, texto y fotografía, enlaces, notas, etc.

Phubbing

Hace referencia al uso del teléfono móvil o la tablet mientras se está en compañía de otras personas (del inglés phone –teléfono- y snubbing -desairar-).

Plataformas de pago online

Sistemas de pago electrónico que facilita las transacciones en línea a través de Internet mediante una entidad



3. Glosario

financiera autorizada tano por quien vende, como por quien compra. Una de las plataformas de pago on-line más utilizadas es PayPal.

Pop-ups[18]

Ventanas emergentes con información no solicitada , habitualmente dedicada a mostrar publicidad. Pueden utilizarse programas bloqueadores de ventanas emergentes para bloquearlas.

Privacidad on-line

Concepto referido a los datos personales que publicamos en la Red como "dirección de correo electrónico", "fotografías", "teléfono" o "currículum profesional". En las redes sociales debemos facilitarlos de forma voluntaria para crearnos un perfil y poder participar así en las mismas, por lo que es necesario prestar atención al tipo de datos que compartimos para asegurar nuestra privacidad también en Internet.

Programa malicioso (Malware)[19]

Engloba a todo tipo de programa o código informático que se instala en nuestro equipo sin consentimiento ni conocimiento con el objetivo de alterar su funcionamiento y la información que contiene.

Qwerty

Se denomina así al uso de letras consecutivas del teclado para generar una contraseña. Este tipo de contraseñas son inseguras y fáciles de descifrar.

Rastro digital

Hace referencia a la información personal que circula por Internet, tanto la que se ha subido de manera voluntaria, como la que no, como por ejemplo notificaciones en el Boletín Oficial del Estado, multas, juicios, etc.

3. Glosario

Redes P2P

Del inglés "peer to peer" (entre iguales), es una red que conecta un gran número de ordenadores para compartir cualquier información que esté en formato digital. Todas las personas que se conectan a la Red aportan ancho de banda y capacidad de almacenamiento, siendo que a mayor cantidad de material compartido, mayor acceso a privilegios de velocidad y contenido.

Redes Sociales[20]

Estructuras sociales virtuales donde hay personas que se encuentran y relacionan entre sí. Las relaciones pueden ser de distinto tipo, como intercambios financieros, amistad, relaciones sexuales, etc. Se usa también como medio para la interacción como chats, foros, juegos en línea, blogs, etc. .

Reputación digital

Es la opinión o consideración social que se tiene sobre una persona u organización, a partir de lo que se construye sobre ella en la Red. Cada acción en Internet deja trazas que pueden ser localizadas y tratadas de modo independiente y ajeno a la voluntad de la propia persona, de ahí la importancia de saber gestionar y reflexionar sobre lo que publicamos ya que la red será testimonio de ese hecho.

Robots emisores de spam[21]

En la web, se conoce como robot a un programa que recorre la Red llevando a cabo tareas concretas, como por ejemplo crear listas de correos electrónicos para ser integradas en bases de datos que posteriormente se usan para hacer envíos de tipo spam.

3. Glosario

Saturación de servidores

Cuando aumenta el tráfico de información en tus equipos se reduce el ancho de banda saturando la capacidad de red del servidor, haciendo que sea imposible llegar a él.

Selfie (auto-foto)

Fotografía que una persona se hace a ella misma a través del móvil, Tablet o webcam para difundirla en la Red.

Servidores

Un servidor es un nodo que, formando parte de una red, provee servicios a otros nodos denominados clientes. Por ejemplo un servidor de archivos permite a varios ordenadores acceder a ficheros almacenados en un lugar centralizado y común.

Sex-casting

Variación del sexting que se produce cuando la imagen con contenido sexual es grabada en una webcam y se difunde a través del correo electrónico o las redes sociales.

Sexting

Práctica que consiste en el envío de imágenes o videos de contenido íntimo a través de dispositivos móviles de forma voluntaria a personas conocidas en la mayoría de los casos. En ocasiones, cuando el vínculo entre quien envía la fotografía y quien la recibe se rompe como por ejemplo en una ruptura de pareja, esta última puede utilizarla para chantajear, extorsionar y amenazar a su expareja produciendo así una situación de ciberacoso o maltrato.

3. Glosario

Sextorsión

Es un nuevo tipo de violencia sexual, en la cual, la víctima es chantajeada y, a veces, extorsionada (bajo la amenaza de publicar en la red imágenes suyas de contenido sexual) para obligarla a realizar favores sexuales, enviar nuevas imágenes eróticas, o exigirla dinero (Ver "Cuadernillo de sextorsión")

Sistema operativo

Conjunto de programas que se encarga de coordinar el funcionamiento de un ordenador, cumpliendo la función de interface entre los programas de aplicación, circuitos y dispositivos. Algunos de los más conocidos son el DOS, el Windows, el UNIX[22].

Software

Programas o elementos lógicos que hacen funcionar un ordenador o una red, o que se ejecutan en ellos, en contraposición con los componentes físicos del ordenador o la Red[23] . El software más importante de una computadora es el sistema operativo[24].

Tecnoadicción

Hace referencia a la falta de control en el consumo de las tecnologías, provocando cambios en la conducta y una pérdida de interés por otras actividades. Se define por las siguientes tres características: tolerancia (se necesita aumentar el tiempo de conexión para lograr satisfacción; abstinencia (por no utilizar la tecnología); y dependencia (al disminuir la tolerancia y aumentar la abstinencia la vida de las personas tecnoadictas se ve modificada).

TIC[25]

Acrónimo de "Tecnología de la Información y la Comunicación", es un concepto dinámico e histórico que modifica

3. Glosario

su contenido en función de cada época. Posibilita un nuevo entorno (Sociedad de la Información) que permite acceder, compartir, y reelaborar un gran volumen de información a escala global y en tiempo real. Todavía se mantiene vigente la brecha digital de género en intensidad, como en frecuencia y tipo de uso.

URL[26]

Del inglés "Uniform Resource Locator" (Localizador Uniforma de Recursos), es el sistema unificado de identificación de recursos en la Red.

Viralidad

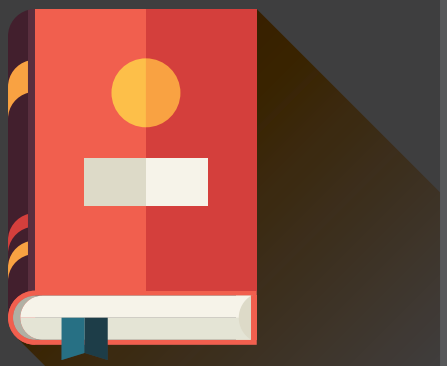
Hace referencia a la rapidez y exponencialidad con que se distribuye la información en la Red. La viralidad es una de las características claves de la comunicación en Internet, donde la información se reproduce, multiplica y se expande como un virus, sobre todo los contenidos caseros, anónimos y de carácter sexual.

Virus[27]

Pequeños programas que tienen la capacidad de autoduplicarse en diferentes dispositivos. Una vez que se difunden, los virus se activan bajo determinadas circunstancias y pueden provocar algún daño o molestia en los equipos infectados.

Wifi abierta

Del inglés "Wireless Fidelity", se utiliza como denominación genérica para los productos que incorporan cualquier variante dela tecnología inalámbrica 802.11, que permite la creación de redes de trabajo sin cables (conocidas como WLAN, Wireless Local Area Netwoks)[28]. Es abierta cuando puedes acceder a ella libremente y sin contraseña.



4. Recursos

Páginas webs de interés

Adminstración Pública

Agencia Española de Protección de Datos

→ www.agpd.es/portalweb/index-ides-idphp.php

Agencia Europea de Seguridad de las Redes y de la Información (ENISA)

→ http://www.enisa.europa.eu/

Brigada de Investigación Tecnológica. Cuerpo Nacional de Policía

→ http://www.policia.es/org_central/judicial/udef/bit_alertas.html.

Grupo de Delitos Telemáticos. Unidad Central Operativa de la Guardia Civil

→ https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

INSAFE. Programa Safer Internet. Comisión Europea

→ http://www.saferinternet.org/

Instituto Nacional de Ciberseguridad de España

→ http://www.inteco.es/

Observatorio Nacional de Telecomunicaciones y de la Sociedad de la Información

→ http://www.ontsi.red.es/ontsi/

4. Recursos

Oficina de atención al usuario de telecomunicaciones

→ http://www.usuariosteleco.es/Paginas/index.aspx

Oficina de Seguridad del Internauta

→ http://www.osi.es/

Agentes sociales

Asociación de internautas

→ http://www.internautas.org/

Chaval.es en la Red

→ http://www.chaval.es/chavales/

Centro de Seguridad de la Información de Cataluña. CESICAT

→ https://www.cesicat.cat/

Pantallas Amigas

→ http://www.pantallasamigas.net/

Protégeles

→ http://www.protegeles.com/

4. Recursos

Materiales consultados

Agencia Española de Protección de Datos (s.f.) *"Guía para la Lucha contra el Spam".*

→ http://goo.gl/cEa8qi

Asociación de Internautas (2002) *"III Estudio sobre bulos y fraudes en Internet".*

→ http://goo.gl/JdBxoF

Avilés, Ángel-Pablo (2013) *"X1Red+Segura – Informando y Educando. V1.0"*

→ http://goo.gl/tHRK9j

Calvo González, Soraya (2014) *"Materiales Didácticos para la coeducación. Construyendo contigo la igualdad. Unidad didáctica número 15, Identidades digitales".* Consejería de Presidencia. Instituto Asturiano de la Mujer y Políticas de Juventud.

→ http://goo.gl/Ix8smw

Canet Aymerich, Laura; Grisolía Pereira, Cristina y I Querol Bello, Raque (2006) "*Nuevos tiempos, nuevos usos y nuevas tecnologías".* Ayuntamiento de Barcelona.

→ http://goo.gl/9PrRjZ

Castaño Collado, Cecilia (2012) *"La brecha digital de género en España: análisis multinivel. (España, Europa, CCAA)".* Instituto de la Mujer. Madrid.

→ http://goo.gl/0A8svZ

4. Recursos

Consejería de Educación, Economía, Innovación y Ciencia (s.f.) *"Guía didáctica. Educar para proteger: familia y escuela".* Junta de Andalucía.

→ http://goo.gl/Lk7kgc

Consejería de Innovación, Ciencia y Empresa (s.f.) *"Guía de formación TIC para padres y madres de adolescentes. Educar para proteger. Edición 1.0."* Junta de Andalucía.

→ http://goo.gl/HPxHCI

Departamento Municipal de Educación (s.f.) *"Educar a los menores en el uso sin riesgos de Internet. Guía para Madres y Padres".* Colección Educación. Ayuntamiento de Vitoria –Gasteiz.

→ http://goo.gl/tFnjGO

Díaz-Aguado Jalón, Mª José (Dir.), Martínez Arias, Rosa y Martínez Babarro, Javier (2013) *"La evolución de la adolescencia española sobre la igualdad y la prevención de la violencia de género".* Ministerio de Sanidad, Servicios Sociales e Igualdad. Delegación del Gobierno para la Violencia de Género.

→ http://goo.gl/pAJNRa

Fernandez Calvo, Rafael; Asociación Técnica de Informática (s.f.) *"Glosario"* Anetcom. Conselleria de Economía, Industria, Turismo y Empleo. Generalitat Valenciana.

→ http://goo.gl/9mHFgw

Fundación Mapfre (Marzo 2014) *"Controla TIC"*. Magisterio (Suplemento), núm. 12015.

→ http://goo.gl/RdcxlJ

4. Recursos

INE (2014) *"Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares".*

→ http://www.ine.es

INTECO (2004) *"Estudio sobre la Ciberseguridad y Confianza en los hogares españoles".*

→ http://goo.gl/0Ha0Az

INTECO (2007) *"Consejos generales de seguridad".*

→ http://goo.gl/47m90p

INTECO (s.f.) *"Guía SOS contra el Ciberbullying para educadores."*

→ http://goo.gl/rqhaRY

INTECO (s.f.) *"Guía SOS contra el Ciberbullying para padres".*

→ http://goo.gl/EzXjXl

INTECO (s.f.) *"Guía SOS contra el Grooming para padres y educadores".*

→ http://goo.gl/RRfmQV

INTECO (s.f.) *"Guía de actuación contra el Ciberacoso para padres y educadores".*

→ http://goo.gl/qGAeN9

INTECO (s.f.) *"Guías legales: Protección del Derecho al Honor, a la Intimidad y a la propia imagen en Internet".*

→ http://goo.gl/IftLB2

INTECO (s.f.) *"Guía legal sobre Ciberbullying y Grooming".*

→ http://goo.gl/qv2NyP

4. Recursos

INTECO (s.f.) *"Guía legal sobre Privacidad en Internet".*

→ http://goo.gl/VAsZaU

INTECO (s.f.) *"Guía sobre seguridad y privacidad de las herramientas de geolocalización".*

→ http://goo.gl/0G1Ujg

INTECO (2009) *"Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres".*

→ http://goo.gl/4UHT86

INTECO (2012) *"Estudio sobre la percepción de los usuarios acerca de su privacidad en Internet".*

→ http://goo.gl/0uKpnY

Norton (s.f.) *"Glosario de seguridad en internet".*

→ http://goo.gl/u6yYkB

Orjuela López, Liliana. et al., (2014) *"Informe acoso escolar y ciberacoso: propuestas para la acción".* Save the Children. Ministerio de Sanidad, Servicios Sociales e Igualdad.

→ http://goo.gl/fCDjCg

Pérez San-José, Pablo (Dir.) (2011) *"Guía sobre adolescencia y sexting: qué es y cómo prevenirlo".* Observatorio de la Seguridad de la Información. INTECO y PantallasAmigas.

→ http://goo.gl/jUKs5n

Pérez San-José, Pablo. (Dir.) (2012) *"Guía para usuarios: identidad digital y reputación on line".* INTECO.

4. Recursos

→ http://goo.gl/q8zsVQ

"Plan de confianza en el ámbito digital" (2013). Ministerio de Industria, Energía y Turismo y Ministerio de Hacienda y Administraciones Públicas.

→ http://goo.gl/3mx08Q

Presidencia de Gobierno (2013) *"Estrategia de Ciberseguridad Nacional"*. Departamento de Seguridad Nacional.

→ http://goo.gl/3FCM6D

Protégeles (2009) *"Menores y Tecnoadicción"*. Estudio empírico. Madrid.

→ http://goo.gl/vydpfF

Protégeles (s.f.) *"Ciberbullying y privacidad. Guía para profesores"*. Programa Daphne III.

→ http://goo.gl/CnmeFB

Protégeles (s.f.) *"Guía parental. Manteniendo a sus niños seguros en Internet"*.

→ http://goo.gl/ph8lic

Red2Red Consultores (2008) *"Mujeres y nuevas tecnologías de la información y la comunicación"*. Instituto de la Mujer. Madrid.

→ http://goo.gl/oEbTfG

Save the Children (s.f.) *"Una experiencia de buena práctica en intervención sobre el abuso sexual infantil". Informe sobre el Programa de Prevención y sensibilización del abuso sexual infantil (1998 – 2004).*

→ http://goo.gl/krTOBb

4. Recursos

Torres Albero, Cristóbal (Dir.), Robles, José Manuel y de Marco, Stefano (2013) *"El ciberacoso como forma de ejercer la violencia de género en la juventud: un riesgo en la sociedad de la información y del conocimiento"*. Madrid. Servicio de Publicaciones del Ministerio de Sanidad, Servicios Sociales e Igualdad. Delegación del Gobierno para la Violencia de Género.

→ http://goo.gl/84Hc5z

Urbas, Andrea; Reiman, Mariela (2009) *"Por un uso seguro y responsable de las tecnologías de la información y comunicación"*. Asociación Chicos.net. Ciudad de Buenos Aires. Argentina.

→ http://goo.gl/YzWLrA

Herramientas de seguridad

Oficina de Seguridad del Internauta

→ http://goo.gl/sOAuSd

Para sistemas Android

→ http://goo.gl/tjvpSI

Para sistema Windows

→ http://goo.gl/p2v26N

Referencias

[1] INE (2014) *"Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares".*
Disponible en: http://www.ine.es
Consultado [22/1072014]

[2] Torres Albero, Cristóbal (Dir.), Robles, José Manuel y de Marco, Stefano (2013) *"El ciberacoso como forma de ejercer la violencia de género en la juventud: un riesgo en la sociedad de la información y del conocimiento"* . Servicio de Publicaciones del Ministerio de Sanidad, Servicios Sociales e Igualdad. Delegación del Gobierno para la Violencia de Género. pág.163.
Disponible en: http://www.msssi.gob.es/ssi/violenciaGenero/publicaciones/estudiosinvestigaciones/Estudios_Investigaciones/Ciberacoso.htm

Díaz-Aguado Jalón, Mª José (Dir.), Martínez Arias, Rosa y Martínez Babarro, Javier (2013) *"La evolución de la adolescencia española sobre la igualdad y la prevención de la violencia de género".* Servicio de Publicaciones del Ministerio de Sanidad, Servicios Sociales e Igualdad. Delegación del Gobierno para la Violencia de Género. pág. 301.
Disponible en: en:http://www.msssi.gob.es/ssi/violenciaGenero/publicaciones/estudiosinvestigaciones/Estudios_Investigaciones/Evoluc_Adolescenc_Prevenc_V_G.htm

Consultado [10/11/2014]

[3] Definición de acoso sexual de la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres. Según el Art. 184 del Código Penal se define, como el comportamiento por el cual se solicitan favores de naturaleza sexual, para sí o para un tercero, en el ámbito de una relación laboral, docente o de prestación de servicios, continuada o habitual, y con tal comportamiento provocare a la víctima una situación objetiva y gravemente intimidatoria, hostil o humillante, continuados o habituales provocando a la víctima una situación objetiva y gravemente intimidatoria, hostil o humillante.

[4] Fernandez Calvo, Rafael; Asociación Técnica de Informática (s.f.) *"Glosario"* Anetcom. Conselleria de Economía, Industria, Turismo y Empleo. Generalitat Valenciana.
Disponible en: http://www.usc.es/atpemes/IMG/pdf/glosario_Internet_pymes.pdf
Consultado [1/10/2014]

[5] *Ibid.*

[6] Norton (s.f.) *"Glosario de seguridad en internet".*
Disponible en: http://es.norton.com/security-glossary/article
Consultado [1/10/2014]

[7] Avilés, Ángel-Pablo (2013) *"X1Red+Segura – Informando y Educando. V1.0"*

Referencias

Disponible en: https://www.gdt.guardiacivil.es/webgdt/publicaciones/x1redmassegura/x1red+segura.pdf
Consultado [1/10/2014]

[8] Fernandez Calvo, Rafael; Asociación Técnica de Informática (s.f.) *"Glosario"* Anetcom. Conselleria de Economía, Industria, Turismo y Empleo. Generalitat Valenciana.
Disponible en: http://www.usc.es/atpemes/IMG/pdf/glosario_Internet_pymes.pdf
Consultado [1/10/2014]

[9] *Ibid.*

[10] *Ibid.*

[11] *Ibid.*

[12] Avilés, Ángel-Pablo (2013) *"X1Red+Segura – Informando y Educando. V1.0"*
Disponible en: https://www.gdt.guardiacivil.es/webgdt/publicaciones/x1redmassegura/x1red+segura.pdf
Consultado [1/10/2014]

[13] Fernandez Calvo, Rafael; Asociación Técnica de Informática (s.f.) *"Glosario"* Anetcom. Conselleria de Economía, Industria, Turismo y Empleo. Generalitat Valenciana.
Disponible en: http://www.usc.es/atpemes/IMG/pdf/glosario_Internet_pymes.pdf
Consultado [1/10/2014]

[14] *Ibid.*

[15] Avilés, Ángel-Pablo (2013) *"X1Red+Segura – Informando y Educando. V1.0"*
Disponible en: https://www.gdt.guardiacivil.es/webgdt/publicaciones/x1redmassegura/x1red+segura.pdfConsultado [1/10/2014]

[16] *Ibid.*

[17] Real Academia Española

Referencias

Disponible en: http://lema.rae.es/drae/?val=pederasta
Consultado [1/10/2014]

Save the Children (s.f.) *"Una experiencia de buena práctica en intervención sobre el abuso sexual infantil" Informe sobre el Programa de Prevención y sensibilización del abuso sexual infantil (1998 – 2004)*
Disponible en: http://www.savethechildren.es/docs/Ficheros/26/informe%20abuso%20sexual%20def.pdf
Consultado [1/10/2014]

[18] Avilés, Ángel-Pablo (2013) *"X1Red+Segura – Informando y Educando. V1.0"*
Disponible en: https://www.gdt.guardiacivil.es/webgdt/publicaciones/x1redmassegura/x1red+segura.pdf
Consultado [1/10/2014]

[19] Fernandez Calvo, Rafael; Asociación Técnica de Informática (s.f.) **"Glosario"** Anetcom. Conselleria de Economía, Industria, Turismo y Empleo. Generalitat Valenciana.
Disponible en: http://www.usc.es/atpemes/IMG/pdf/glosario_Internet_pymes.pdf
Consultado [1/10/2014]

[20] Avilés, Ángel-Pablo (2013) *"X1Red+Segura – Informando y Educando. V1.0"*
Disponible en: https://www.gdt.guardiacivil.es/webgdt/publicaciones/x1redmassegura/x1red+segura.pdf
Consultado [1/10/2014]

[21] Fernandez Calvo, Rafael; Asociación Técnica de Informática (s.f.) *"Glosario"* Anetcom. Conselleria de Economía, Industria, Turismo y Empleo. Generalitat Valenciana.
Disponible en: http://www.usc.es/atpemes/IMG/pdf/glosario_Internet_pymes.pdf
Consultado [1/10/2014]

[22] *Ibid.*

[23] Fernandez Calvo, Rafael; Asociación Técnica de Informática (s.f.) *"Glosario"* Anetcom. Conselleria de Economía, Industria, Turismo y Empleo. Generalitat Valenciana.
Disponible en: http://www.usc.es/atpemes/IMG/pdf/glosario_Internet_pymes.pdf
Consultado [1/10/2014]

Referencias

[24] Avilés, Ángel-Pablo (2013) *"X1Red+Segura – Informando y Educando. V1.0"*
Disponible en: https://www.gdt.guardiacivil.es/webgdt/publicaciones/x1redmassegura/x1red+segura.pdf
Consultado [1/10/2014]

[25] Instituto de la Mujer y para la Igualdad de Oportunidades. "*Plan de acción para la igualdad de oportunidades de mujeres y hombres en la socied*ad de la *información 20*14-2017"
Disponible en: http://www.inmujer.gob.es/areasTematicas/sociedadInfo/docs/PlanAccionSocInformacion.pdf
Consultado [4/11/2014]

[26] Fernandez Calvo, Rafael; Asociación Técnica de Informática (s.f.) *"Glosario"* Anetcom. Conselleria de Economía, Industria, Turismo y Empleo. Generalitat Valenciana.
Disponible en: http://www.usc.es/atpemes/IMG/pdf/glosario_Internet_pymes.pdf
Consultado [1/10/2014]

[27] Avilés, Ángel-Pablo (2013) *"X1Red+Segura – Informando y Educando. V1.0"*
Disponible en: https://www.gdt.guardiacivil.es/webgdt/publicaciones/x1redmassegura/x1red+segura.pdf
Consultado [1/10/2014]

[28] Fernandez Calvo, Rafael; Asociación Técnica de Informática (s.f.) "*Glosario"* Anetcom. Conselleria de Economía, Industria, Turismo y Empleo. Generalitat Valenciana.
Disponible en: http://www.usc.es/atpemes/IMG/pdf/glosario_Internet_pymes.pdf
Consultado [1/10/2014]

Materiales didácticos **"Confianza y seguridad de las mujeres en la Red"**

Identidad digital, reputación y privacidad on-line

Actividades didácticas

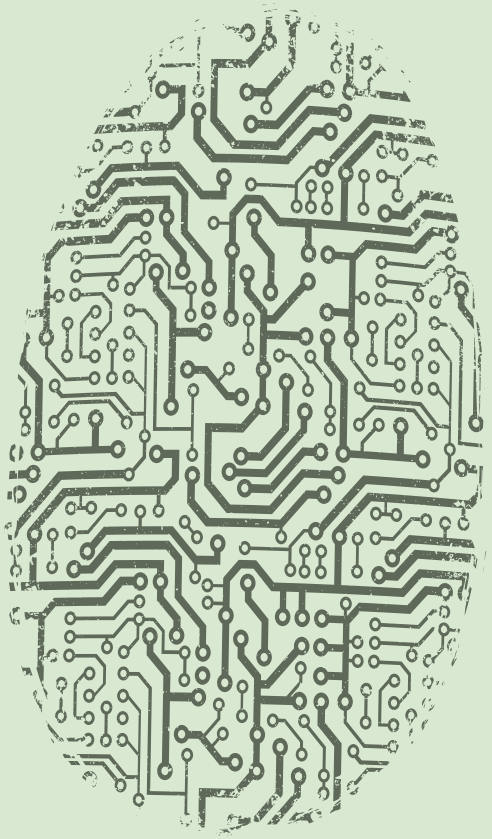
Objetivos generales

Al acabar las actividades, las participantes serán capaces de:

- Identificar cuáles son las prácticas más importantes para gestionar la identidad y reputación digital en la Red.
- Asegurar la confidencialidad de los datos de carácter personal propios o de terceras personas en la Red.

¿Dónde sucede?

Correo electrónico | Redes sociales | Juegos en línea | Chat | Mensajería instantánea



1 Actividad — Envío de mails

2 Actividad — Derecho al olvido en Internet

3 Actividad — La plaza del pueblo

4 Actividad — Configuración de la privacidad en las redes sociales

5 Actividad — Etiquetado de las imágenes en las redes sociales

6 Actividad — Suplantación de la identidad

MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
SECRETARÍA DE ESTADO DE SERVICIOS SOCIALES E IGUALDAD
INSTITUTO DE LA MUJER Y PARA LA IGUALDAD DE OPORTUNIDADES
Unión Europea
Fondo Social Europeo

Envío de mails

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Tomar conciencia del rastro que se deja en la Red cuando publicamos y compartimos información de carácter personal, incluyendo fotografías y vídeos.
- Reflexionar acerca del alcance y las posibles consecuencias cuando se vulnera la confidencialidad de los datos de carácter personal de terceras personas en la Red.
- Aprender a gestionar la confidencialidad de datos en el envío de correos electrónicos.

1
Actividad

Recursos y materiales

PC

Tiempo

15 min.

Envío de mails

1
Actividad

Desarrollo

1. Cada una de las participantes entrará en su cuenta de correo electrónico de manera individual, y comprobará:
    a) Si en los últimos 10 correos que ha recibido se muestran las direcciones de todas las personas destinatarias o están ocultas.
    a) Si en los últimos 10 correos que ha enviado se muestran las direcciones de todas las personas destinatarias o están ocultas.
2. Para facilitar el debate posterior, y poner de manifiesto las consecuencias de estos actos, el equipo facilitador leerá el siguiente caso basado en un hecho real:

CASO BASADO EN UN HECHO REAL

El concejal de cultura de un pequeño Ayuntamiento decidió sumarse a las nuevas tecnologías y remitir el pregón de fiestas por correo electrónico a todos sus contactos. Al hacer el envío, olvidó poner las direcciones en la pestaña "CCO" [con copia oculta], así que las direcciones, nombres y apellidos de todos sus contactos fueron visibles. Algunas de las personas que recibieron el correo, ofendidas por ver cómo sus datos personales se habían hecho públicos, solicitaron información sobre qué hacer para corregir lo que consideraban una irregularidad. Les dijeron que aunque el concejal lo hizo por error y sin mala fe, el daño no era reparable: la información ya se había remitido y todo el mundo tenía los correos electrónicos. Finalmente, decidieron interponer denunciar ante la Agencia de Protección de Datos, que impuso una infracción al Ayuntamiento.

Recuerda que

- Es importante preservar la privacidad de nuestros contactos y evitar el reenvío en cadena. Cuando envíes correos electrónicos a un grupo de personas debes asegurarte de poner las direcciones en la pestaña "CCO" (copia oculta), así garantizas la protección de datos de carácter personal de tus destinatarias.
- Si te apuntas a una lista de correo y al recibir los mensajes, las direcciones están visibles, tienes derecho a exigir que no vuelva a ocurrir, e incluso a denunciar si quieres conservar la privacidad de tus datos personales.

Envío de mails

1
Actividad

Desarrollo

3. En plenario, el equipo facilitador lanzará las siguientes preguntas y conducirá el debate acerca de la importancia de la confidencialidad en la Red:

   a) ¿Cómo solemos enviar nosotras los correos electrónicos?, ¿ponemos todas las direcciones visibles u ocultas?, ¿y cuándo nos escriben a nosotras?
   b) ¿Cuándo es importante mantener la confidencialidad de las personas destinatarias en los correos electrónicos utilizando la "copia oculta" (CCO)?
   c) ¿Qué consecuencias puede tener para nosotras que otras personas conozcan nuestro correo electrónico sin nuestro consentimiento?

Derecho al olvido en Internet

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Conocer la información pública (accesible en la Red) que se vincula a nuestro nombre en los buscadores más utilizados en Internet.
- Saber qué pasos hay que seguir en caso de que deseemos dar de baja los datos personales de un buscador o servicio on-line.

2 Actividad

Recursos y materiales

PC

PIZARRA

Tiempo

15 min.

Derecho al olvido en Internet

2
Actividad

Desarrollo

1. Las participantes entrarán de manera individual en: www.google.es (el buscador utilizado en España en un 94% de los casos), y cada una de ellas pondrá en el "campo de búsqueda" su nombre y apellidos entre comillas.
2. Deberán dedicar aproximadamente 5 minutos para comprobar qué información se vincula con su nombre, y responder individualmente a las siguientes preguntas:
    a) ¿Sabías que esta información era accesible en la Red?
    b) ¿Es información veraz?, ¿está actualizada o desactualizada?
    c) ¿Te favorece de alguna manera que esté publicada en la Red, te perjudica o te resulta indiferente?
    d) Si quisieras que esa información desaparezca, ¿sabrías cómo hacerlo?
3. Finalizadas las búsquedas individuales, a través de una lluvia de ideas grupal, irán comentando las cuestiones que les hayan suscitado mayor inquietud sin entrar en temas demasiado personales. El equipo facilitador hará una recogida en la pizarra o papelógrafo de las cuestiones más interesantes o sorprendentes que hayan salido, apuntando que la reputación on-line es la opinión o consideración social que se tiene sobre una persona u organización, construida a partir de lo que se muestra sobre ella en la Red. Se configura a partir de la información personal, con independencia del momento en el que fue generada. Cada acción en Internet deja trazas que pueden ser localizadas y tratadas de modo independiente y ajeno a la voluntad de la propia persona, de ahí la importancia de saber gestionar y reflexionar sobre lo que publicamos ya que la red será testimonio de ese hecho.

Recuerda que

- Deberías revisar periódicamente el rastro que dejas en Internet, y así saber qué puede saberse de ti a través de los buscadores más populares como por ejemplo "google".
- El "derecho al olvido" en la Red ya está reconocido por el Tribunal de Justicia de la Unión Europea, y puedes acogerte a él en caso de que lo necesites. Google dispone de un formulario para que puedas tramitarlo entrando en el siguiente enlace: https://support.google.com

Derecho al olvido en Internet

2
Actividad

Desarrollo

4. Finalizada la dinámica, se expondrá el siguiente caso explicando el "derecho al olvido":

CASO BASADO EN UN HECHO REAL

Una alta ejecutiva, directiva de una empresa de finanzas, puso por curiosidad su nombre en un buscador de Internet, y se sorprendió al ver que aparecía relacionada con una denuncia por impago ocurrida hacía 20 años. La denuncia quedó resuelta en su día, y no quería que apareciera en Internet esa situación superada ya en el pasado.

Estaba preocupada por el efecto negativo que podría tener sobre su reputación profesional, y exigió al buscador que eliminase esa información ya obsoleta, pero se negaron a hacerlo, justificándose en que simplemente mostraban información de otra página web. Así que se puso en contacto con esta web que contenía la denuncia, pero se negaron a retirarla porque alegaban que la información era cierta.

La plaza del pueblo

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Reconocer los riesgos que amenazan la seguridad y privacidad en la Red.
- Valorar las posibles consecuencias cuando terceras personas violan nuestra intimidad en la Red.

Recursos y materiales


Tijeras


Papel


Imperdibles


Tarjetas

El equipo facilitador aportará 9 tarjetas con los roles que tienen que interpretar. Habrá dos tipos de tarjetas. El contenido de cada una de las tarjetas se encuentra en la siguiente ficha para recortar.

3
Actividad

Tiempo

25 min.

La plaza del pueblo

3
Actividad

Recursos y materiales

Tarjetas para recortar.

1
Dueña del bar
Escenario

2
Directora del Banco
Escenario

3
Dependienta de una panadería
Escenario

4
Estudiante
Rol

5
Alcaldesa
Rol

6
Mendiga
Rol

7
Vecina humilde
le ha tocado la lotería
Rol

8
Morosa
Rol

9
Vecina
Rol

La plaza del pueblo

3
Actividad

Desarrollo

1. Se llevará a cabo una dinámica de roles. El equipo facilitador, pedirá la participación voluntaria de 9 mujeres. El resto de las participantes permanecerán como observadoras del juego.

2. A las 9 participantes se les entregará una tarjeta donde pondrá el rol que tienen que interpretar:

3. Para las mujeres que interpretan los roles de las tarjetas 1, 2 y 3:
    - Saben qué papel les ha tocado, quienes son y cómo tienen que comportarse si estuvieran en el siguiente contexto: "plaza del pueblo" de un municipio imaginario.
    - Se tendrán que colocar entre ellas las tarjetas en una parte visible con un alfiler o imperdible.

4. Para las mujeres que interpretan los roles de las tarjetas 4, 5, 6, 7, 8 y 9:
    - No saben qué papel tienen que representar y tampoco se les da ningún tipo de instrucciones sobre cómo deben actuar.
    - La única información que saben es que están en la "plaza del pueblo", y las escenas se desarrollan: "entrando en el bar", "hablando en el banco" o "comprando en la panadería".
    - Se tendrán que colocar entre ellas las tarjetas en el hombro con un alfiler o imperdible, de tal manera que las compañeras puedan ver la tarjeta con el rol que tienen que interpretar, pero ellas mismas no. Deben permanecer sin saber lo que pone en sus tarjetas hasta el final de la actividad.

5. La consigna del juego es la siguiente: tienen que relacionarse y charlar en función del rol que cada una ve en la tarjeta de la otra, pero no pueden decirle cuál es el papel que representa.

Recuerda que

- Internet en ocasiones funciona como "la plaza del pueblo", y las etiquetas que nos ponen construyen nuestra imagen social, y en Internet, nuestra "reputación digital".
- El rastro que cada persona deja en Internet perdurará siempre, y dada la rapidez con que se propaga la información, es casi imposible eliminarlo, así que ¡cuidado con lo que compartes! La viralidad es una de las características claves de la comunicación en Internet, donde la información se reproduce, multiplica y se expande como un virus.
- Si participas en la Red dando tus opiniones, recuerda ser respetuosa y no publiques informaciones falsas, a veces podemos hacer daño aunque sea bromeando.

La plaza del pueblo

3
Actividad

Desarrollo

6. Pasados 10 minutos se da por finalizado el juego de roles y las participantes vuelven a sentarse. Aquellas que han interpretado los roles de las tarjetas 4, 5, 6, 7, 8 y 9 no podrán todavía saber qué papel les había tocado.

7. Después de la teatralización, el equipo facilitador preguntará:

   - A las participantes que han interpretado los roles de las tarjetas 1, 2 y 3: ¿qué diferencias de comportamiento habéis tenido con cada personaje?
   - A las participantes que han interpretado los roles de las tarjetas 4, 5, 6, 7, 8 y 9: ¿cómo os habéis sentido?, ¿cómo os han tratado?, ¿habéis notado un trato especial?, ¿qué pensáis que tenéis escrito en vuestras tarjetas? Una vez contestadas y debatidas estas preguntas, podrán mirar la tarjeta representada.

Configuración de la privacidad en las redes sociales

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Tomar conciencia de la importancia de controlar la privacidad en las redes sociales.
- Saber configurar las opciones de privacidad en las redes sociales.

4
Actividad

Recursos y materiales

PC

Tiempo

10 min.

Configuración de la privacidad en las redes sociales

4
Actividad

Desarrollo

1. Se trabajará en grupos de 3 mujeres como máximo y cada grupo elegirá una relatora.

2. Se pedirá a cada grupo que debata sobre las siguientes cuestiones:

    a) ¿Tengo perfil o no de Facebook? Si no tengo perfil de Facebook y quiero hacerlo, ¿conozco cómo se hace y cómo puedo configurar mi privacidad?
    b) ¿Cómo lo tengo configurado?, ¿he tomado las precauciones para proteger mi privacidad?, ¿es accesible la política de privacidad de la red social Facebook?, ¿la he leído y estoy conforme antes de darme de alta?
    c) ¿Me he planteado qué cuestiones de mi vida personal quiero que se conozcan en la red social?, ¿soy consciente de la transcendencia de hacer públicas todas ellas?

3. Una vez que cada grupo haya debatido las cuestiones, cada relatora expondrá en plenario las conclusiones de su grupo.

4. El equipo facilitador entrará en Facebook y hará una simulación colectiva para que las participantes sigan conjuntamente el enlace de Facebook que lleva a su política de uso de datos.

Recuerda que

- Todas las redes tienen una política de privacidad, tómate tu tiempo para configurar de manera segura el perfil que quieres tener.
- Debes estar al tanto de los cambios en la política de privacidad de las redes en las que participas.
- Cuando te inscribas en una nueva red social debes leer con detenimiento su política de privacidad, y tienes derecho a preguntar lo que consideres necesario en caso de no entender algo.

Etiquetado de las imágenes en las redes sociales

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Tomar conciencia de que cualquier imagen en Internet, ya sea suya o no, puede asociarse a su identidad en la Red.
- Aprender a gestionar el etiquetado de las imágenes.

Recursos y materiales

PC

5
Actividad

Tiempo

15 min.

Etiquetado de las imágenes en las redes sociales

5
Actividad

Desarrollo

1. Se trabajará en grupos de 3 mujeres como máximo y cada grupo elegirá una relatora.

2. Se pedirá que lean previamente el siguiente caso real para responder después a una serie de preguntas:

CASO BASADO EN UN HECHO REAL

Julia ha sido etiquetada junto a más gente en una foto de la fiesta de su facultad. La foto aparece en un post con el título "Botellón en la facultad". Julia acude a una entrevista de trabajo y la entrevistadora le confiesa que ha visto esa foto al buscar más detalles sobre su formación académica, lo que le supone un gran bochorno y quizá la pérdida de una oportunidad de trabajo. Julia sabía de la existencia de la foto pero no pensó en las consecuencias. Ahora Julia quiere que la des-etiqueten de la foto.

a) ¿Qué puede hacer Julia para no ser etiquetada en la foto?, ¿habéis pensado como tenéis configurada vuestra privacidad en las redes sociales?
b) ¿Qué podía haber hecho en la entrevista de trabajo ante una situación así sobre su vida personal?
c) ¿Conozco cómo se etiquetan y se des-etiquetan las imágenes subidas en las redes sociales?

3. Una vez reflexionado en pequeños grupos, el equipo docente mostrará de manera guiada el contenido del enlace de una red social que lleva a "cómo funcionan las etiquetas" y cómo gestionarlas.

Recuerda que

- Si decides publicar vídeos o fotos en tus redes sociales, valora el contenido de las mismas puesto que te identifican físicamente.
- Cuando subes una imagen de alguna persona a la Red sin su consentimiento, estás violando su privacidad. Para un uso responsable debes pedir permiso antes de hacerlo y etiquetarla en la fotografía. Así, esa persona estará informada en todo momento de las fotografías suyas que circulan por la Red, y podrá eliminarlas cuando lo desee.

Etiquetado de las imágenes en las redes sociales

5
Actividad

Desarrollo

4. Para finalizar, se abrirá un debate sobre cómo se construye nuestra identidad digital. Con la llegada de la web 2.0 cualquier persona puede participar, publicar y compartir tanto textos como imágenes o vídeos en Internet, en diferentes espacios como:

    a) Fotografías: Flikcr, Picasa, Fotolog.

    b) Vídeos: Youtube, Vimeo.

    c) Presentaciones: Slideshare.

    d) Redes sociales y profesionales: Facebook, Tuenti, Twitter, Myspace, Xing, Viadeo, Linkedin.

    e) Blogs personales: Blogger, Wordpress.

Toda actividad que genera una persona en la Red constituye su visibilidad, que puede ser positiva o negativa. Esta visibilidad puede ser autoconstruida a partir de los posts de un blog, los mensajes de Twitter, los comentarios a vídeos, fotos..., pero también puede ser fruto de referencias o comentarios de terceras personas.

Suplantación de identidad

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Analizar situaciones reales de suplantación de la identidad en Internet.

6 Actividad

Recursos y materiales


Papel


Bolígrafos


Textos con los los 2 casos

Tiempo

20 min.

Suplantación de identidad

6
Actividad

Desarrollo

1. Se trabajará en 2 grupos. Cada grupo elegirá una relatora.
2. A un grupo se le entregará la noticia A: "Condenado por suplantar la identidad de otro en una web de contactos"; y al otro grupo la noticia B: "Detenido un hombre por ofrecer servicios sexuales de su expareja en la web".

A. CASO BASADO EN UNA NOTICIA

Condenado por suplantar la identidad de otra persona en una web

Dos personas iniciaron una relación virtual a través de Internet. La persona procesada entró fraudulentamente en la cuenta de correo electrónico gratuito de la víctima, y envió mensajes a los contactos que tenía en su agenda virtual, difundiendo de esta manera sus datos personales. Unido a esto, la imputada modificó las claves de acceso, impidiendo que la víctima pudiera acceder a ellas. Un tiempo después, la persona acusada utilizó los datos personales de la víctima para inscribirse en una página de contactos a su nombre. Un juzgado dictó condena de cuatro años de cárcel y pagar 5.400 € por "intromisión de la intimidad y falsedad de documento mercantil".

Recuerda que

- El robo de identidad es un delito que se ha incrementado con el uso de Internet. La suplantación de identidad no solamente puede derivar en fraudes económicos sino que también puede afectar a la reputación de la víctima, violando su espacio privado y personal, así como su honor.

Suplantación de identidad

6
Actividad

Desarrollo

B. CASO BASADO EN UN NOTICIA:

Detenido un hombre por ofrecer servicios sexuales de su expareja

La víctima, de 20 años, interpuso una denuncia porque estaba recibiendo numerosas llamadas telefónicas de hombres interesados en los servicios sexuales que supuestamente ella ofrecía en una web, donde figuraban su nombre, su número de teléfono y unas fotografías de contenido erótico. La Policía inició entonces las investigaciones e informó a la víctima de los pasos que debía seguir para bloquear y borrar el anuncio.

Realizadas las investigaciones pertinentes, los agentes determinaron que el autor del anuncio era su exnovio, que había cometido el delito como venganza hacia ella por terminar con la relación debido a sus continuos ataques de celos. Tras declarar, se le puso en libertad con cargos, comunicando las diligencias policiales al Juzgado de Instrucción de Guardia.

3. Cada grupo debatirá y contestará por escrito las siguientes preguntas durante 5 minutos:

a) ¿Qué es la identidad digital?, ¿cómo se construye?

b) ¿Qué ha motivado la suplantación de la identidad?

c) ¿Qué crees que podría haber hecho la víctima para protegerse?

d) ¿Qué consecuencias ha tenido para el suplantador?

Suplantación de identidad

6
Actividad

Desarrollo

4. Cada relatora leerá la noticia de su grupo en el plenario y después las respuestas de su grupo.

5. El equipo facilitador guiará el debate, haciendo hincapié en las diferencias encontradas entre el primer y el segundo caso, lanzando la siguiente pregunta: ¿Qué diferencias o similitudes hay entre las dos historias?

> Además, recordar que la identidad digital es el rastro que cada persona va dejando en Internet, el conjunto de características que nos identifican dentro de la Red, es decir, lo que somos en la Red para las demás personas. La identidad digital no existe a priori, sino que se va construyendo a medida que vamos participando en diferentes comunidades al generar contenidos personales: Datos personales, imágenes, videos, opiniones y comentarios en blogs, etc

Consejos y buenas prácticas

Recomendaciones preventivas para proteger tu identidad digital y privacidad

- Si decides hacerte un perfil en las redes sociales, diferencia el perfil personal del profesional, nunca los vincules.
- Dedica tiempo suficiente a configurar los parámetros de privacidad y seguridad de tus redes sociales para asegurarte de quién puede tener acceso a tus datos personales, revisándolos periódicamente ya que pueden cambiar.
- Si decides usar herramientas de geolocalización, es aconsejable que pienses en su utilidad y si realmente son necesarias.
- No facilites datos personales innecesarios o que resulten inapropiados, una vez que lo hayas hecho, es muy probable que queden fuera de tu control.
- Si decides publicar vídeos o fotos en tus redes sociales, valora el contenido de las mismas puesto que te identifican físicamente.
- Si participas en la Red dando tus opiniones, recuerda ser respetuosa y no publiques informaciones falsas.
- Cuida y ten presente lo que las demás personas comentan de ti en la Red. Tu reputación on-lie tendrá relevancia no sólo en el presente sino también en el futuro, por tanto, piensa antes de publicar cualquier información en Internet.
- Al utilizar el correo electrónico, asegúrate de proteger la privacidad de tus contactos y la tuya.

Consejos si tu identidad y reputación se ven afectadas de manera negativa

- Si consideras que tu información personal se ha utilizado indebidamente, puedes reclamar al proveedor del servicio de Internet, bajo el amparo del derecho de acceso, rectificación, cancelación u oposición (ARCO) al tratamiento.
- Además, en el caso de que dicho comportamiento sea constitutivo de delito, puedes denunciarlo ante las Fuerzas y Cuerpos de Seguridad del Estado que disponen de unidades policiales especializadas[1] y canales de denuncia a disposición de las personas usuarias.
- Has de saber que la Agencia Española de Protección de Datos pone a disposición una sede electrónica con la posibilidad de solicitar la tutela de derechos, o plantear una denuncia en relación con tus datos personales.
- En 2014, una Sentencia del Tribunal de Justicia de la Unión Europea reconoce el derecho al olvido, por el cual, cualquier persona tiene derecho a exigir la cancelación de sus datos personales que aparecen en buscadores de Internet, siempre y cuando la informa ción hacia la que enlace comporte daños hacia su persona, afectando así a sus derechos fundamentales.
- Si te apuntas a una lista de correo y al recibir los mensajes, las direcciones están visibles, tienes derecho a exigir que no vuelva a ocurrir, e incluso a denunciar si quieres conservar a privacidad de tus datos personales.

Identidad digital, reputación y privacidad on-line

Datos de interés

Identidad digital: Información que publico + Información que comparto + Información que existe sobre mi [2].

¿Qué riesgos pueden afectar a nuestra privacidad y seguridad en la Red?

- Suplantación de identidad para el fraude, falsedad o robo de información. Ejemplos comunes de este tipo de riesgos son: Creación en las redes sociales de un perfil falso para interactuar haciéndose pasar por ti, o envío de correos electrónicos en tu nombre.
- Vulneración de nuestra intimidad que puede derivar en sobrexposición, y/o acceso a datos sensibles por:
  - Configuraciones insuficientes de las opciones de privacidad.
  - Alteración de la privacidad derivada de la sincronización entre plataformas.
  - Etiquetado en imágenes por otras personas.
  - Sexting.
  - Uso de cookies sin nuestro conocimiento.
  - Terceras personas pueden compartir información tuya sin tu consentimiento y conocimiento.
- Ataques a la imagen y reputación: Amenazas, burlas, injurias, etc.
- Permanencia de la información en la Red, ya que es imborrable, desactualizada, y descontextualizada.

Siguiendo las recomendaciones de INTECO, hay que diferenciar entre seguridad y privacidad. La privacidad trata sobre la determinación de cada persona a la hora de decidir qué información sobre ella suministra y con qué propósito. La seguridad se centra en la confianza de que esas decisiones sean respetadas, por ejemplo, mediante la correcta protección de los datos personales almacenados.

Evaluación

Para reforzar los contenidos aprendidos, piensa si son verdaderas o falsas las siguientes afirmaciones:

Una persona puede solicitar que su nombre y datos personales desaparezcan de los resultados de una búsqueda en Internet.	*verdadero*	*falso*
Solamente son suplantadas las personas famosas e influyentes.	*verdadero*	*falso*
La ley de protección de datos de carácter personal no se aplica en las redes sociales.	*verdadero*	*falso*
Utilizar distintos perfiles en las redes te permite separar las cuestiones personales y profesionales.	*verdadero*	*falso*
Es sencillo eliminar el rastro que dejamos en la Red.	*verdadero*	*falso*

Identidad digital, reputación y privacidad on-line

Palabras Clave

Referencias

[1]La Brigada de Investigación Tecnológica está encuadrada en la Unidad de Delincuencia Económica y Fiscal (UDEF) que es el órgano de la Dirección General de la Policía y de la Guardia Civil encargado de la investigación y persecución de las actividades delictivas, de ámbito nacional e internacional, en materia de delincuencia económica y fiscal, así como la coordinación operativa y apoyo técnico a las respectivas Unidades Territoriales.

- Brigada de Investigación Tecnológica de la Policía Nacional: http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html
- Grupo de Delitos Telemáticos de la Guardia Civil: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

[2] Pérez San-José, Pablo. (Dir.) (2012) *"Guía para usuarios: identidad digital y reputación on line"*. INTECO.
Disponible en: http://www.inteco.es/CERT/guias_estudios/guias/Guia_Identidad_Reputacion_usuarios
[Consultado 06/07/2014]

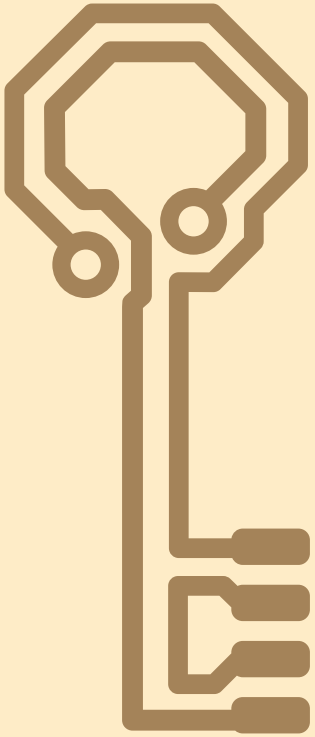
Contraseñas

Actividades didácticas

Objetivos generales

Al acabar las actividades, las participantes serán capaces de:

- Verificar si sus contraseñas cumplen con las recomendaciones mínimas de seguridad.
- Hacer uso de las técnicas necesarias para crear contraseñas seguras en los servicios y dispositivos.



¿Dónde sucede?

Correo electrónico | Redes sociales | Juegos en línea | Redes P2P | Mensajería instantánea | Dispositivos de almacenamiento externo

1 Actividad
La información que es importante para mi

2 Actividad
Ser o no ser, esa es la cuestión

MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
SECRETARÍA DE ESTADO DE SERVICIOS SOCIALES E IGUALDAD
INSTITUTO DE LA MUJER Y PARA LA IGUALDAD DE OPORTUNIDADES
Unión Europea
Fondo Social Europeo

La información que es importante para mi

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Reconocer los riesgos que van asociados al robo de contraseñas personales.
- Tomar conciencia de la importancia de crear contraseñas seguras para resguardar nuestra información.

1
Actividad

Recursos y materiales


PC


Papel


4 tarjetas en blanco


Bolígrafos

Tiempo

25 min.

La información que es importante para mi

1
Actividad

Desarrollo

1. Cada participante deberá coger 4 tarjetas (o un folio y dividirlo en 4 partes).
2. En cada tarjeta escribirá una frase importante para ella, sin que la vean las demás. Por ejemplo, escribirán frases como: "la clave de mi tarjeta de crédito"; "mi contraseña de correo"; "la receta de tarta de manzana de mi abuela"; "la clave de la nube donde guardo mis fotos"; "la contraseña de mi móvil". Previamente, el equipo facilitador deberá dejar claro que en ningún caso deberán citar sus claves reales, sino simplemente escribir textualmente frases que hagan referencia a información importante como aparece en el ejemplo.
3. Cuando estén escritas, las doblarán y dejarán en el suelo cerca de ellas.
4. Posteriormente, el equipo facilitador dará 1 minuto de tiempo de reloj, para que cada participante escriba en un folio una contraseña para el juego y su nombre de pila para saber después a qué participante corresponde cada una.
5. Cuando hayan terminado, el equipo facilitador recogerá todas las contraseñas y mientras una de las facilitadoras comprueba la seguridad de las mismas en: **https://www.microsoft.com/es-es/security/pc-security/password-checker.aspx** (o cualquier otro comprobador de contraseñas) la otra facilitadora iniciará un debate grupal hasta que su compañera haya finalizado sobre la siguiente noticia:

Recuerda que

- Las contraseñas son la llave de entrada que te permite acceder a diferentes servicios y dispositivos como la cuenta de correo o el teléfono móvil.
- La seguridad de tu información en la Red dependerá en gran medida del tipo de contraseña que utilices por lo que debes tener especial cuidado en seguir las recomendaciones establecidas para construir una que sea segura.
- Tómate tu tiempo a la hora de crear una nueva contraseña, y ten en cuenta que es la llave de acceso a tu información personal y confidencial.

La información que es importante para mi

1
Actividad

Desarrollo

BASADO EN NOTICIA DE PRENSA “LAS CONTRASEÑAS MÁS UTILIZADAS Y FÁCILES DE DESCIFRAR EN INTERNET DURANTE EL 2013”

¿Qué contraseña utiliza en Internet? Si es "password" o "123456" lo mejor será que la cambie, pues es una de las claves más utilizadas por internautas y más fáciles de averiguar según una lista anual de las peores contraseñas en la red.

La lista incluye las 25 contraseñas más comunes encontradas en la Red y, por tanto, las que son más fáciles de piratear. La contraseña "123456" ese año fue clasificada como la peor.

Entre los diez primeros puestos de la lista aparecen también 12345678, 123456789, 111111 y 1234567.

También aparecen en estos diez puestos: abc123 o, iloveyou.

De entre las 25 contraseñas también destacan aquellas que utilizan palabras relacionadas con Adobe y sus programas, quizá conectado con las importantes brechas de seguridad que sufrió todo el entorno de Adobe durante el 2012."Photoshop", o "adobe123", son claras muestras de que es muy importante no utilizar como contraseña el mismo nombre del sitio web o aplicación a la que se está accediendo.

Las 25 contraseñas, por orden de uso son las siguientes:

123456; password; 12345678; qwerty; abc123; 123456789; 111111; 1234567; iloveyou; adobe123; 123123; Admin; 1234567890; letmein; photoshop; 1234; monkey; shadow; sunshine; 12345; passwordl; princess; azerty; trustnol; 000000

La información que es importante para mi

1
Actividad

Desarrollo

6. La facilitadora que esté comprobando las contraseñas, apuntará el resultado de cada una de ellas, de tal manera que si es BAJA le quitará a la participante todas sus tarjetas; si es REGULAR le quitará 3; si es MEDIA le quitará 2; si es ALTA le quitará 1; y si es MUY ALTA no le quitará ninguna.
7. Cuando todas las participantes hayan "sufrido" las consecuencia del bajo nivel de sus contraseñas se debatirá en plenario qué ha pasado, cómo se sienten las participantes que han perdido información y qué podrían haber hecho para conservarla.

Ser o no ser, esa es la cuestión

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Comprobar de manera inmediata el grado de seguridad y robustez que tienen las contraseñas creadas.
- Aprender a crear y administrar contraseñas seguras.

2 Actividad

Recursos y materiales


PC


Papel


Boligrafos

Tiempo

20 min.

Ser o no ser, esa es la cuestión

2
Actividad

Desarrollo

1. Se trabajará en grupos de 3 mujeres como máximo y cada grupo elegirá una relatora.
2. Después, cada participante de manera individual, deberá pensar y escribir en un folio 3 contraseñas que considere seguras. Puesto que es una dinámica de aprendizaje, no utilizarán sus contraseñas reales sino inventadas.
3. Posteriormente, irán comprobando la seguridad de las contraseñas en cualquiera de estos comprobadores de contraseñas. Se recomienda al equipo facilitador que seleccione una de ellas previamente con el fin de elegir la más adecuada en función del perfil de cada grupo de participantes, y el tiempo disponible para llevar a cabo la dinámica.:
    a) http://password.social-kaspersky.com
    b) https://www.microsoft.com/es-es/security/pc-security/password-checker.aspx
    c) http://password.es/comprobador/
4. Cuando todas las participantes hayan comprobado sus contraseñas, cada relatora compartirá en plenario tanto las que han resultado más inseguras como las que han resultado más seguras.
5. El equipo facilitador deberá insistir en la necesidad de construir contraseñas seguras explicando que cada persona usuaria de Internet utiliza una media de cinco servicios diferentes con sus contraseñas, y que aunque tener una distinta para cada aplicación resulta a veces complicado, utilizar siempre la misma puede poner en riesgo nuestra información, ya que existen múltiples programas diseñados para averiguarlas, y hackers especialistas en hacerlo[1]. Cuanto más corta y sencilla es nuestra contraseña, menos tiempo tardarán en descubrirla. Además, si no la cambias con cierta frecuencia, en caso de que algún servicio web sea hackeado y robadas sus bases de datos, quienes "hackean" dispondrá de tu nombre de usuaria y contraseña. A parte, al utilizar la opción de "pregunta de seguridad" para recuperar las contraseñas, es aconsejable poner respuestas que incluyan algún código que te inventes y solo conozcas tu (algo que luego puedas recordar), ya que las preguntas suelen ir dirigidas a aspectos de la vida cotidiana, y alguien que te conozca podría averiguarla fácilmente.

Recuerda que

- Puedes utilizar comprobadores de seguridad de contraseñas antes de decidirte por la definitiva, de esa manera podrás confirmar que has hecho una elección segura y mantendrás tu información a buen recaudo.
- Cuando utilices la opción de "pregunta de seguridad" para recuperar tus contraseñas, es importante que pongas respuestas falsas o sólo conocidas por ti, ya que las preguntas suelen ir dirigidas a aspectos de la vida cotidiana, y alguien que te conozca mínimamente podría averiguarla sin muchos problemas.
- Algunos ejemplos de gestores de contraseñas son: Password Memory 5; Passpack; Keeper Password & Data Vault; LastPass Manager; KeePassX.

Contraseñas

Consejos y buenas prácticas

Para evitar que otras personas accedan a nuestra información, haremos lo siguiente[2]:

- NO pondremos la misma contraseña en distintas cuentas como redes sociales, correo electrónico, banca on-line, etc.
- NO permitiremos que queden almacenadas en los navegadores. Es más seguro escribir la contraseña cada vez.
- NO utilizaremos palabras sencillas, nombres propios o lugares: "María José".
- NO utilizaremos palabras completas que aparecen en el diccionario, independientemente del idioma (a menos que combines mayúsculas y minúsculas).
- NO utilizaremos fechas señaladas como cumpleaños, aniversarios, nacimientos, etc.: "15-02-1976".
- NO combinaremos palabras sencillas con fechas señaladas: "Leonor230552".
- NO pondremos números consecutivos: "123456".
- NO pondremos letras consecutivas del teclado (qwerty): "asdfg".
- NO pondremos nuestro número de teléfono móvil o fijo.

Contraseñas

Datos de interés[3]

Las contraseñas son la llave de entrada para acceder a nuestros diferentes servicios y dispositivos.

Siguiendo las recomendaciones de Windows, para que una contraseña sea segura, ésta ha de cumplir una serie de recomendaciones que nos ayudarán a proteger nuestra información. Deberemos pensar en contraseñas imaginativas y personales que además sean:

- **Secretas:** No le digas a nadie tus contraseñas, ni las escribas en papeles o libretas que estén a la vista. Tampoco las guardes en un archivo de tu ordenador, y menos con el nombre "contraseñas".
- **Robustas:** Con ocho caracteres como mínimo, incluyendo letras mayúsculas, minúsculas, números y símbolos. A mayor longitud y combinaciones, mayor seguridad: aLuCiNaNte%55.
- **No las repitas:** Procura tener una contraseña para cada cosa. Hay trucos para crearlas que explicamos más abajo.
- **Cámbialas de vez en cuando:** Es aconsejable variar de contraseña cada cierto tiempo.

Un **generador aleatorio de contraseñas** es una aplicación que te permite tener contraseñas complejas, diferentes y seguras, con sólo recordar la clave de acceso al gestor, conocida como "contraseña maestra". Muchas de las empresas que comercializan antivirus cuentan con estas aplicaciones, ya que también pueden defendernos de la suplantación de identidad (phishing), porque para la ciberdelincuencia será más difícil acceder a nuestras cuentas de correo electrónico o aplicaciones y hacerse pasar por nosotras. Para utilizar un "gestor de contraseñas" deberíamos tener en cuenta lo siguiente:

- Utiliza una clave de acceso al gestor segura y robusta (contraseña maestra).
- Realiza copias de seguridad del fichero de claves.
- Perderás el acceso a tus contraseñas si olvidas la clave "contraseña maestra" de acceso al gestor.
- Revisa antes tu equipo y asegúrate de que no tenga ningún virus o malware que pueda robar tus contraseñas.

Trucos para construir buenas contraseñas

- Cambia las vocales por números, por ejemplo, siendo que: a=1, e=2, i=3, o=4, u=5
  - Guitarra: G53t1rr1

  Puedes complicarlo cuanto quieras: Sólo números pares, empezar por el número de tu cumpleaños, etc.
- Utiliza el mismo patrón para recordarlo, y añade por ejemplo el número que caracteres tiene el nombre del servicio:
  - FACEBOOK: 8G53t1rr1 / Foro Motera: 10G53t1rr1
- Utiliza reglas mnemotécnicas, como elegir la primera letra de cada palabras de una frase:
  - No hay mal que 100 años dure: Nhmq100ad

Contraseñas

Evaluación

Para reforzar los contenidos aprendidos, piensa si son verdaderas o falsas las siguientes afirmaciones:

Una contraseña es robusta cuando tiene más de 8 caracteres	*verdadero*	*falso*
Si cambias la contraseña cada 6 meses estarás asegurando tu información ante posibles ataques informáticos	*verdadero*	*falso*
Es más seguro utilizar siempre la misma contraseña para que no se te olvide y evitar así bloquear tus cuentas	*verdadero*	*falso*
Los "gestores de contraseñas" aumentan la seguridad de nuestras claves	*verdadero*	*falso*
La fecha de cumpleaños de mi abuela es una buena contraseña, ya que ninguna de las personas que conozco tiene esa información	*verdadero*	*falso*

Contraseñas

Palabras Clave

contraseña
encriptación
qwerty
password
hacker
robusta
cifrado
phishing
gestor
de
maestra
login

Referencias

[1] Kapersky Lab (2012) *"¿Sabes cuánto tarda un hacker en descifrar tus contraseñas?"*. Publicaciones de Prensa.
Disponible en: http://goo.gl/84Yu8O
[Consultado 06/07/2014]

[2] Información elaborada a partir de contenidos web:
Oficina de Seguridad del Internauta, *"Contraseñas"*.
Disponible en: http://www.osi.es/contrasenas
[Consultado 06/07/2014]

Panda Security, (2014) *"Cómo crear contraseñas seguras"*.
Disponible en: http://goo.gl/7B01Ur
[Consultado 06/07/2014]

[3] *Ibid.*

Materiales didácticos **"Confianza y seguridad de las mujeres en la Red"**

Ciberacoso

Actividades didácticas

Objetivos generales

Al acabar las actividades, las participantes serán capaces de:

- Identificar situaciones de ciberacoso.
- Reconocer el ciberacoso como una práctica perjudicial para las personas que lo sufren.
- Conocer los pasos a seguir en caso de que seas ciberacosada.

¿Dónde sucede?

Correo electrónico

Redes sociales

Juegos en línea

Mensajería instantánea

1 Actividad
Ciberacoso

2 Actividad
Redactando una nota de prensa breve

MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
SECRETARÍA DE ESTADO DE SERVICIOS SOCIALES E IGUALDAD
INSTITUTO DE LA MUJER Y PARA LA IGUALDAD DE OPORTUNIDADES
Unión Europea
Fondo Social Europeo

Ciberacoso

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Identificar los diferentes ámbitos donde suelen darse situaciones de ciberacoso.
- Reconocer las características y tipos de estrategias que utilizan las personas que ciberacosan en cada ámbito.

1
Actividad

Recursos y materiales


Bolígrafos


Papel

Tiempo

20 min.

Ciberacoso

1
Actividad

Desarrollo

1. Se trabajará en grupos de 5 mujeres y cada grupo elegirá una relatora.

2. Cada grupo tendrá que idear al menos 2 pequeñas historias de ciberacoso diferentes, especificando el ámbito, la víctima, el medio electrónico por el que se ejecuta, la frecuencia, el contenido y las consecuencias del mismo. El equipo facilitador aclarará que las historias serán inventadas y pueden referirse a diferentes ámbitos y personajes, (en la vivienda, en el trabajo, en la escuela, alguien de la comunidad, jefes, familiares, de carácter sexual o no, etc.)

3. Una vez finalizado el trabajo grupal, cada relatora pondrá en común los resultados en plenario.

4. Para concluir la actividad, el equipo facilitador sistematizará las estrategias más comunes de quienes ciberacosan, incluyendo las que no hayan salido en los grupos[1]. :

- Distribuir en Internet una imagen comprometida de contenido sexual (real o trucada), o datos susceptibles de perjudicar a la víctima.
- Dar de alta a la víctima en un sitio Web donde se la puede ridiculizar, humillar, estigmatizar. Por ejemplo, donde se escoge a la persona más tonta, más fea, etc.
- Crear un perfil o espacio falso en nombre de la víctima en el que ésta comparte intimidades, realiza demandas y ofertas sexuales explícitas, etc.
- Usurpar la identidad de la víctima y, en su nombre, hacer comentarios ofensivos o participaciones inoportunas en chats de tal modo que despierte reacciones adversas hacia quien en realidad es la víctima.

Recuerda que

- El ciberacoso es el acto por el cual se amenaza, hostiga y humilla a una persona a través de diferentes medios de comunicación digital -como el correo electrónico, mensajería instantánea, redes sociales, blogs- de forma repetitiva y recurrente con la finalidad de dañar su dignidad y autoestima.
- Los ámbitos y tipos en los que se puede dar el acoso son amplios, así por ejemplo, puede ser: escolar, sexual, laboral, inmobiliario, familiar, académico, profesional, etc.
- Las víctimas de 'ciberacoso', como las de acoso no virtual, pueden sufrir problemas de estrés, sentimientos de humillación, ansiedad, depresión, ira, impotencia, fatiga, enfermedad física, pérdida de confianza en sí mismas, pudiendo incluso derivar en suicidio.

Ciberacoso

1
Actividad

Desarrollo

- En la misma línea, provocar en la víctima el sentimiento de estar siendo vigilada e inducir a que reaccione de forma inadecuada o desproporcionada y se vea excluida (o auto excluida) del chat, comunidad virtual etc. en la que estaba participando.
- Con frecuencia los ciberacosadores engañan a las víctimas haciéndose pasar por una amistad o persona conocida concertando un encuentro digital para llevar a cabo sus fines.
- Divulgar por Internet grabaciones con móviles o cámara digital en las que se intimida, pega, agrede, persigue, etc. a una persona. El agresor se complace no sólo del acoso cometido sino también de inmortalizarlo, convertirlo en objeto de burla y obtener reconocimiento por ello. Algo que se incrementa cuando los medios de comunicación se hacen eco de ello.
- Dar de alta en determinados sitios web la dirección de correo electrónico de la persona acosada para convertirla en blanco de Spam, contactos con desconocidos, etc.
- Hacer correr falsos rumores sobre un comportamiento reprochable atribuido a la víctima, de tal modo que quienes lo lean reaccionen y tomen represalias en contra de la misma.
- Enviar mensajes ofensivos y hostigadores a través de e-mail, SMS, servicios de mensajería instantánea o redes sociales.
- Perseguir e incomodar a la persona acosada en los espacios de Internet que frecuenta.
- Realizar comunicaciones a través de diferentes medios digitales: silenciosas; con amenazas; con insultos; de contenido sexual; colgando o desconectando cuando se responde; en horas inoportunas, etc.

Redactando una noticia de prensa

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Conocer los elementos que caracterizan el ciberacoso.

2
Actividad

Recursos y materiales


PC


PIZARRA


Bolígrafos


Papel

Tiempo

20 min.

Redactando una noticia de prensa

2
Actividad

Desarrollo

1. Se trabajará en grupos de 5 mujeres y cada grupo elegirá una relatora.
2. Cada grupo tendrá que trabajar en uno de los ámbitos y tipos de ciberacoso que haya salido en la actividad 1 (escolar, laboral, sexual, inmobiliario, etc.)
3. Se explicará a las participantes que son periodistas de un periódico de tirada nacional y que tienen que redactar una nota breve sobre los elementos que caracterizan el tipo de ciberacoso que les hayan encargado. Para ello deberán encontrar información en Internet sobre casos reales e identificar qué elementos son fundamentales en el caso seleccionado.
4. Una vez finalizado el trabajo, las relatoras leerán uno de los casos reales encontrados en Internet y la nota redactada por su grupo.
5. El equipo facilitador preguntará a las participantes si han encontrado más casos de víctimas mujeres que de hombres.
6. Para cerrar la dinámica, el equipo facilitador recordará que las características del ciberacoso son:

- Intromisión constante en la vida privada de una persona utilizando los medios digitales.
- Se realiza de forma repetitiva.
- Se realiza en contra de la voluntad de la víctima e incluye amenazas constantes de diferente naturaleza.
- Las amenazas vertidas en la Red, se vayan a materializar o no, generan ansiedad y temor.
- Se puede llegar a suplantar la identidad de la víctima o incluso usurparle sus datos personales para chantajearla.
- El poder de distribución de la información es una amenaza para la víctima y una herramienta de dominación de quien ciberacosa.
- En ocasiones se dañan los equipos de las víctimas y la información que ellos contienen.
- No necesita la proximidad física con la víctima.

Recuerda que

- Las redes sociales son una importante fuente de información para quienes ciberacosan, por lo tanto valora qué datos personales compartes.
- El ciberacoso puede ser muy traumático debido a la amenaza de difusión o a la difusión de la información nociva para la victima a través de Internet con gran rapidez.

Ciberacoso

Consejos y buenas prácticas

- Recuerda que cuanta más información personal hagas pública en Internet, más vulnerable serás ante el ciberacoso.
- Para proteger tu seguridad en Internet utiliza dos cuentas de correo electrónico: una profesional y otra personal.
- Utiliza contraseñas robustas y recuerda no compartirlas con nadie, ya que son tu DNI en Internet.

Qué hacer en el caso de ser víctima de ciberaco

- Pide ayuda a tu círculo familiar y de amistades, haciéndoles saber que eviten publicar datos personales sobre ti.
- Para evitar que la persona que te ciberacosa acceda a tus equipos informáticos, mantén tu antivirus actualizado y modifica tus contraseñas con periodicidad.
- Si por tu situación personal o profesional, puedes correr el riesgo de ser ciberacosada, es aconsejable cambiar tu nombre real en las redes sociales por un alias o nickname para evitar ser localizada por personas desconocidas.
- Bloquea y filtra los mensajes de quien te ciberacosa. Muchos de los servicios de correos y blogs disponen de sistemas para habilitar este tipo de filtros.
- En el caso de ser ciberacosada a través del correo electrónico, puedes pedir al proveedor del sitio web que elimine la cuenta desde la cual estás recibiendo el acoso. Puedes notificarlo por medio de un correo electrónico adjuntando los correos que has recibido.
- Si te están ciberacosando a través de alguna red social, puedes reportar dicho abuso al proveedor del sitio web.
- Evita responder a las provocaciones de quien te ciberacosa. Recopila y guarda todas las pruebas para una posible denunciar posterior.
- Ponte en contacto[2] con las autoridades a través de la Policía Nacional (Brigada de Investigación Tecnológica) o Guardia Civil (Grupo de Delitos Telemáticos) y formula la denuncia.

Ciberacoso

Datos de interés

Cibercoso: Acto por el cual se amenaza, hostiga y humilla a una persona a través de diferentes medios de comunicación digital

En el ciberacoso aunque tanto hombres como mujeres pueden ser víctimas, el porcentaje de víctimas femeninas es siempre mayor que las masculinas[3]. Por otra parte, el ciberacoso es otra manera de ejercer la violencia contra las mujeres y en el caso del ciberacoso sexual la mayoría de quienes lo sufren son menores y mujeres.

Según un estudio, el 52% de las víctimas de ciberacoso en Estados Unidos tenían entre 18 y 29 años, y no identificaban dichos comportamientos como actos de ciberacoso[4].

Evaluación

Para reforzar los contenidos aprendidos, piensa si son verdaderas o falsas las siguientes afirmaciones:

El ciberacoso es menos dañino que el acoso en el mundo físico	*verdadero*	*falso*
Una característica del ciberacoso es la frecuencia repetitiva de las amenazas	*verdadero*	*falso*
Las personas que ciberacosan no buscan información de la víctima en las redes sociales	*verdadero*	*falso*
Cuanta más información personal compartas en Internet, más vulnerable eres ante un ciberacoso	*verdadero*	*falso*
El ciberacoso puede darse en múltiples ámbitos como el escolar, laboral, sexual, inmobiliario o familiar	*verdadero*	*falso*

Ciberacoso

Palabras Clave

amenazas
redes
humillación
ciberacoso
provocaciones
sociales
intimidación
abuso
víctima
laboral
acoso
psicológico
comunicación
escolar
digital
vulnerabilidad
inmobiliario
bullying
mobbing
hostigamiento
sexual
familiar

Referencias

[1] Torres Albero, Cristóbal (Dir.), Robles, José Manuel y de Marco, Stefano (2013) *"El ciberacoso como forma de ejercer la violencia de género en la juventud: un riesgo en la sociedad de la información y del conocimiento".* Madrid. Servicio de Publicaciones del Ministerio de Sanidad, Servicios Sociales e Igualdad. Delegación del Gobierno para la Violencia de Género.
Disponible en: http://www.msssi.gob.es/ssi/violenciaGenero/publicaciones/estudiosinvestigaciones/PDFS/El_Ciberacos_Juvent.pdf

[2] La Brigada de Investigación Tecnológica está encuadrada en la Unidad de Delincuencia Económica y Fiscal (UDEF) que es el órgano de la Dirección General de la Policía y de la Guardia Civil encargado de la investigación y persecución de las actividades delictivas, de ámbito nacional e internacional, en materia de delincuencia económica y fiscal, así como la coordinación operativa y apoyo técnico a las respectivas Unidades Territoriales.

- Brigada de Investigación Tecnológica de la Policía Nacional: http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html
- Grupo de Delitos Telemáticos de la Guardia Civil: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

[3] Torres Albero, Cristóbal (Dir.), Robles, José Manuel y de Marco, Stefano (2013) *"El ciberacoso como forma de ejercer la violencia de género en la juventud: un riesgo en la sociedad de la información y del conocimiento".* Madrid. Servicio de Publicaciones del Ministerio de Sanidad, Servicios Sociales e Igualdad. Delegación del Gobierno para la Violencia de Género.
Disponible en: http://www.msssi.gob.es/ssi/violenciaGenero/publicaciones/estudiosinvestigaciones/PDFS/El_Ciberacos_Juvent.pdf

[4] Tjaden, P. y Thoennes, N. (1998). *Stalking in America: Findings from the national survey against women violence. W*ashington, DC: National Institute of Justice, Centers for Disease Control and Prevention. Citado en Torres Albero, Cristóbal (Dir.), Robles, José Manuel y de Marco, Stefano (2013) *"El ciberacoso como forma de ejercer la violencia de género en la juventud: un riesgo en la sociedad de la información y del conocimiento"*, página 21, Madrid. Servicio de Publicaciones del Ministerio de Sanidad, Servicios Sociales e Igualdad. Delegación del Gobierno para la Violencia de Género.
Disponible en: http://www.msssi.gob.es/ssi/violenciaGenero/publicaciones/estudiosinvestigaciones/PDFS/El_Ciberacos_Juvent.pdf

Materiales didácticos **"Confianza y seguridad de las mujeres en la Red"**

Sexting

Actividades didácticas

Objetivos generales

Al acabar las actividades, las participantes serán capaces de:

- Reconocer los comportamientos de riesgo asociados a compartir vídeos y fotos a través del móvil con terceras personas.
- Identificar medidas preventivas que ayuden a disminuir los riesgos en el uso de la práctica de sexting.

¿Dónde sucede?

Correo electrónico

Redes sociales

Juegos en línea

Mensajería instantánea

1 Actividad
Chantaje por despecho

2 Actividad
Prueba de amor: te entrego mis fotos

3 Actividad
Prensa y sexting

MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
SECRETARÍA DE ESTADO DE SERVICIOS SOCIALES E IGUALDAD
INSTITUTO DE LA MUJER Y PARA LA IGUALDAD DE OPORTUNIDADES
Unión Europea
Fondo Social Europeo

Chantaje por despecho

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Reconocer que la práctica de sexting puede conllevar riesgos de sufrir acoso en la Red.
- Construir pautas de autocuidado para las mujeres que practican sexting utilizando la webcam.
- Tomar conciencia de la necesidad de pedir ayuda ante las consecuencias negativas del sexting.

1
Actividad

Recursos y materiales


Rotuladores de colores


Papel


PC


Proyector


Papel continuo/cartulinas

Tiempo

20 min.

Chantaje por despecho

1
Actividad

Desarrollo

1. El equipo facilitador leerá el siguiente caso:

CASO BASADO EN UNA HISTORIA REAL

Marta de 36 años, tuvo una relación de pareja durante 4 años con Jorge. En ocasiones, Marta le enviaba fotos y videos eróticos personales como parte de los juegos sexuales que llevaban a cabo, y ambos disfrutaban con esa práctica. Marta decidió terminar la relación, y Jorge, despechado, comenzó a distribuir las fotografías y vídeos de su exnovia a través de las redes, consiguiendo un gran número de visitas en pocas horas.

2. Una vez expuesto el caso, se trabajará en grupos de 5 mujeres como máximo y cada grupo elegirá una relatora.

3. Cada grupo tendrá que construir un mural contestando a las siguientes preguntas:
   a) ¿A qué riesgos te expones si practicas sexting?
   b) ¿Cómo puedes perder el control del contenido que produces cuando haces sexting?
   c) ¿Qué medidas puedes tomar en el caso de que pierdas el control sobre tus imágenes o videos?

4. Al finalizar, se colgarán los murales por el aula, y cada relatora expondrá en plenario los resultados para hacer un debate conjunto.

Chantaje por despecho

1
Actividad

Recuerda que

- El sexting es una práctica que consiste en el envío de imágenes o videos de contenido íntimo, a través del móvil y de forma voluntaria.
- Quienes reciben estas fotografías o vídeos, normalmente son del entorno conocido y de confianza, parejas y personas a las que gustar, con las que ligar o flirtear. En algunos casos, este envío supone una prueba de amor, pero esto cambia en el momento en el que se termina la relación, ya que muchas veces este tipo de materiales acaban en las redes sociales fuera de nuestro control, pudiendo sufrir incluso situaciones de ciberacoso.
- Existen numerosas webs dedicadas a la pornografía cuyo contenido se nutre en parte de fotos y vídeos, creados de forma amateur por parejas que se graban inicialmente de forma voluntaria y privada. Cuando la pareja se rompe, en la mayoría de estos casos son ellos, quienes por despecho y venganza, facilitan este tipo de materiales a dichos portales webs.
- Cualquier mujer, independientemente de su edad, y de la duración de la relación (parejas estables o puntuales) puede ser víctima de las consecuencias negativas de la práctica del sexting.
- Los contenidos caseros, anónimos y de carácter sexual se difunden de manera viral, es decir, con mucha rapidez y exponencialmente.
- En el caso de que pierdas el control sobre tus imágenes o videos, puedes solicitar a los buscadores la retirada de los resultados de búsqueda que hagan referencia a esas imágenes o videos. Además algunas webs permiten escribirles para solicitar la retirada de material que viole la intimidad de terceros.

Prueba de amor: te entrego mis fotos

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Tomar conciencia de la facilidad y rapidez con que nuestras fotografías pueden difundirse en la Red.
- Reflexionar sobre cómo influyen las TIC en las maneras de relacionarnos socialmente y con las parejas.

2
Actividad

Recursos y materiales

Rotuladores de colores

Papel continuo/cartulinas

Tiempo

25 min.

Redactando una noticia de prensa

2
Actividad

Desarrollo

1. Se llevará a cabo una teatralización, para lo cual, el equipo facilitador pedirá cinco voluntarias para hacer los papeles de: una chica adolescente; un chico adolescente y tres amigos del chico. La chica y el chico tienen una relación de pareja desde hace 2 semanas y van al mismo instituto (las edades y el lugar de estudios o trabajo pueden variar en función del grupo de participantes).
2. Las voluntarias tendrán que interpretar el papel descrito en el siguiente guion, entregándose copia del **guion** a cada personaje:

Chica

Simula que se hace unas fotos insinuantes, sexys, porque quiere gustar a su pareja, y como prueba de amor le pone un Whatsapp, avisándole de que le quiere hacer un regalo. Como no recibe respuesta se inquieta, y dice "le voy a mandar una foto "medio desnuda" y simula que la manda escribiendo "soy toda tuya" "¿dónde estás?"

.

Chico

Está con los amigos del baloncesto y apenas presta atención al móvil. Cuando ha pasado un rato, coge el teléfono y ve una foto de la chica medio desnuda, no lee el mensaje, se sorprende y le dice a sus amigos: "¡mirad qué buena está mi novia!". Aunque se lo piensa dos veces, acepta compartirla con ellos por la presión del grupo, pero les pide que no se la pasen a nadie más.

3 Amigos del chico

Están con el chico ven la foto, se ríen y se la piden: "¡vamos, vamos que rule!"

La **facilitadora** explicará que unos días después la foto se cuelga en una red social del instituto.

Recuerda que

- Esta práctica puede llevarte a la exposición pública de tu intimidad y a sufrir situaciones de acoso, chantaje, sentimientos de humillación, pérdida de autoestima, aislamiento u otros problemas psicológicos, y en caso de menores, a ser objetivo de pederastas, multiplicándose el riesgo si la imagen va asociada con datos personales.
- Antes de hacerte una foto o un vídeo de contenido erótico y enviársela a terceras personas, piensa en las consecuencias que puede tener hacia ti. Tienes que ser consciente de que una vez que la foto ha sido enviada, no puedes hacer nada. Si la foto se carga correctamente, no se puede cancelar o rectificar, es irreversible.
- La facilidad y la rapidez con la que pueden ser difundidas las fotos o vídeos que envías, supone una pérdida de privacidad y de control de los contenidos íntimos enviados.
- Si decides hacer esta práctica, puedes optar por que no se te pueda identificar en las imágenes y así evitar riesgos futuros.

Redactando una noticia de prensa

2
Actividad

Desarrollo

3. Después de la teatralización el equipo facilitador preguntará:
    a) ¿Cómo os parece la actuación de la chica? y ¿el comportamiento del chico y sus amigos?
    b) ¿Creéis que es frecuente este tipo de actuaciones? ¿por qué?
    c) ¿Pensáis que si el chico hubiera estado sólo, sin sus amigos hubiera compartido la foto de ella?
    d) ¿Cómo acaba la historia?

4. Si no sale del grupo, el equipo facilitador leerá el final de la historia: "la chica no volvió a tener noticias del que consideraba su novio, y terminó cambiando su aspecto físico y marchándose a otra ciudad al descubrir que su foto había circulado por la red social del instituto. El chico siguió con su vida normal como si nada hubiera pasado".

5. Basándonos en las conclusiones del grupo se hará una reflexión sobre los mitos del amor romántico y los mandatos de género.

6. Posteriormente se hará una lluvia de ideas sobre:
    a) ¿Cómo se podrían haber evitado los riesgos? ¿conocía la chica las consecuencias de esta práctica?
    b) ¿Tienen influencia las madres y padres, o los y las educadoras en este tipo de situaciones?

7. Para ilustrar la dinámica, se proyectará en el aula algunos ejemplos de casos basados en hechos reales:

Redactando una noticia de prensa

2
Actividad

Desarrollo

CASO 1 BASADO EN HECHOS REALES

Una mujer envió a su novio una foto suya desnuda. Él la utilizó como su foto de perfil en WhatsApp, de forma que todo el mundo con quien se intercambiaba mensajes podía verla.

CASO 2 BASADO EN HECHOS REALES

Un profesor de secundaria descubrió que dos chicas habían sido grabadas en vídeo por sus novios realizando actos sexuales con ellos, y que dichos vídeos habían estado circulando por el instituto.

CASO 3 BASADO EN HECHOS REALES

Elisa envió fotos desnuda a su novio, quien las compartió con algunos de sus mejores amigos para presumir. Uno de estos amigos las publicó inmediatamente en una red social específica de imágenes.

Prensa y sexting

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Identificar las diferencias en la práctica del sexting realizada por mujeres o por hombres.

3
Actividad

Recursos y materiales

PC

Tiempo

15 min.

Prensa y sexting

3
Actividad

Desarrollo

1. Se formarán grupos de 5 mujeres y cada grupo elegirá una relatora.
2. Cada grupo tendrá que buscar en Internet ejemplos de mujeres y hombres que hayan sufrido las consecuencias de haber realizado sexting.
3. Una vez finalizado el trabajo grupal, cada relatora pondrá en común los resultados en plenario (al menos habrán tenido que encontrar cuatro casos, dos de mujeres y dos de hombres).
4. Después se debatirá en plenario si existen o no diferencias entre ellas y ellos en este tipo de prácticas y sus consecuencias.

Recuerda que

- Si decides hacerte fotos, grabar, enviar o almacenar imágenes de contenido íntimo o sexual, has de saber que puedes correr el riesgo de ser víctima de violencia de género en la Red (ciberacoso, sextorsión).
- Los roles y estereotipos de género se reproducen en la Red, haciendo que los hombres que practican sexting se conviertan en "don juanes", mientras que las mujeres pasan a ser juzgadas y estigmatizadas.

Sexting

Consejos y buenas prácticas

- Piensa qué tipo de imágenes personales vas a enviar, ya que una vez enviadas se escaparan de tu control y no podrán ser recuperadas, especialmente si se reproducen de manera víri ca.
- Los círculos de amistades y las relaciones personales cambian, así que piensa bien a quien decides enviar tus fotos.
- Controla los soportes de almacenamiento donde guardas tus fotos y vídeos, ya que pueden ser sustraídos por otras personas sin tu consentimiento.
- Procura no utilizar WIFIs abiertas, ya que tus datos serán más vulnerables al robo.
- Cuida el tipo de imágenes que subes a las redes sociales, ya que si algunas son comprometedoras, podrían afectarte en un futuro tanto en lo personal como en lo profesional.
- No contribuyas a difundir fotos que recibes en cadena ya que esto te hace cómplice. Si recibes imágenes de este tipo y conoces el origen delictivo debes denunciarlo.
- Es recomendable proteger tus dispositivos o almacenamiento en la nube, mediante contraseñas robustas, ya que en caso de robo o pérdida, será más complicado acceder a tu información personal.
- Si decides hacer esta práctica, no subas a la Red imágenes que puedan identificarte y así evitas riesgos futuros.
- Si hay menores en la unidad familiar, intenta que la webcam esté en un lugar común para evitar posibles situaciones de riesgo.
- Si utilizas un ordenador portátil con webcam, procura tapar la webcam cuando no la estés utilizando.

Consejos y buenas prácticas

Consejos si te están acosando por haber practicado sexting

- Pide ayuda a tu círculo familiar, de amistades y/o educativo, ya que la vulneración de tu intimidad puede haberte provocado gran sufrimiento y angustia.
- No accedas a las peticiones y chantajes de quienes te quieran acosar, chantajear o amenazar, tienes que saber que estas acciones son un delito grave y que la ley puede perseguirles.
- Guarda en otro dispositivo y borra aquella información sensible y delicada que tengas en el dispositivo en el que estás siendo acosada.
- Si las imágenes han sido publicadas en una red social, ponte en contacto con quien administra el sitio web solicitando la retirada de las mismas. Estás en tu derecho de solicitar la eliminación de tus imágenes.
- Recopila y guarda todas las pruebas y amenazas para una posible denuncia.
- Ponte en contacto[1] con la **Brigada de Investigación Tecnológica** de la Policía Nacional y/o el **Grupo de Delitos Telemáticos** de la Guardia Civil.
- Puedes presentar una denuncia ante la Agencia Española de Protección de Datos, si se han difundido imágenes tuyas sin autorización.
- Puedes acudir también al Centro de Seguridad en Internet para menores: www.protegeles.com

Sexting

Datos de interés

Sexting: envío voluntario a terceras personas de imágenes o videos de contenido sexual mediante dispositivos móviles.

En relación con el intercambio de contenidos personales, por ejemplo vídeos o fotos privadas, como prueba de confianza o acto de intimidad con la pareja, "prueba de amor", este tipo de acciones son una puerta abierta para que se de el sexting. Según el estudio[2] sobre ciberacoso de la Delegación del Gobierno para la Violencia de Género, en relación a las conductas de riesgo de "sexting":

- El 2% de las chicas y el 4,5% de los chicos, han colgado una foto suya de carácter sexual.
- El 1,3% de las chicas y el 2,5% de los chicos han colgado una foto de su pareja de carácter sexual.

Una variación del sexting es el sex-casting, que se produce cuando la imagen con contenido sexual es grabada en una webcam y se difunde a través de correo electrónico o redes sociales.

La difusión de imágenes sexuales realizadas sin consentimiento de quien aparece en ellas es delito. Dicha conducta se considera descubrimiento y revelación de secretos según el artículo 197 del Código Penal, estando además penada con prisión de uno a cuatro años. Para evitar que la difusión no consentida de imágenes, cuando la captación de las mismas es consentida, quede sin sanción penal, está prevista su tipificación como delito en el proyecto de reforma del Código Penal. La posesión o difusión de imágenes, videos con contenido sexual, protagonizado por menores, se considera un delito de pornografía infantil, según el artículo 189 del Código Penal, también el compartir un contenido de pornografía infantil y el poseer para el propio uso material pornográfico en el que han intervenido menores de edad.

La mayoría de edad penal (la exigencia de responsabilidad penal) en España está en los 18 años, aunque la legislación de menores (Ley Orgánica 5/2000 reguladora de la responsabilidad penal de los menores) establece que a las personas mayores de catorce años y menores de dieciocho que cometan delitos o faltas se les pueden imponer distintas medidas – desde una amonestación a medidas de internamiento en régimen cerrado- y, además, responderán solidariamente de los daños y perjuicios causados sus progenitores/as, tutores/as, acogedores/as o guardadores/as.

Por debajo de los 14 años no es imputable, es decir, no es penalmente responsable, pero sus conductas pueden dar lugar a responsabilidad civil de quienes ejercen la tutoría legal, al ser responsables del menor.

Sexting

Datos de interés

Los mandatos de género son construcciones sociales que actúan como imperativos sobre mujeres y hombres condicionando no sólo las relaciones entre los sexos sino también la construcción de la identidad de unas y otros (cómo deben ser, sentir, hacer, o estar). Derivan del conjunto de normas, valores, prácticas y representaciones que asignan atributos y funciones diferentes según el sexo dándoles diferente valor y estructurando relaciones asimétricas de poder. Aunque estos mandatos varían con el tiempo, aún hoy en día, las mujeres son quienes se ocupan fundamentalmente del trabajo reproductivo (los cuidados). En el proceso de socialización diferenciada, aprendemos modelos de comunicación y vinculación afectiva-amorosa distinto a los hombres, siendo ésta una de las claves para entender porqué las mujeres entran en relaciones de subordinación-dominación (violencia) y se mantienen en ellas aunque les dañen. A las mujeres se nos educa en el mandato social de agradar e intentar satisfacer las "necesidades" de las y los otros, incluida la pareja.

De ahí, que sean mayoritariamente las mujeres, las que envíen fotos o vídeos de contenido sexual a sus parejas buscando el agrado y la satisfacción de ellos, sin pensar en las consecuencias que puede llegar a tener para ellas.

Los mitos del amor romántico y la vivencia del mismo, se basan en una rígida división de roles sexuales (él es el salvador, ella es el descanso del guerrero) y estereotipos de género mitificados (él es valiente, ella miedosa; él es fuerte, ella vulnerable; él es varonil, ella es dulce; él es dominador, ella es sumisa). Estos modelos de feminidad y masculinidad patriarcal son la base de las relaciones de subordinación-dominación que experimentamos al establecer relaciones afectivas buscando un ideal que no se corresponde con la realidad (mito del príncipe azul y la princesa maravillosa; mito de la media naranja; mito de la exclusividad; mito de la fidelidad, mito de la perdurabilidad, mito de la convivencia; mito de la omnipotencia; mito del libre albedrío, mito del emparejamiento)[3].

Evaluación

Para reforzar los contenidos aprendidos, piensa si son verdaderas o falsas las siguientes afirmaciones:

El sexting sólo se practica entre adolescentes	*verdadero*	*falso*
Las fotos que se publican en la Red, escapan de tu control	*verdadero*	*falso*
Cuando recibo una imagen comprometedora, es recomendable compartirla y reenviarla	*verdadero*	*falso*
El sexting con tu pareja es una práctica segura	*verdadero*	*falso*
Las imágenes que cuelgo en mis redes privadas nunca podrán ser usadas para chantajearme	*verdadero*	*falso*

Sexting

Palabras Clave

Referencias

[1] La Brigada de Investigación Tecnológica está encuadrada en la Unidad de Delincuencia Económica y Fiscal (UDEF) que es el órgano de la Dirección General de la Policía y de la Guardia Civil encargado de la investigación y persecución de las actividades delictivas, de ámbito nacional e internacional, en materia de delincuencia económica y fiscal, así como la coordinación operativa y apoyo técnico a las respectivas Unidades Territoriales.

- Brigada de Investigación Tecnológica de la Policía Nacional: http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html
- Grupo de Delitos Telemáticos de la Guardia Civil: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

[2] Torres Albero, Cristóbal (Dir.), Robles, José Manuel y de Marco, Stefano (2013) *"El ciberacoso como forma de ejercer la violencia de género en la juventud: un riesgo en la sociedad de la información y del conocimiento*". Ministerio de Sanidad, Servicios Sociales e Igualdad. Delegación del Gobierno para la Violencia de Género.

[3] Herrera Gómez, Coral (2011) *"Los mitos del amor romántico"*.
Disponible en: http://goo.gl/zZWm2D
[Consultado: 02/09/2014]

Materiales didácticos **"Confianza y seguridad de las mujeres en la Red"**

Extorsión sexual / Sextorsión

Actividades didácticas

Objetivos generales

Al acabar las actividades, las participantes serán capaces de:

- Identificar la violencia sexual que se produce en la Red.
- Reconocer los posibles riesgos que conlleva compartir experiencias y materiales (imágenes, vídeos o fotos) de contenido comprometido en la Red.
- Identificar medidas preventivas que ayuden a disminuir los riegos de sufrir sextorsión.
- Identificar los pasos a seguir en caso de ser víctima de sextorsión.

¿Dónde sucede?

Correo electrónico

Redes sociales

Juegos en línea

Mensajería instantánea

1 Actividad
Agencias de modelos

2 Actividad
Vota mis fotos en Internet

3 Actividad
Cibersexo por la webcam

MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
SECRETARÍA DE ESTADO DE SERVICIOS SOCIALES E IGUALDAD
INSTITUTO DE LA MUJER Y PARA LA IGUALDAD DE OPORTUNIDADES
Unión Europea
Fondo Social Europeo

Agencias de modelos

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Tomar conciencia del alcance que supone el envío de materiales de carácter comprometido a través de las redes.
- Identificar elementos de sospecha ante la sextorsión.

1
Actividad

Recursos y materiales


Bolígrafos


Papel


PC

Tiempo

20 min.

Agencias de modelos

1
Actividad

Desarrollo

1. El equipo facilitador leerá el siguiente caso:

CASO BASADO EN UNA NOTICIA REAL

Gracias a la denuncia de una mujer de 32 años a través del portal de colaboración ciudadana alojado en la web del Grupo de Delitos Telemáticos del Instituto Armado, la Guardia Civil ha detenido a un hombre que se hacía pasar por el dueño de dos prestigiosas agencias de modelos para conseguir fotografías de mujeres desnudas a través de Internet. El extorsionador había logrado contactar con más de 400 mujeres, muchas de ellas menores de edad. El detenido creaba perfiles falsos en las redes sociales para dar credibilidad a sus supuestas exitosas empresas, y ofrecía a las mujeres participar en un casting on-line para incluirlas en el book de sus agencias. El casting se realizaba por medio de la webcam, mientras el detenido pedía que posasen cada vez con menos ropa con la excusa de comprobar si sus cuerpos se ajustaban a lo que buscaba la agencia, hasta que acababan desnudándose. Una vez conseguidas las imágenes de las víctimas, el detenido las obligaba a realizar actos obscenos ante la cámara bajo la amenaza de difundirlas entre sus contactos.

2. Se abrirá un debate con los hechos del caso expuesto, en torno a las siguientes preguntas:

a) ¿Por qué crees que las mujeres creyeron que se trataba de agencias de modelos reales?
b) ¿Cómo podrían haber comprobado que era una estafa y no un servicio real?

Recuerda que

- Las ofertas de trabajo con condiciones demasiado atractivas que se publican en la Red, pueden estar asociadas a estafas y engaños que además de tener consecuencias económicas, también pueden atentar contra tu dignidad y honor.
- Tienes que contrastar la información que lees en Internet y asegurarte de que son sitios legítimos.

Agencias de modelos

1
Actividad

Desarrollo

3. A continuación, se trabajará en grupos de 5 mujeres como máximo y cada grupo elegirá una relatora.

4. Cada grupo tendrá que encontrar al menos dos agencias de modelos en Internet que ofrezcan servicios de modelaje, casting on-line, fotografía, book, etc., dirigidos principalmente a mujeres.

5. Una vez encontradas las dos agencias, se responderá por grupos a las siguientes preguntas:

   a) ¿Qué elementos inspiran confianza en las páginas webs encontradas?
   b) ¿Queda clara la protección de datos de carácter personal, incluidas las imágenes, o puede dar lugar a ambigüedades?
   c) ¿Una menor de edad podría tener acceso al casting on-line o al envío de sus fotografías?
   d) ¿El casting on-line requiere fotografías en ropa interior, de baño, o vídeos?, ¿mandarías tus fotos a esa agencia?

6. En plenario, se expondrán los resultados de la búsqueda y las principales conclusiones a las que han llegado.

Recuerda que

- Has de ser consciente del alcance y la rapidez con que se difunden los archivos en la Red teniendo en cuenta que el origen de las imágenes con contenido íntimo que compartimos en la Red puede ser:

  Voluntario: La víctima ha compartido este tipo de material en Internet, a través de las redes sociales, con sus contactos o parejas sentimentales de forma privada, siendo consciente de la existencia de dichas imágenes y quiénes tienen acceso a ellas.

  Involuntario: Quienes ciberacosan consiguen el material a través de terceras personas, obteniéndolo por estar publicado en Internet, o directamente de forma ilegal mediante grabaciones no consentidas o robo de contenidos por accesos no autorizados a los dispositivos de las víctimas. En este caso las víctimas no son conscientes de quiénes tienen dicho material.

Vota mis fotos en Internet

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Analizar la cosificación que se hace de los cuerpos de las mujeres en la Red.
- Reconocer las distintas causas y consecuencias que tiene para mujeres y hombres compartir fotografías de contenido comprometido en la Red.

2 Actividad

Recursos y materiales


Bolígrafos


Papel


PC

Tiempo

15 min.

Vota mis fotos en Internet

2
Actividad

Desarrollo

1. Se trabajará en grupos de 5 mujeres y cada grupo elegirá una relatora.
2. Se pedirá que hagan una búsqueda en Internet de webs donde se voten fotos de chicas.
3. Con los resultados encontrados tendrán que reflexionar teniendo en cuenta las siguientes cuestiones:
    a) ¿Por qué las mujeres participan en ese tipo de webs?, ¿por qué participan los hombres?
    b) ¿Crees que participan de la misma manera?
4. A continuación, el equipo facilitador leerá un caso basado en una noticia real: :

CASO BASADO EN UNA NOTICIA REAL

Condenado un joven de 27 años por ciberacosar y sextorsionar a más de 100 mujeres, la mayoría menores de edad. El acusado ha explicado que hay una web, en la que veía "chicas provocativas" y en la que participaba frecuentemente en los foros para ligar en la Red.

5. Tras la lectura del caso, se lanzará la siguiente pregunta:
    a) ¿Por qué algunos chicos pasan a extorsionar a las chicas con las que previamente han intentado ligar?

Vota mis fotos en Internet

Recuerda que

- La sextorsión es un nuevo tipo de violencia sexual, en donde la víctima es chantajeada y a veces extorsionada, bajo la amenaza de publicar y hacer circular en la Red fotografías suyas o vídeos de contenido sexual, erótico e íntimo. La víctima puede ser chantajeada y obligada a realizar favores sexuales, a enviar a quienes la ciberacosan más imágenes eróticas o pornográficas, o se le puede exigir dinero a cambio de no publicarlas.
- Cuando compartes fotos de contenido sensible en la Red, pierdes absolutamente el control de ellas.
- Si decides hacerte fotos, grabar, enviar o almacenar imágenes de contenido íntimo o sexual, has de saber que puedes correr el riesgo de ser víctima de sextorsión. Es importante comprender que este tipo de materiales mal utilizados pueden comprometer nuestra imagen y honor tanto en lo personal como en lo profesional. Ten bajo tu control los soportes de almacenamiento en los que tengas guardadas dichas imágenes.
- En la Red se reproducen las mismas relaciones de desigualdad de género y comportamientos machistas que en otros ámbitos de la vida, con el agravante de que se puede permanecer en el anonimato.
- Las TIC permiten conocer a gente diferente abriendo muchas posibilidades y oportunidades de relacionarnos, pero es importante estar alerta ante cualquier signo de sospecha de violencia.

Cibersexo por la webcam

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Identificar los riesgos que supone practicar sexo a través de la webcam.
- Descubrir técnicas que sirvan para proteger tu imagen en el caso de que practiques sexo a través de la webcam.
- Reconocer qué pasos hay que seguir ante una situación de sextorsión.

3
Actividad

Recursos y materiales


Rotuladores de colores


Papel


Papel continuo/cartulinas

Tiempo

20 min.

Cibersexo por la webcam

3
Actividad

Desarrollo

1. Se trabajará en grupos de 5 mujeres como máximo y cada grupo elegirá una relatora.
2. Cada grupo tendrá que construir un mural contestando a las siguientes preguntas, tomando la historia de Bárbara como referente:

CASO BASADO EN UNA HISTORIA REAL

"Me llamo Bárbara, tengo 20 años y estoy sufriendo sextorsión por parte de un chico con el que tuve cibersexo por webcam hace 5 meses. Durante la grabación empecé a sentirme incómoda por sus peticiones, así que corté la imagen y entonces él se enfadó, y me amenazó diciéndome que lo había grabado todo, y que lo iba a publicar en internet. Discutimos y no volvimos a hablar. Pero ayer, después de tanto tiempo, se puso en contacto conmigo y me dio un plazo de 24h para volver a tener cibersexo; sino, difundirá el primer vídeo entre mis contactos. Estoy muy asustada ¿qué puedo hacer?"

   a) ¿Qué conductas pueden ponerte en riesgo de sufrir sextorsión?
   b) ¿Qué comportamientos puedes tener para prevenir la sextorsión si tienes prácticas sexuales en la Red?
   c) ¿Qué puedes hacer si eres víctima de sextorsión?

3. Al finalizar, se colgarán los murales por el aula, y cada relatora expondrá en plenario los resultados, para hacer un debate conjunto recordando que existen determinadas **conductas de riesgo** que pueden facilitar el ciberacoso (ver" Recuerda que"de la Actividad 3)

Recuerda que

- Siempre que no utilices la webcam, es aconsejable que la desconectes.
- No debes de acceder nunca a las peticiones y chantajes de quien te ciberacosa, ni facilitarle información. Tan sólo recuérdale que sus acciones son un delito grave y que la ley le puede perseguir.
- Puedes ponerte en contacto con la Brigada de Investigación Tecnológica de la Policía Nacional y/o el Grupo de Delitos Telemáticos de la Guardia Civil, cuando sientas el menor indicio de sospecha de acoso o violencia.

Conductas de riesgo

- Exhibiciones voluntarias a través de la webcam de contenido erótico, sexual e íntimo.
- Autofoto (selfie) de contenido erótico, sexual e íntimo.
- Grabaciones de prácticas sexuales.
- Chatear con personas desconocidas.
- Publicación de datos personales de carácter confidencial en las redes sociales.

Extorsión sexual / Sextorsión

Consejos y buenas prácticas

Recomendaciones para prevenir situaciones de sextorsión

- Sé consciente del riesgo que corres si compartes material de contenido íntimo con personas de tu círculo de confianza o incluso con parejas sentimentales, ya que en el caso de ruptura, pueden ser quienes difundan los materiales o incluso te chantajeen.
- Intenta mantener tus dispositivos (Smartphone, PC) libres de software pirata o virus para evitar el robo de claves personales, ficheros o contenidos privados.
- Es recomendable proteger tus dispositivos mediante contraseñas robustas ya que en caso de robo o pérdida, será más complicado acceder a tu información personal.
- Desactiva la descarga automática de ficheros, y antes de abrir uno que te hayan enviado, analízalo con un antivirus para comprobar que no contiene malware que infecte tu dispositivo.
- Recuerda que los datos personales que publiques en la Red, son muy difíciles de controlar en un futuro, especialmente si se reproducen de manera vírica.

Consejos si eres víctima de sextorsión:

- Pide ayuda a tu círculo familiar y de amistades.
- No accedas a las peticiones y chantajes de quienes te quieran acosar, chantajear o amenazar.

Tienes que saber que sus acciones son un delito grave y que la ley puede perseguirles.

- Recopila y guarda todas las pruebas y amenazas por si decides emprender acciones legales en algún momento.
- Borra y guarda en otro dispositivo aquella información sensible y delicada que tengas en el dispositivo en el que estás siendo acosada.
- Si las imágenes han sido publicadas en una red social, ponte en contacto con quien administra el sitio web solicitando la retirada de las mismas. Estás en tu derecho para solicitar la eliminación de tus imágenes.
- Comprueba que no tienes instalado ningún tipo de virus en tu equipo; muchas veces la ciberdelincuencia que sextorsiona a sus víctimas intentn controlar sus equipos.
- Ponte en contacto[1] con la **Brigada de Investigación Tecnológica** de la Policía Nacional y/o el **Grupo de Delitos Telemáticos** de la Guardia Civil.
- Puedes presentar una denuncia ante la Agencia Española de Protección de Datos, si se han difundido imágenes tuyas sin autorización.

Extorsión sexual / Sextorsión

Datos de interés

Chantaje sexual online que se ejerce principalmente contra mujeres y adolescentes a partir de fotos y vídeos.

En España la sextorsión no está tipificada específicamente como delito en el Código Penal, aunque puede implicar diferentes actos ilícitos tales como: Extorsión, chantaje, amenazas, explotación sexual, abuso sexual y corrupción de menores, revelación de secretos, daños al honor, interceptación de comunicaciones, producción, tenencia y/o distribución de pornografía infantil.

Es la utilización de contenidos sexuales a los que se ha tenido acceso y que se han compartido a través de internet, para obtener algo de otra persona a cambio, amenazándola con publicarlos si no se accede a enviar nuevas imágenes, a mantener contactos sexuales, a continuar la relación e impedir la separación, etc.

La sextorsión es una forma de explotación sexual, en la cual se chantajea a una persona por medio de una imagen de sí misma desnuda que ha compartido a través de Internet. La víctima es posteriormente coaccionada para tener relaciones sexuales con quien chantajea, para producir pornografía u otras acciones, que pueden ser constitutivas de distintos delitos (coacciones, amenazas, contra la libertad sexual, etc.)

Con independencia de todo lo indicado hay que tener en cuenta que la mayoría de los términos utilizados en este escrito no están tipificados como tales en el Código Penal, si bien dichas conductas pueden incluirse en distintas figuras delictivas a las se ha hecho referencia.

Existe el Centro de Seguridad en Internet para menores, integrado en el Safer Internet Programme de la Comisión Europea, cuyo objetivo principal es sensibilizar a jóvenes en el uso seguro y responsable de Internet y de las Tecnologías de la Información y Comunicación. En España, el Centro de Seguridad en Internet está coordinado por la organización de protección de la infancia PROTEGELES, en consorcio desde marzo de 2012 con el CESICAT (Centro de Seguridad de la Información de Cataluña).

Extorsión sexual / Sextorsión

Evaluación

Para reforzar los contenidos aprendidos, piensa si son verdaderas o falsas las siguientes afirmaciones:

La sextorsión es un tipo de violencia sexual digital	*verdadero*	*falso*
Las imágenes que cuelgo en mis redes privadas nunca podrán ser usadas para chantajearme	*verdadero*	*falso*
Es imposible que otras personas roben mis imágenes a través de mi webcam	*verdadero*	*falso*
Las fotos que se publican en la red, se quedarán siempre en Internet	*verdadero*	*falso*
Abrir archivos adjuntos de personas desconocidas no entraña riesgo	*verdadero*	*falso*

Extorsión sexual / Sextorsión

Palabras Clave

chantaje
virtual
ciberdelitos
privacidad
malware
víctimas
sexting
acoso
riesgo
imagen
intimidad
violencia
extorsión
abuso
digital
sexual
denuncia
webcam
ciberacoso

Extorsión sexual / Sextorsión

Referencias

[1] La Brigada de Investigación Tecnológica está encuadrada en la Unidad de Delincuencia Económica y Fiscal (UDEF) que es el órgano de la Dirección General de la Policía y de la Guardia Civil encargado de la investigación y persecución de las actividades delictivas, de ámbito nacional e internacional, en materia de delincuencia económica y fiscal, así como la coordinación operativa y apoyo técnico a las respectivas Unidades Territoriales.

- Brigada de Investigación Tecnológica de la Policía Nacional: http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html
- Grupo de Delitos Telemáticos de la Guardia Civil: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

Materiales didácticos **"Confianza y seguridad de las mujeres en la Red"**

Acoso sexual a menores en Internet / Grooming

Actividades didácticas

Objetivos generales

Al acabar las actividades, las participantes serán capaces de:

- Reconocer el tipo de estrategias que suelen llevar a cabo quienes acosan en la Red con una finalidad sexual.
- Reconocer los signos de alerta ante situaciones de acoso sexual en Internet.
- Identificar medidas preventivas que ayuden a evitar situaciones de acoso sexual en la Red.
- Conocer qué pasos hay que seguir en caso de ser víctima de grooming.

¿Dónde sucede?

Correo electrónico | Redes sociales | Juegos en línea | Mensajería instantánea

1 Actividad
Amistades engañosas en la Red

2 Actividad
Acoso en la Red: el caso del whatsapp

MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
SECRETARÍA DE ESTADO DE SERVICIOS SOCIALES E IGUALDAD
INSTITUTO DE LA MUJER Y PARA LA IGUALDAD DE OPORTUNIDADES

Unión Europea
Fondo Social Europeo

Amistades engañosas en la Red

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Comprender el alcance que supone el envío de materiales de carácter íntimo y erótico a través de las redes.
- Identificar los elementos de sospecha ante una situación de grooming.
- Tomar conciencia de los peligros que conlleva hablar con personas desconocidas por Internet.

1
Actividad

Recursos y materiales


Bolígrafos


Papel


Sobres

Tiempo

30 min.

Amistades engañosas en la Red

1
Actividad

Desarrollo

1. Se explicará que se va a llevar a cabo una dinámica de roles. La historia que se va a representar tiene el siguiente contexto: Dos adolescentes se han conocido a través de un chat en Internet durante el verano. Una (chica 1) está pasando las vacaciones en la playa con su familia, y la otra (chica 2) se ha quedado trabajando en la ciudad. Hablan todos los días, tanto por las redes sociales como por mensajería instantánea.
2. El equipo facilitador dividirá al grupo en dos. Un grupo representará a la chica 1, y el otro a la chica 2. Los mensajes que se manden entre ellas los tendrán que escribir realmente en un papel, ya que luego servirá para cerrar la dinámica. Se explicará a cada grupo su papel en privado, de tal manera que el otro grupo no lo sepa.

Consignas para representar a la chica 1

Eres una chica de 15 años que está aburrida pasando las vacaciones en la playa con tu familia. Has conocido a una nueva amiga por un chat y te cae fenomenal. Es muy divertida, provocadora y te ha contado muchas cosas de su vida ganándose así tu confianza. Tu nueva amiga tiene un gran complejo con su físico y a ti te gustaría ayudarla.

Consignas para representar a la chica 2

En realidad no eres una chica, eres un hombre de 35 años que pretende ganarse la confianza de una adolescente para obtener fotografías de ella desnuda y poder acosarla sexualmente. Te haces pasar por una chica de 16 años divertida, provocadora y con problemas de sobrepeso, que se ha quedado el verano trabajando. Te haces amiga de la adolescente para ganarte su confianza y pedirle que te envié fotografías, primero en bañador y luego en top-less. Si la chica te reclama también fotografías, aducirás tus complejos físicos para evitar mandárselas. Una vez que consigas las fotografías, le explicarás que en realidad eres un hombre, y que si no mantiene relaciones sexuales contigo le pasarás a sus familiares las imágenes.

Recuerda que

- Antes de compartir fotos de contenido comprometido en la Red, piensa que existe la posibilidad de poner en peligro tu privacidad e intimidad, teniendo consecuencias graves para tu vida y tu salud integral.
- Cuando aceptes a personas desconocidas en las redes sociales, asegúrate de conocerlas bien antes de compartir información personal con ellas. Por ejemplo, puedes buscar sus referencias en la Red. Hay veces que quienes ciberacosan utilizan todo tipo de estrategias de manipulación, como decirte que comparten intereses comunes contigo (actividades lúdicas y de ocio, aficiones: Música, lectura, deporte, etc.) para ganarse tu confianza.
- El acoso y la violencia sexual son un delito. Nadie tiene derecho a coaccionarte para mantener relaciones o prácticas sexuales contra tu voluntad.

Amistades engañosas en la Red

1 Actividad

Desarrollo

3. Una participante de cada grupo será la encargada de leer los mensajes escritos en papel entre las dos chicas. Es importante tener en cuenta que ambas están alejadas por muchos kilómetros.

4. Una vez terminada la representación se abrirá un debate para reflexionar sobre:
   a) ¿Qué podría haber hecho la adolescente para asegurarse de que su nueva amiga era de fiar?
   b) ¿Existe un perfil específico de quienes ciberacosan? ¿Y de víctima?
   c) ¿Qué tipos de mensajes creéis que se utilizan para enganchar, seducir y acosar a la víctima?

5. Para finalizar la actividad, el equipo facilitador leerá los siguientes **signos de alerta que deben tenerse en cuenta para evitar el grooming** en caso de que no hayan salido en las reflexiones de los grupos.

Si acabas de conocer a alguien por Internet, mantente alerta si...

- Demuestra un interés desmesurado sobre ti y tus gustos. Alguien que te pregunta de manera insistente sobre tu situación familiar, donde vives, qué estudias, etc., puede no tener buenas intenciones.
- Se comporta de manera exageradamente amable, ofreciéndote regalos o ayuda constante sin que se la pidas.
- Te manda fotografías suyas de carácter comprometido y te pide que hagas lo mismo.
- Sientes que con la información que le has ido contando gracias a la confianza que te ha dado, empieza a manipularte o chantajearte pidiéndote cosas con las que no te sientes cómoda.

Rechaza su amistad hasta que puedas comprobar fehacientemente de quién se trata y qué expectativas de relación tiene contigo.

Acoso en la Red: el caso del whatsapp

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Identificar los distintos medios telemáticos que utilizan quienes ciberacosan.
- Construir pautas para la prevención del grooming.

2 Actividad

Recursos y materiales


Boligrafos


Papel


PC

Tiempo

20 min.

Acoso en la Red: el caso del whatsapp

2
Actividad

Desarrollo

1. Se trabajará en grupos de 4 mujeres como máximo y cada grupo elegirá una relatora.

2. Para iniciar la dinámica se realizará una breve lluvia de ideas para concretar el **significado de grooming**, recordando por parte del equipo facilitador, que se trata de un **tipo de ciberacoso sexual en el que una persona adulta intenta ganarse la confianza de un o una menor, con la intención de llevar a cabo un abuso sexual.** Las estrategias de quienes cometen este delito son diversas: Establecer lazos de amistad simulando también ser menores; seducir, engatusar, provocar, hasta conseguir el control emocional del o la menor y que cumpla con las peticiones de quien acosa (envío de datos personales y material íntimo de la víctima). Una vez establecidos los supuestos lazos de amistad, se inicia el acoso, chantajeando a la víctima, para obtener material pornográfico de ésta o tener un encuentro físico con él o la menor para abusar sexualmente de ésta.

3. Cada grupo tendrá que encontrar en la Red al menos dos casos de grooming y:
    a) Pensar qué tipo de estrategias hay en común en los casos hallados.
    b) Proponer medidas de prevención.

4. El equipo facilitador leerá el siguiente caso basado en un hecho real para poder utilizarlo también en el debate posterior.

Recuerda que

- No accedas al chantaje y evita quedar físicamente con alguien que sólo has conocido por la Red, ya que puede estar engañándote. Si lo haces, ve acompañada de alguna amistad o familiar.
- Las adolescentes en particular tienen más riesgo de sufrir este tipo de violencia, así que ante el primer signo de alerta, coméntalo con alguna persona adulta de confianza para que pueda aconsejarte y ayudarte.
- El papel de las familias es clave en el proceso de detección y abordaje de las situaciones de acoso sexual a menores.
- Cualquiera puede sufrir acoso sexual en la Red, sin embargo, en su mayoría suelen ser menores y mujeres quienes sufren más este tipo de abusos.

Acoso en la Red: el caso del whatsapp

2
Actividad

Desarrollo

CASO BASADO EN UNA HISTORIA REAL

Un hombre es detenido y acusado por amenazar y chantajear a adolescentes a través de mensajes de Whatsapp. El detenido usaba una foto y un nombre falso de una adolescente para ganarse así la confianza. El pretexto de los mensajes era la búsqueda de amigas para hablar y así poco a poco se ganaba la confianza de sus víctimas para luego obtener sus datos personales y las rutinas de sus vidas privadas. Después las invitaba a jugar un juego supuestamente denominado "conejito" que consistía en que la falsa adolescente enviaba a las menores fotos de ella que debían ser imitadas, y por lo general eran imágenes con alto contenido sexual. Finalmente el acosador es detenido precisamente cuando se encontraba con una menor de edad a la que había citado "bajo amenazas y extorsión", para realizar un vídeo pornográfico.

5. Cuando cada grupo haya terminado su búsqueda y reflexión, la relatora lo expondrá en plenario para debatir las conclusiones entre todas las participantes.

Acoso sexual a menores en Internet / Grooming

Consejos y buenas prácticas[1]

- Es recomendable que si necesitas aportar datos personales en Internet lo hagas de forma privada y segura.
- Puedes utilizar un seudónimo o nicks en Internet, de esta manera estarás más protegida y no revelarás tu identidad real a personas extrañas.
- No aceptes ni agregues a personas desconocidas en tus redes sociales. Con frecuencia, quienes tienen intenciones delictivas, suelen argumentar que están buscando simplemente contactos o amistades con intereses o aficiones comunes.
- Rechaza y bloquea los mensajes de tipo sexual o pornográfico que te lleguen a través del chat o cualquier otro canal.
- Si decides subir fotos tuyas o de tus amistades en sitios públicos, primero piensa en el contenido de éstas y pide permiso, ya que estarías poniendo en peligro tu privacidad y la de terceras personas. Si el contenido de la foto es comprometido, valora y ten presente que esa foto puede llegar a verla cualquier persona, te conozca o no. Por ejemplo, una vez que compartes fotos en redes sociales como Facebook o Tuenti, aunque tengas activados los filtros de privacidad, cualquiera de tus contactos con los que has compartido las fotos podría copiarlas y distribuirlas.
- Cuida y mantén tu equipo seguro: utiliza programas para proteger tu ordenador contra el software malintencionado.
- Modifica tus claves personales para evitar ser espiada en tus redes sociales y correos, y procura utilizar contraseñas robustas y complejas.

En el caso de ser víctima de grooming

- Nunca cedas al chantaje. Pide ayuda a tu círculo familiar y de amistades.
- Ponte en contacto[2] con la **Brigada de Investigación Tecnológica** de la Policía Nacional y/o el **Grupo de Delitos Telemáticos** de la Guardia Civil.
- Puedes contartar también con el Centro de Seguridad en Internet para menores: www.proteleges.com
- Recopila y guarda todas las amenazas (conversaciones, mensajes, capturas de pantalla...) para poder aportarlas como pruebas.
- Borra y guarda en otro dispositivo aquella información sensible y delicada que tengas en el dispositivo en el que estás siendo acosada.
- Comprueba que no tienes instalado ningún virus en tu dispositivo que permita a otras personas acceder a tus archivos.

Acoso sexual a menores en Internet / Grooming

Datos de interés

Grooming: Acoso sexual en la Red de una persona adulta a una menor con una finalidad sexual.

El acoso sexual en la Red de una persona adulta a una menor con finalidad sexual es un delito tipificado en el artículo 183.bis del Código Penal: *"A través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño".*

A través de la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, el grooming ha quedado tipificado como delito en España, al haber introducido un nuevo artículo 183 bis, mediante el que se regula el internacionalmente denominado «child grooming», previéndose además penas agravadas cuando el acercamiento al menor se obtenga mediante coacción, intimidación o engaño.

Evaluación

Para reforzar los contenidos aprendidos, piensa si son verdaderas o falsas las siguientes afirmaciones:

En el grooming tanto quien acosa como la víctima son menores	*verdadero*	*falso*
En el grooming el tipo de acoso es con una intencionalidad exclusivamente sexual	*verdadero*	*falso*
El acoso sexual a menores en la Red es un delito	*verdadero*	*falso*
El chantaje es la principal arma con la que cuentan los ciberacosadores	*verdadero*	*falso*
Sólo las personas más vulnerables pueden sufrir acoso sexual	*verdadero*	*falso*

Acoso sexual a menores en Internet / Grooming

Palabras Clave

Referencias

[1] Información elaborada a partir de la documentación contenida en el portal web Ciberfamilias.
Disponible en: http://www.ciberfamilias.com/grooming/
[Consultado 06/07/2014]

[2] La Brigada de Investigación Tecnológica está encuadrada en la Unidad de Delincuencia Económica y Fiscal (UDEF) que es el órgano de la Dirección General de la Policía y de la Guardia Civil encargado de la investigación y persecución de las actividades delictivas, de ámbito nacional e internacional, en materia de delincuencia económica y fiscal, así como la coordinación operativa y apoyo técnico a las respectivas Unidades Territoriales.

- Brigada de Investigación Tecnológica de la Policía Nacional: http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html
- Grupo de Delitos Telemáticos de la Guardia Civil: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

Materiales didácticos **"Confianza y seguridad de las mujeres en la Red"**

Ciberacoso escolar / Cyberbullying

Actividades didácticas

Objetivos generales

Al acabar las actividades, las participantes serán capaces de:

- Reconocer el ciberacoso escolar como una de las formas de violencia en la infancia, así como una vulneración de derechos.
- Identificar medidas preventivas contra el ciberacoso escolar.
- Identificar medidas a tomar ante un posible caso de ciberacoso escolar.

¿Dónde sucede?

Correo electrónico | Redes sociales | Juegos en línea | Mensajería instantánea

1 Actividad
Las redes sociales: un canal para el cyberbullying

2 Actividad
Acosada

MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
SECRETARÍA DE ESTADO DE SERVICIOS SOCIALES E IGUALDAD
INSTITUTO DE LA MUJER Y PARA LA IGUALDAD DE OPORTUNIDADES
Unión Europea
Fondo Social Europeo

Las redes sociales: un canal para el cyberbullying

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Reconocer las consecuencias y medidas que se deben adoptar ante una situación de ciberacoso escolar en caso de sufrirlo nuestras hijas o hijos.

1
Actividad

Recursos y materiales


Rotuladores de colores


Papel continuo / cartulina


PC


Cinta adhesiva


Proyector

Tiempo

20 min.

Las redes sociales: un canal para el cyberbullying

1
Actividad

Desarrollo

1. El equipo facilitador proyectará en el aula los siguientes casos basados en hechos reales para que todas las participantes puedan leerlos a la vez:

CASO 1 BASADO EN HECHOS REALES

Un niño mostró a su madre como en su perfil de una red social, sus compañeros y compañeras de clase se metían con él con publicaciones desagradables e insultantes a través del muro, y cómo para defenderse, él hacía lo mismo. Ante este hecho la madre buscó información en internet y bloquearon a los contactos que le insultaban.

CASO 2 BASADO EN HECHOS REALES

Una joven adolescente se trasladó con su familia a una pequeña localidad, donde tuvo que matricularse a mitad del curso escolar en el instituto de educación secundaria que había en el barrio. Como forma de integración la joven creó un perfil social que estaba vinculado con el centro educativo, pensaba que así conocería más rápido a los chicos y chicas. Sin embargo, transcurridas un par de semanas comenzó a sentir que en la clase la ignoraban o la insultaban puntualmente. Uno de los chicos de clase reconoció su perfil en la red social y empezó a utilizar imágenes distorsionadas de ella para acosarla.

Recuerda que

- El ciberacoso escolar o cyberbullying es un tipo de acoso realizado entre menores a través de medios tecnológicos como: Llamadas reiteradas o mensajes desagradables, dañinos o abusivos a través del móvil o Internet (correos electrónicos, chat, mensajería instantánea, redes sociales, etc.); difusión de comentarios hablando mal sobre alguien o colgando en internet información personal; o envío de fotos hechas con el móvil y utilizadas para amenazar.
- **CONSECUENCIAS:** Para la vida de la víctima que puede sufrir sentimientos de humillación, ansiedad, perdida de la autoestima y la confianza, aislamiento u otros, pudiendo llegar a la depresión.
- **PREVENCION:** El ciberacoso escolar o cyberbullying suele ejercerse por personas del entorno cercano a la víctima, por tanto es importante cuidar la información personal que damos en Internet porque no sabemos el uso que le van a dar. Es fundamental generar un clima de confianza y buena comunicación con tus hijas e hijos para que tengan la complicidad suficiente para contarte sus problemas personales.

Las redes sociales: un canal para el cyberbullying

1
Actividad

Desarrollo

2. Posteriormente se realizarán grupos de 3 mujeres como máximo y cada grupo elegirá una relatora.

3. Cada uno de los grupos deberá construir un mural con la información siguiente:

    a) Consecuencias sobre la vida de las víctimas que sufren ciberacoso escolar o cyberbullying.
    b) Pasos a dar en caso de ser víctima de ciberacoso escolar o cyberbullying.
    c) Medidas preventivas para no sufrir ciberacoso escolar o cyberbullying.

4. Finalizados los murales, cada grupo los colgará con cinta adhesiva en las paredes del aula y se pondrán en común los resultados.

Recuerda que

PASOS A DAR EN CASO DE SER VÍCTIMA

- En caso de que tus hijos e hijas sean víctimas de ciberacoso escolar, debes ponerlo en conocimiento de las autoridades educativas y denunciarlo a la Policía o a la Guardia Civil. Además, puedes informar al servicio desde el cual se está realizando el ciberacoso para que la empresa suministradora del mismo tome las medidas necesarias para que quienes ciberacosan no pueda seguir utilizando ese canal.
- Recuerda que las empresas proveedoras de servicios de redes sociales disponen de opciones para denunciar conductas abusivas. En el caso de la red social Facebook se puede denunciar todo tipo de situaciones abusivas que sean sospechosas de formar parte de un acoso.
- Además aconseja a quienes sufren ciberacoso escolar que no respondan a los mensajes de quienes les acosan ya que puede provocar nuevas agresiones.

Acosada

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Identificar los signos de alerta que pueden hacer sospechar de una situación de ciberacoso escolar o cyberbullying.

2
Actividad

Recursos y materiales


Boligrafos


Papel


PC


Proyector


Corto "Acosada"

Tiempo

20 min.

Acosada

2
Actividad

Desarrollo

1. En primer lugar se visionará el corto "Acosada", de tres minutos de duración, producido por Save the Children.

2. En plenario, el equipo facilitador planteará las siguientes preguntas para la reflexión grupal y el debate:
    a) ¿Cómo os habéis sentido al ver el video? ¿Qué os ha suscitado?
    b) ¿Es una situación de ciberacoso escolar o cyberbullying?, ¿por qué?
    c) ¿Qué tipos de violencias se pueden identificar en la historia?
    d) ¿Qué estrategias llevan a cabo quienes ciberacosan?
    e) ¿Qué motiva a la chica a hablar con su supuesto nuevo amigo y enviarle una fotografía?

3. Una vez debatidas estas cuestiones, el equipo facilitador pedirá a las participantes que se junten en parejas, y piensen en una acción de empoderamiento que se podría llevar a cabo con la protagonista, con el fin de mejorar su autoestima y poder evitar verse involucrada en una situación de ciberacoso escolar.

4. Finalmente, se expondrá en plenario y se cerrará la dinámica pudiendo ilustrar la gravedad del cyberbullying con una historia basada en hechos reales que acompaña a la dinámica.

CASO BASADO EN HECHOS REALES

Una joven sufrió un constante acoso cibernético, desde proposiciones de relaciones sexuales con desconocidos hasta insultos, tras la distribución en su instituto de imágenes de la violación en grupo que sufrió a los 15 años por un grupo de jóvenes de su centro. Con 16 años falleció a causa de la ingesta masiva de medicamentos.

Recuerda que

- El anonimato de quien agrede, las dificultades prácticas para detener la agresión, la no percepción directa e inmediata del daño causado y la adopción de identidades ficticias o roles imaginarios en la Red, convierten al cyberbullying, en un grave problema social y de la comunidad, además de individual.
- Las personas que ciberacosan eligen a víctimas vulnerables con escasas redes de apoyo, por lo que es aconsejable que tus hijas e hijos sientan apoyo por parte de sus familias y sus grupos de amistades para poder dar respuesta a una situación de ciberacoso.

Ciberacoso escolar / Cyberbullying

Consejos y buenas prácticas

Consejos dirigidos a madres y padres para prevenir situaciones de ciberacoso:

- Genera un clima de confianza y buena comunicación con tus hijas e hijos para que tengan la complicidad suficiente de contarte sus problemas personales.
- Ten una actitud proactiva e implícate en sus actividades.
- Explícales la importancia de un uso responsable de las TIC para asegurarles una navegación segura (tiempo de conexión, limitación de horarios y contenidos).
- Adviérteles de los riesgos que existen en la Red; explícales la importancia de cuidar su imagen y su privacidad.
- Haz entender a tus hijas e hijos la importancia de una cultura de respeto entre las personas en el ámbito digital "no hagas a nadie lo que no quieras que te hagan a ti".
- Explícales que las imágenes que comparten, pueden pasar de mano en mano sin control.
- Adviérteles sobre los riesgos de contactar y chatear con personas extrañas.
- Incentiva los usos alternativos de la tecnología que no solo sean las redes sociales. Actividades como, crear contenidos, investigar, diseñar o programar, pueden crear hábitos interesantes y fomentar relaciones personales con menos riesgo.
- Recuerda que si ocurre dentro del colegio o instituto, debes ponerlo en conocimiento de las autoridades educativas y contactar[1] con la Policía Nacional (Brigada de Investigación Tecnológica) o Guardia Civil (Grupo de Delitos Telemáticos).

En caso de que tus hijos e hijas sientan que puedan estar sufriendo ciberacoso escolar o cyberbullying dales estos consejos:

- Diles que no respondan a las llamadas ni mensajes de las personas que les estén acosando o les hagan sentir mal; hacerlo puede desencadenar nuevas agresiones.
- Aconséjales que no lean los mensajes que les pueden hacer daño, pero pídeles que te los reenvíen para que puedas consérvalos, por si en un futuro hubiera que denunciar la situación, ya que tener esas pruebas será muy útil.
- En el caso de las redes sociales, puedes bloquear los perfiles de quienes les acosan.
- Hazles saber que pueden acudir al profesorado en caso de sufrir la agresión en el centro escolar, además de contarlo en casa.

Ciberacoso escolar /Cyberbullying

Datos de interés

Cyberbullying: Tipo de ciberacoso realizado entre menores en el entorno escolar por medios tecnológicos.

Las personas adultas tienen un papel fundamental para combatir y prevenir de manera adecuada el acoso escolar y el ciberacoso. Es importante tener en cuenta que hablamos de menores y es necesario garantizar los derechos de quienes agreden y de las víctimas, de acuerdo con los estándares internacionales y la legislación nacional[2]. Además, es importante considerar que la responsabilidad no es sólo de quien inicia la agresión, sino también de quienes difunden y reenvían los mensajes, convirtiéndose en cómplices del abuso.

En los estudios sobre esta problemática se pone de manifiesto que el ciberacoso es una realidad en los centros educativos españoles. Las cifras parecen estar creciendo en los últimos años, según algunos estudios[3] desde un 19.4% en 2008 hasta un 23.5% en 2011. También las personas implicadas en la difusión desde el 11.6% hasta un 17.5%.

El ciberacoso escolar puede implicar entre otros, el incurrir en alguno de estos delitos (recogidos en el Código Penal):

- Delitos contra la libertad: Amenazas (artículos 169-171), coacciones (artículo 172), torturas y otros delitos contra la integridad moral (artículo 173-177).
- Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio.
- Dlitos contra el honor, la calumnia (capítulo i; artículos 205-207) y la injuria (capítulo ii; artículos 208-210).
- Delito de inducción al suicidio de otra persona (artículo 143).

Ciberacoso escolar/Cyberbullying

Evaluación

Para reforzar los contenidos aprendidos, piensa si son verdaderas o falsas las siguientes afirmaciones:

El cyberbullying se da cuando una persona adulta acosa a un o una adolescente por Internet	*verdadero*	*falso*
El cyberbullying es un ataque estrictamente sexual	*verdadero*	*falso*
El cyberbullying es un grave problema para las víctimas agravado por el anonimato de quienes agreden o acosan, la no percepción directa e inmediata del daño causado y la adopción de roles imaginarios en la Red	*verdadero*	*falso*
El Código Penal español ofrece protección a los niños y niñas que sufren ciberacoso	*verdadero*	*falso*
El ciberacoso es una realidad en los centros escolares españoles	*verdadero*	*falso*

Ciberacoso escolar/Cyberbullying

Palabras Clave

violencia
menores
acoso
escolar
maltrato
cyberbullying
y
delito
iguales
entre
digital
identidad
hostigamiento
engaño
ciberacoso
amenaza

Referencias

[1] La Brigada de Investigación Tecnológica está encuadrada en la Unidad de Delincuencia Económica y Fiscal (UDEF) que es el órgano de la Dirección General de la Policía y de la Guardia Civil encargado de la investigación y persecución de las actividades delictivas, de ámbito nacional e internacional, en materia de delincuencia económica y fiscal, así como la coordinación operativa y apoyo técnico a las respectivas Unidades Territoriales.

- Brigada de Investigación Tecnológica de la Policía Nacional: http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html
- Grupo de Delitos Telemáticos de la Guardia Civil: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

[2] Orjuela López, Liliana. et al., (2014) *"Informe acoso escolar y ciberacoso: propuestas para la acción"*. Save the Children. Ministerio de Sanidad, Servicios Sociales e Igualdad.
Disponible en: http://www.savethechildren.es/docs/Ficheros/675/Acoso_escolar_y_ciberacoso_informe_vOK_-_05.14.pdf
[Consultado 18/07/2014]

[3] *Ibíd.*, p.24

Materiales didácticos **"Confianza y seguridad de las mujeres en la Red"**

Tecnoadicciones

Actividades didácticas

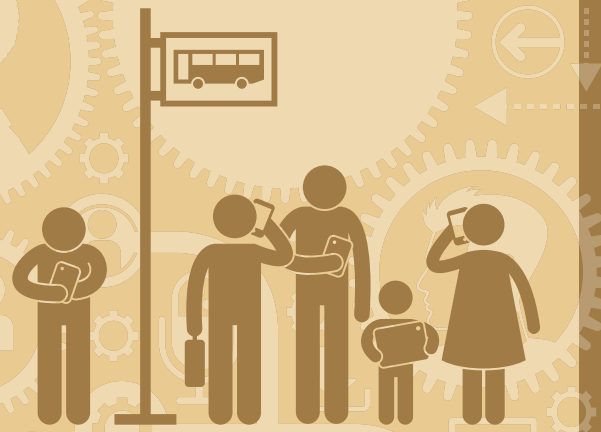
Objetivos generales

Al acabar las actividades, las participantes serán capaces de:

- Reconocer las tecnoadicciones como un problema asociado al uso abusivo de las nuevas tecnologías de la información y la comunicación.
- Identificar alternativas de ocio y uso responsable de las nuevas tecnologías de la información y la comunicación para evitar caer en una tecnoadicción.

¿Dónde sucede?

Internet · Redes sociales · Juegos en línea · Mensajería instantánea · Teléfonos inteligentes · TV



1 Actividad — El apagón

2 Actividad — Regreso al pasado

3 Actividad — Tomando el pulso a las tecnoadicciones

4 Actividad — Decálogo de buenas intenciones

MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
SECRETARÍA DE ESTADO DE SERVICIOS SOCIALES E IGUALDAD
INSTITUTO DE LA MUJER Y PARA LA IGUALDAD DE OPORTUNIDADES
Unión Europea
Fondo Social Europeo

El apagón

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Tomar conciencia del tiempo que se dedica a utilizar dispositivos tecnológicos.
- Reflexionar sobre si utilizamos las nuevas tecnologías de la información y la comunicación de forma abusiva o no.
- Construir grupalmente actividades alternativas al uso de las TIC para la prevención de las tecnoadicciones.

1
Actividad

Recursos y materiales


Rotuladores de colores


Papel continuo / cartulina


PC


Cinta adhesiva


Proyector


Tarjetas

Tiempo

30 min.

El apagón

1
Actividad

Recursos y materiales (Dispositivos tecnológicos)

Cartas para recortar

1

TV

4

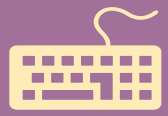
Teléfono fijo

7

Teléfono inteligente

2

Tableta

5

PC

8

Portatil

3

Video consola

6

Redes sociales

9

Correo electrónico

El apagón

1
Actividad

Recursos y materiales (Actividades alternativas)

Cartas para recortar.

10

Tomar un café

11

Leer un libro

12

Biblioteca

13

Jugar juego de mesa

14

Hacer deporte

15

Bailar

16

Escribir una carta

17

Disfrutar al aire libre

18

Ir a un concierto

El apagón

1 Actividad

Desarrollo

1. Se trabajará en grupos de 5 mujeres aproximadamente y cada grupo elegirá una relatora.

2. Se pedirá a las participantes que realicen la siguiente actividad:

   a) Dibujar un gran reloj en la cartulina o papel continuo distribuyendo las 24 horas del día en tramos de 15 minutos.
   b) A cada grupo se le entregarán las **tarjetas tecnológicas** y en torno a la esfera del reloj se pondrán los números correspondientes de las tarjetas en función del uso que hicieron de cada elemento tecnológico el día anterior tantas veces como se hayan utilizado.
   c) Se debatirá en el grupo sobre los resultados que se han obtenido.

3. Posteriormente, el equipo facilitador distribuirá las **tarjetas alternativas** y explicará que ha habido un apagón tecnológico, y que entonces tienen que pintar un nuevo reloj en el que deberán buscar alternativas para conseguir los mismos objetivos que antes, por ejemplo:
   - Si utilizamos el móvil para hablar con las amigas, elegiremos una actividad de socialización presencial con ellas.
   - Si utilizamos la videoconsola para jugar, elegiremos un juego al aire libre o de mesa.

4. Finalmente, se hará un debate en plenario para mostrar las alternativas al posible abuso de las nuevas tecnologías de la información y comunicación, dejando claro que el uso de las mismas puede ser positivo, pero no el abuso.

Recuerda que

- Cualquier persona, independientemente de su edad y sexo, puede sufrir las consecuencias de la adicción a las tecnologías.
- Debes evitar mirar tu móvil o smartphone de manera constante cuando estás con otras personas (phubbing), piensa que si lo haces puedes dejar de disfrutar de su compañía.
- Si haces un uso abusivo de los aparatos tecnológicos puedes estar perdiéndote muchas otras cosas importantes, aparte de colocarte en riesgo de sufrir una tecnoadicción; ¡disfruta de los encuentros presenciales con otras personas además de conectarte con ellas por Internet.

El apagón

1
Actividad

CASO 1: BASADO EN UNA NOTICIA REAL. CONSECUENCIAS NEGATIVAS DE LA TECNOADICCIÓN.

Una dependienta de 35 años de edad, no superó el periodo de prueba para acceder a un puesto de trabajo en unos grandes almacenes, ya que consultaba su teléfono móvil constantemente, incluso cuando había clientela en la tienda. Sus responsables la llamaron la atención en varias ocasiones, pero explicó que "no podía separarse de su teléfono".

CASO 2: BASADO EN UNA NOTICIA REAL. CONSECUENCIAS NEGATIVAS DE LA TECNOADICCIÓN.

Marta, ama de casa de 58 años, decidió ingresar en un programa de atención a las tecnoadicciones al darse cuenta de que desde que sus dos hijas se habían independizado, pasaba más de 8 horas al día conectada a internet y las redes sociales, dejando de lado su cuidado personal y sus relaciones sociales. El apoyo de su familia fue clave para encontrar nuevos espacios de ocio y superar su problemática.

Regreso al pasado

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Conocer las posibles ventajas y riesgos del uso de las TIC.

.

2 Actividad

Recursos y materiales

Boligrafos

Papel

Tiempo

25 min.

Regreso al pasado

2
Actividad

Desarrollo

1. Se trabajará en grupos de 4 mujeres como máximo y cada grupo elegirá una relatora.

2. El equipo facilitador entregará a cada grupo una frase diferente de entre las siguientes propuestas:
    a) Mis dos hijas pequeñas y yo nos vamos de viaje en coche. Es de noche ya, y de repente, el coche se para en mitad de una carretera secundaria. ¡No hay forma de arrancarlo!...
    b) Todos los días voy en metro a trabajar, y observo cómo se comporta la gente...
    c) Salgo a cenar con unas amigas, pero una de ellas pasa totalmente de nosotras...
    d) Mi hija se ha ido a vivir a Londres. Me gustaría hablar con ella y que me cuente como le están yendo las cosas por allí. ¿Cómo hablo con ella?...
    e) Me encanta leer novelas, de lo que sean, me paso el día leyendo, pero últimamente...
    f) Mi hijo José es muy estudioso, aunque le cuesta concentrarse...
    g) Los hijos de mi amiga Pilar se pasan el día jugando...
    h) No puedo soportar más ese sonido, viene de casa de mi vecina, es un ruido casi constante, un pop, pop, pop...
    i) Cuando me levanto lo primero que hago... Después...
    j) Cuando voy de viaje, me gusta hacer muchas fotos..

3. A continuación se explicará la actividad: consiste en regresar al pasado, para después volver. Lo que se persigue es que cada grupo redacte (e incluso, ilustren si quieren) dos pequeñas historias a partir de lo que se cuenta en la frase entregada. Para escribir la primera de las historias, deberán regresar al pasado y relatar qué hubiera pasado en esa situación sin móvil, ordenadores, tablets, etc. Para escribir la segunda de las historias deberán situarse en el presente y continuar la frase tal y como es hoy en día, con móviles, ordenadores, tablets, etc.

Recuerda que

- Las TIC han mejorado nuestra vida en muchos aspectos, pero su uso abusivo es perjudicial, llegando a crear tecnoadicciones. Si pasas el día consultando el móvil, delante del ordenador, actualizando tus redes sociales, etc. te estarás perdiendo muchas actividades que pueden ser gratificantes para ti, como por ejemplo la compañía física de las amistades.
- Toma consciencia de los usos que haces de los tiempos con las TIC, un regreso al pasado de vez en cuando -como en esta actividad- puede venirte bien.

Regreso al pasado

2
Actividad

Desarrollo

4. Al finalizar, en plenario, la relatora de cada grupo leerá las dos historias.

5. Después, el equipo facilitador abrirá el debate sobre los usos de los tiempos en la era de las nuevas tecnologías, beneficios y desventajas de éstas. Para animar el debate, el equipo facilitador podrá realizar las siguientes preguntas:

    a) ¿En cuáles de las situaciones de las historias se abusa de las TIC?
    b) ¿Echáis de menos aficiones a las que ahora no dedicáis tanto tiempo desde que tenéis el móvil, el ordenador o la tablet con conexión a Internet?

.

Tomando el pulso a las tecnoadicciones

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Reconocer en nuestras conductas los signos que pueden alertarnos en relación a un consumo abusivo de las TIC.

.

3
Actividad

Recursos y materiales

Cuadernillo Tecnoadicciones

Tiempo

20 min.

Tomando el pulso a las tecnoadicciones

3
Actividad

Desarrollo

1. Las participantes se colocarán de pie en el centro del aula, preferiblemente en fila.

2. El equipo facilitador formulará cada una de las afirmaciones que aparecen más abajo dando las siguientes indicaciones:
   - Si lo haces muy a menudo, te situarás a la derecha del aula.
   - Si lo haces en muy pocas ocasiones, te situarás a la izquierda del aula.
   - Si lo haces de vez en cuando, te quedarás en el centro del aula.

3. Afirmaciones:
   a) Dedico 3 horas o más de mi tiempo libre a ver la televisión.
   b) Utilizo Internet únicamente como herramienta de interacción y diversión.
   c) Diariamente uso los juegos de mi móvil o Tablet.
   d) Cuando estoy con mis amigas, pareja o familiares no presto atención al teléfono móvil (phubbing).
   e) Prefiero enviar un mensaje de texto o WhatsApp, a mantener una conversación telefónica.
   f) Utilizo las redes sociales para ligar, encontrar personas con mis mismos gustos o hacer nuevas amistades.
   g) Miento en Internet acerca de mi misma.
   h) Estoy constantemente activa en las redes sociales.
   i) Procuro decir la verdad sobre mí misma en Internet, y además me gusta colgar fotos personales.
   j) Prefiero la diversión que ofrece Internet, un videojuego o la TV, antes que otras actividades recreativas.

4. Después de lanzar cada afirmación, las participantes se distribuirán por el aula y cada una de ellas comentará porqué se ha situado en ese lugar. El equipo facilitador dará la palabra a quienes se vayan a los extremos con el fin de animar el debate. Es importante que en la devolución final, el equipo facilitador haga hincapié en que el uso de las TIC conlleva asociados numerosos elementos positivos, pero que el abuso de las mismas puede traernos problemas de adicción.

Recuerda que

Las tecnoadicciones hacen referencia a la falta de control en el consumo de las tecnologías, provocando cambios en la conducta y una pérdida de interés por otras actividades, y se define por las siguientes tres características[1]:

- Tolerancia: La persona necesita aumentar cada vez más el tiempo que pasa utilizando el aparato para así obtener un nivel adecuado de satisfacción.
- Abstinencia: La sensación desagradable que experimenta la persona cuando no puede usar la tecnología, por lo que cada vez la utiliza más y de forma más compulsiva.
- Dependencia: Momento en el que la persona necesita aumentar progresivamente el tiempo de uso de la tecnología (tolerancia) y además, se siente mal si no puede hacerlo (abstinencia), con sentimientos y conductas que repercuten en sus relaciones sociales y en su rendimiento escolar y/o laboral.

El decálogo de las buenas intenciones

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Reflexionar sobre el uso responsable de las nuevas tecnologías de la información y comunicación.
- Identificar los beneficios y riesgos que traen consigo las TIC.

.

4 Actividad

Recursos y materiales

PC Papel Bolígrafos

Tiempo

20 min.

El decálogo de las buenas intenciones

4
Actividad

Desarrollo

1. Se trabajará en grupos de 3 mujeres como máximo y cada grupo elegirá una relatora.
2. Se pedirá a las participantes que se conecten a Internet y busquen información para construir un decálogo que incorpore cinco beneficios y cinco riesgos en el uso de las TIC. Una vez finalizados los decálogos, la relatora de cada grupo pondrá en común las conclusiones en plenario reforzando los beneficios de las TIC y generando así un debate conjunto.
3. Para finalizar la actividad, se leerá el siguiente caso:

CASO BASADO EN UN HECHO REAL. CONVERSACIONES EN UN BLOG.

"¿Soy adicta a Internet? Dejé de trabajar hace meses y me cambié de piso, eso hizo que me alejara de mis amigas y compañeras de trabajo, así que ya no me hablo con ninguna de ellas. Prácticamente no salgo de casa, nunca he sido de salir mucho, pero ahora mi vida social es cero. Paso unas 8 horas conectada a internet, trato de hacer un buen uso, leo, uso programas de mecanografía, me informo de las noticias y sobre todo consulto una gran cantidad de páginas y blog sobre música (¡me encantaría ser DJ!). Hace poco cerré una de mis cuentas de Facebook, que era donde estaba por así decirlo mi vida social, y donde incluso logré salir con algún chico, pero pensé que quizás no era buena idea pasar tanto tiempo conectada a las redes sociales. En realidad no he logrado quitarme del todo, porque tengo otra cuenta donde no me conoce nadie y a veces desperdicio mi día en ella o viendo videos en Youtube. Espero que alguien me pueda ayudar, en verdad me gustaría mucho salir de esto"

Como herramienta pedagógica de distensión, puede visualizarse el siguiente video para debatir en plenario: "No dejes que los dispositivos móviles controlen tus actos. No te conviertas en un Phonbie" Video: "The Phonbies". Asociación Protégeles. Disponibleen: http://www.thephonbies.com/

Recuerda que

- Las nuevas tecnologías de la información y la comunicación ofrecen muchas posibilidades, sin embargo, ten presente el uso que haces de ellas para evitar caer en una tecnoadicción.
- Algunos de los efectos asociados a las tecnoadicciones son: Trastornos y pérdida del sueño; dolores musculares; ansiedad; irritabilidad; depresión y déficit de atención; deterioro de las relaciones familiares y sociales; cese de otras actividades recreativas o deportivas; negación, minimización y/o ocultamiento de la conducta; pérdida de control sobre la misma.

Consejos y buenas prácticas

En general:

- No duermas con el teléfono conectado al lado.
- Planifica las actividades diarias.
- Desactiva las alertas de las redes sociales en los móviles.
- Presta atención a quien se encuentre a tu lado y aprovecha la compañía de las otras personas sin estar pendiente del móvil.
- Planifica tu consumo o compras por Internet.
- Pide ayuda si crees que tienes una tecnoadicción.

Internet:

- Rompe con las rutinas de conexión.
- Utiliza señales y alarmas que indiquen que ha pasado el tiempo planificado y debes desconectarte.
- Elabora un horario realista dentro del cual se contemple no sólo el tiempo dedicado a navegar, sino también otras actividades.
- Conoce las posibilidades formativas de la Red, incluyendo Internet como una herramienta de ayuda al estudio, trabajo o formación.
- Instala filtros de contenido que impidan el acceso a páginas con contenido no adecuado, sobre todo entre menores y adolescentes.

Dispositivos móviles (tablets y smartphone):

- Busca un dispositivo adecuado a tus necesidades y edad.
- Marca límites a la "personalización" de tus dispositivos (compra de melodías, fondos y logos, carcasas, fundas...).
- Toma conciencia del tiempo que pasas hablando y mandando mensajes.
- Delimita los espacios de uso de los dispositivos.
- Si tienes hijas o hijos, retrasa al máximo la edad para que estén en posesión de un teléfono móvil propio.

Consejos y buenas prácticas

Videojuegos y consolas:

- Pon la consola o el ordenador en un espacio común.
- Juega físicamente con otras personas para compartir emociones y puntos de vista.
- Limita el tiempo dedicado a jugar con la consola.
- Valora el nivel de violencia, las habilidades requeridas y la edad adecuada antes de comprar un videojuego.

Televisión:

- Pon la televisión en espacios comunes de la casa.
- Limita el tiempo de uso y evita mantenerla encendida de forma permanente.
- Ve la televisión con un objetivo concreto (por ejemplo: una serie determinada), no "ver por ver".
- Apaga la televisión mientras se está comiendo y aprovecha esos momentos para el diálogo familiar o grupal.

En el caso de que tengas menores a tu cargo, no puedes controlar y vigilar todo lo que hacen, interésate por las cosas que les gustan y sus preferencias en relación a la tecnología, fomentándoles el espíritu crítico.

Tecnoadicciones

Datos de interés

Tecnoadicción: Dependencia relacionada con el abuso de las tecnologías (adicción a Internet, teléfonos móviles, consolas, etc.)

Algunas conductas asociadas a las tecnoadicciones:

- Puesto que las nuevas tecnologías de la información y la comunicación forman parte ya de nuestra vida cotidiana, es difícil determinar dónde está el límite entre el uso necesario y el uso adictivo.
- El "phubbing" hace referencia al uso del teléfono móvil o la tablet mientras se está en compañía de otras personas (del inglés phone –teléfono- y snubbing -desairar-).
- La nomofobia (del inglés No Mobile Phobia) habla del miedo que tienen algunas personas a salir sin el móvil o a no tener conexión.
- El "fomo" (del inglés Fear of Missing Out – miedo a perderse algo), se refiere al sentimiento de exclusión social en el ámbito de las nuevas tecnologías, sobre todo de las redes sociales, y se da cuando la persona necesita estar conectada constantemente con el fin de no sentirse excluida.

¿Quiénes pueden sufrir tecnoadicción?

Como pasa con otras adicciones, cualquier persona puede desarrollar una tecnoadicción, sin embargo, la adolescencia representa un momento de especial vulnerabilidad a la tecnoadicción, tanto para chicas como para chicos, por distintos motivos:

- Las nuevas tecnologías ofrecen la posibilidad de estar en contacto con el grupo de iguales permanentemente, escapando al control paterno y materno.
- Pueden acceder y hablar de temas que cara a cara resultaría más difícil.
- Les permite mostrarse como les gustaría ser y no como son, y así obtener popularidad (amistades en la Red)

Según datos recopilados del Proyecto de Investigación EU NET ADB, financiado por la Comisión Europea y realizado en siete países, el 21,3% de adolescentes españoles está en riesgo de ser adicto a internet por el tiempo que dedica a navegar por la Red, frente al 12,7% de la media europea[2].

Tecnoadicciones

Evaluación

Para reforzar los contenidos aprendidos, piensa si son verdaderas o falsas las siguientes afirmaciones:

Las tres características propias de la tecnoadicción son la tolerancia, la abstinencia y la dependencia	*verdadero*	*falso*
La gente adulta tiene muy poca probabilidad de sufrir tecnoadicción	*verdadero*	*falso*
El phubbing es mirar de manera compulsiva el smartphone o tablet cuando estamos acompañadas	*verdadero*	*falso*
La tecnoadicción, como otras adicciones, puede traer asociados cambios en la conducta	*verdadero*	*falso*
Las personas tecnoadictas ven deterioradas sus relaciones familiares y sociales	*verdadero*	*falso*

Tecnoadicciones

Palabras Clave

Referencias

[1] Información elaborada a partir de la documentación contenida en el Portal del ciudadano de la Comunidad de Madrid, *"Tecnoadicciones"*.
Disponible en: http://www.madrid.org/cs/Satellite?cid=1354332892817&language=es&pagename=PortalCiudadano%2FPage%2FPCIU_contenidoFinal
[Consultado 30/06/2014]

[2] Fundación Mapfre (Marzo 2014) *"Controla TIC"*. Magisterio (Suplemento), núm. 12015.
Disponible en: http://issuu.com/gruposiena/docs/12015suplemento?e=8701546/7049640
[Consultado 30/06/2014]

Materiales didácticos **"Confianza y seguridad de las mujeres en la Red"**

Fraude en la Red / Phishing

Actividades didácticas

Objetivos generales

Al acabar las actividades, las participantes serán capaces de:

- Reconocer los fraudes más frecuentes que se dan en la Red a través de las nuevas tecnologías.
- Identificar los tipos de phishing más frecuentes que circulan en la Red.
- Reconocer las medidas de prevención para este tipo de fraudes.
- Conocer qué pasos hay que seguir en caso de ser víctima de phishing.

¿Dónde sucede?

Correo electrónico · Redes sociales · Mensajería instantánea · Webs · SMS

1 Actividad
Phishing en los sistemas de pago

2 Actividad
Phishing bancario

3 Actividad
Dominios parecidos

4 Actividad
La Administración, víctima de ataques de phishing

MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
SECRETARÍA DE ESTADO DE SERVICIOS SOCIALES E IGUALDAD
INSTITUTO DE LA MUJER Y PARA LA IGUALDAD DE OPORTUNIDADES
Unión Europea
Fondo Social Europeo

Phishing en los sistemas de pago

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Analizar los diversos sistemas de pago para evitar ser víctima de phishing.
- Identificar los indicios de fraude en la Red.
- Decidir que hacer en caso de recibir un mail con este tipo de amenaza.

1
Actividad

Recursos y materiales


Rotuladores de colores


Papel continuo / cartulina


PC


Post-it de colores


Proyector

Tiempo

20 min.

Phishing en los sistemas de pago

1
Actividad

Desarrollo

1. Se iniciará la dinámica con una breve lluvia de ideas sobre si conocen y saben que es:
    a) La suplantación de identidad digital y su diferencia con el phishing.
    b) Un servicio de pago a terceros.

2. Una vez realizada la lluvia de ideas, el equipo facilitador sistematizará qué es cada concepto:

Phishing: Es una estafa donde la ciberdelincuencia, haciéndose pasar por una organización legítima y de confianza (entidad bancaria, redes sociales, Administración Pública, servicios de pago, una gran corporación, etc.), intenta obtener datos confidenciales, habitualmente mediante el envío de correos electrónicos. En el cuerpo del correo incorporan un enlace a una página falsa que suplanta la página web real de la empresa o servicio. Es importante recordar que además del correo electrónico, también se utilizan mensajes a través de aplicaciones de mensajería instantánea, en redes sociales o SMS.

Servicio de pago a terceros: Te permite realizar pagos en línea y evitar así facilitar tu número de tarjeta de crédito directamente a quienes venden por Internet si no te inspiran confianza.

Recuerda que

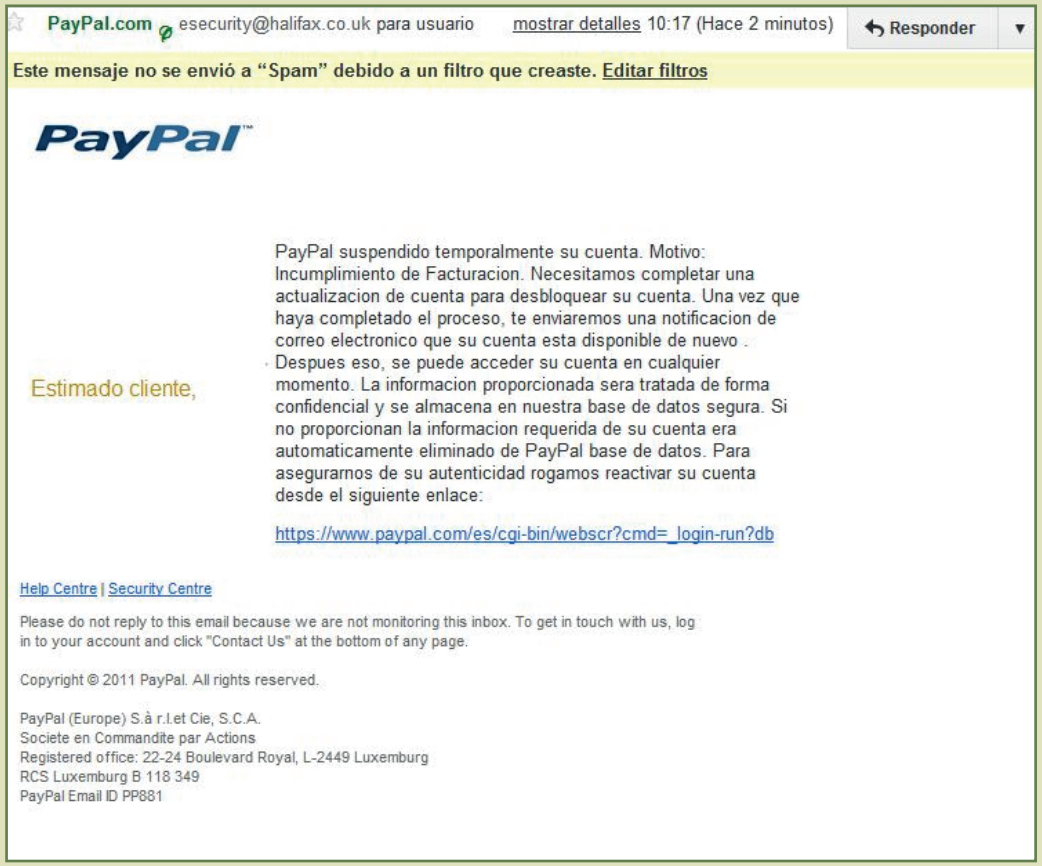
- En un servicio de pago a terceros, realizas una transferencia de dinero a una cuenta en línea y efectúas los pagos desde esa cuenta. De esta forma, no se expone la información de tu tarjeta de crédito o de tu cuenta bancaria en múltiples páginas webs.
- Es frecuente utilizar este tipo de servicios de pago de terceros para comprar productos a través de la web.
- Los sistemas de pago nunca te envían correos electrónicos, solicitándote información personal (contraseñas, datos bancarios). Este tipo de mensajes pueden ser estafas con robo o suplantación de identidad.

Phishing en los sistemas de pago

1 Actividad

Desarrollo

3. Después, el equipo facilitador proyectará en el aula la siguiente imagen:



PayPal.com esecurity@halifax.co.uk para usuario mostrar detalles 10:17 (Hace 2 minutos) Responder

Este mensaje no se envió a "Spam" debido a un filtro que creaste. Editar filtros

PayPal™

Estimado cliente,

PayPal suspendido temporalmente su cuenta. Motivo: Incumplimiento de Facturacion. Necesitamos completar una actualizacion de cuenta para desbloquear su cuenta. Una vez que haya completado el proceso, te enviaremos una notificacion de correo electronico que su cuenta esta disponible de nuevo . Despues eso, se puede acceder su cuenta en cualquier momento. La informacion proporcionada sera tratada de forma confidencial y se almacena en nuestra base de datos segura. Si no proporcionan la informacion requerida de su cuenta era automaticamente eliminado de PayPal base de datos. Para asegurarnos de su autenticidad rogamos reactivar su cuenta desde el siguiente enlace:

https://www.paypal.com/es/cgi-bin/webscr?cmd=_login-run?db

Help Centre | Security Centre

Please do not reply to this email because we are not monitoring this inbox. To get in touch with us, log in to your account and click "Contact Us" at the bottom of any page.

Copyright © 2011 PayPal. All rights reserved.

PayPal (Europe) S.à r.l.et Cie, S.C.A.
Societe en Commandite par Actions
Registered office: 22-24 Boulevard Royal, L-2449 Luxemburg
RCS Luxemburg B 118 349
PayPal Email ID PP881

Phishing en los sistemas de pago

1
Actividad

Desarrollo

3. A continuación, el equipo facilitador pedirá a las participantes que observen con detenimiento la imagen proyectada y se lanzará la siguiente pregunta para la reflexión individual:

    a) ¿Hay algo en el correo que os resulte extraño?
    b) ¿Hay algo raro en el mensaje además del lenguaje?

4. Cada participante recogerá su sospecha en un post-it de colores que irá leyendo en voz alta y colocando en un mural, mientras la facilitadora los irá agrupando por temáticas.

5. Al finalizar, las participantes, junto con el equipo facilitador entrarán en la página oficial de PayPal y leerán el apartado de Política de Privacidad.

6. El equipo facilitador mostrará un caso basado en un hecho real de tal manera que puedan construir un mensaje alternativo no fraudulento:

CASO BASADO EN UNA HISTORIA REAL

En este caso la ciberdelincuencia aprovechó la imagen de PayPal para intentar llevar a cabo un robo de cuentas bancarias. La imagen que se incluye en el mail recibido, se creería que es real si no fuera por la extraña dirección de correo. En el correo electrónico se argumentaba que debido a un incumplimiento de facturación se necesitaba los datos para desbloquear la cuenta. Para poder seguir con el procedimiento se pedía que se accediera a una dirección que parece de PayPal y que se notificara con otro correo el momento en que la cuenta estuviera reactivada. El correo daba todos los datos de PayPal y por supuesto estaba encabezado con el logo de la compañía, sin embargo, era un correo falso.

Recuerda que

- No utilices servicios de pago o realices transferencias bancarias en equipos públicos o compartidos o a través de dispositivos portátiles o teléfonos móviles cuando estén conectados a redes inalámbricas abiertas. La seguridad es poco fiable.
- Si compras en un sitio por primera vez y desconfías de quien vende, averigua si es miembro acreditado del sistema de pago. Por ejemplo, en PayPal, en la página "Comprobar los detalles del pago", antes de enviar el pago, puedes ver un vínculo de acreditación de quien vende junto a su dirección de correo electrónico. Además, la mayoría de las webs comerciales tienen foros en los que se incluyen comentarios y experiencias de quienes han comprado en ese sitio.
- En caso de recibir un correo fraudulento del supuesto servicio, notifícalo al auténtico proveedor.

Phishing bancario

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Tomar conciencia de las estrategias que utiliza la ciberdelincuencia cuando diseña un ataque de phishing "bancario".
- Aprender a prevenir y evitar ser víctima de phishing "bancario".

.

2
Actividad

Recursos y materiales


PC


Listado características phishing (punto 3 Desarrollo)


Papel


Bolígrafos

Tiempo

25 min.

Phishing en los sistemas de pago

2
Actividad

Desarrollo

1. Se dividirá a las participantes en 4 grupos, y cada grupo deberá diseñar el contenido de un correo de phishing: saludo, peticiones, enlaces y logos. Además, se definirá qué se quiere lograr con la estafa: Un beneficio económico, acceder a imágenes personales, robar contraseñas, etc.

2. A cada grupo se le dará una de las siguientes consignas:
    a) Es un grupo que se dedica a la estafa en la Red.
    b) El phishing va dirigido a mujeres y hombres.
    c) El phishing va dirigido a mujeres.
    d) El phishing va dirigido a hombres.

3. Para facilitar el trabajo de los grupos, el equipo facilitador entregará el listado de las características más comunes del phishing:

    Apariencia real: el objetivo de los correos electrónicos de phishing es aparentar que son reales y hacen todo lo posible por parecerse a la organización que suplantan. Para ello, utilizan la imagen gráfica (logotipos), datos de contacto, información de copyright y estilo en general similar a la auténtica. Hay veces que para lograr la confianza de la víctima, incluyen enlaces en el correo a páginas oficiales reales y, al mismo tiempo, enlaces a descargas de virus o páginas fraudulentas para robar información confidencial.

    Los **cebos más frecuentes** que utilizan este tipo de correos fraudulentos son avisos relativos a:

    - Cambios en la política de seguridad de la entidad imitada.
    - Problemas con la configuración de la contraseña.
    - Cambios en la normativa del banco.

Recuerda que

- No abras enlaces webs que vengan desde correos electrónicos que no conozcas.
- Ningún banco solicita datos personales a través del correo electrónico, ni mucho menos las claves de seguridad y acceso. Si recibieras un correo en este sentido, ponte en contacto con tu banco.
- Existen programas que permiten una protección contra correos no deseados o Spam. Asegúrate de que dispones de un programa antispam, de esta manera reducirás el riesgo de sufrir ataques de phishing.
- Si en la barra de direcciones aparece el símbolo de un candado cerrado, significa que es una página que incluye transacciones económicas seguras.

Phishing en los sistemas de pago

2
Actividad

Desarrollo

- Cierre incorrecto de la sesión de la persona usuaria.
- Promoción de nuevos productos.
- Falsas ofertas de empleo.
- Premios, loterías, regalos o ingresos económicos atractivos.
- Recomendaciones de seguridad para combatir el fraude.
- Desactivación del servicio.

Saludos no personalizados: Este tipo de correos están diseñados para ser enviados de forma masiva, por tanto, no se personaliza el saludo, sólo consta un "Estimada cliente/usuaria".

Enlaces disfrazados: Los enlaces en el correo electrónico son presentados de tal forma que aparentan ser auténticos. Usan engaños visuales para confundir a la persona usuaria como:

- Reemplazar caracteres (www.mibanco.com por www.mihanco.com).
- Ventanas emergentes o pop-ups.
- Uso de imágenes oficiales, mediante ventanas emergentes o pop-ups.

Rapidez en la respuesta: Los correos están redactados para provocar urgencia e inmediatez en la actuación ante las peticiones, argumentando la caducidad inmediata del servicio que se tenga contratado (ejemplos: "Tu cuenta debe ser actualizada", "tu cuenta está a punto de ser eliminada", "se detectó actividad sospechosa en tu cuenta").

Imágenes: El correo electrónico de phishing suele contener una imagen para facilitar caer en la trampa haciendo rápidamente clic en la misma y así redireccionando a la página falsa.

Errores ortográficos: Suelen ser textos con errores gramaticales o palabras cambiadas.

Phishing en los sistemas de pago

2
Actividad

Desarrollo

4. Al finalizar, cada grupo mostrará su trabajo y el resto identificará los elementos que permiten detectar el engaño. Se abrirá un debate sobre la seguridad en la Red y los posibles estereotipos de género que hayan podido surgir.

5. Para ilustrar el debate, el equipo facilitador leerá un caso basado en una historia real:

CASO BASADO EN UNA HISTORIA REAL

Una persona experimentada en Internet, y bastante desconfiada con respecto a sus datos personales y en especial de los bancarios, estuvo a punto de ser estafada mediante phishing. Recibió el clásico mail que simula a una entidad bancaria donde aparecía un enlace que apuntaba a una web falsa (http://www.caja-madrId.com), esta persona sabía perfectamente que se trataba de un phishing. Entró en la web fraudulenta para enseñar a su compañera de trabajo este tipo de estafas, y mostrarla que aunque era una copia perfecta de la página original no debía "picar" en este tipo de correos falsos. Al día siguiente fue a consultar su cuenta bancaria, y sin darse cuenta cogió la dirección grabada en el historial de Internet que correspondía a la web falsa, donde tecleó su usuaria y contraseña, facilitando así sus datos a los estafadores. Entonces se fijó que la conexión no era segura porque no aparecía el candado, e inmediatamente se fue a la web oficial de la entidad y cambio sus contraseñas de acceso.

Dominios parecidos

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Conocer las técnicas que se usan en las estafas de phishing mediante dominios parecidos para poder identificar este tipo de amenazas.
- Prevenir ser víctimas de este tipo de phishing.

3
Actividad

Recursos y materiales


PC


Papel


Bolígrafos

Tiempo

15 min.

Dominios parecidos

3
Actividad

Desarrollo

Los engaños visuales son las armas que suelen utilizar los grupos ciberdelincuentes para estafar, imitando los sitios legítimos. Un ejemplo clásico es la red social Facebook, ya que existen múltiples dominios similares, que sin embargo son páginas maliciosas (facebook-ims.com; facebooks.bz; gjfacebook.com; image-facebook.com; kfacebook.net).

1. Se trabajará en grupos de 3 mujeres como máximo y cada grupo elegirá una relatora.
2. Cada grupo intentará descubrir páginas de bancos o sitios webs conocidos que sean fraudulentos, utilizando la técnica de cambiar algunas letras de la dirección URL real.
3. Al finalizar la búsqueda, cada relatora pondrá en común los resultados encontrados, y borrará después el historial para que las páginas falsas desaparezcan del mismo.
4. El equipo facilitador ilustrará la dinámica con la lectura de dos noticias:

NOTICIAS

Según el Informe Trimestral PandaLabs (abril-junio) 2010, cada vez crece más el número de dominios con la palabra Facebook, pero sin embargo son páginas fraudulentas. En la mayoría de los casos, cuando accedes a alguna de estas direcciones web (URL) se muestra una interfaz similar a la del auténtico Facebook para obtener tus claves de acceso, y después te redirigen a la página real para no levantar sospechas. Un ejemplo seria: http://facebooks.bz.
Otro tipo de engaño muy habitual es el de imitar sitios reales, como el canal de video YouTube, o el de ofrecernos vídeos que al tratar de visualizarlos nos solicitan la instalación de un código (códec) que finalmente se trata de un virus.

Recuerda que

- Asegúrate de entrar directamente a la URL (dirección web) de la entidad a la que deseas acceder escribiéndola correctamente en el navegador de tu ordenador asegurándote de la legitimidad del sitio web.
- Si accedes a una entidad mediante un enlace (link), asegúrate de que estás en la página oficial y no en una web falsa que la suplanta. Para ello, debes comprobar que la dirección web tiene las letras "https" (la "s" corresponde a "seguro") en lugar de HTTP.

La Administración, víctima de ataques de phishing

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Detectar posibles situaciones de phishing, incluido el que utiliza a las Administraciones Públicas como cebo.
- Prevenir a ser víctimas de este tipo de phishing.
- Decidir que hacer en caso de detectar en el correo electrónico una amenaza de este tipo de phishing.

4

Actividad

Recursos y materiales


Tarjetas


Papel


Bolígrafos

Tiempo

20 min.

La Administración, víctima de ataques de phishing

4
Actividad

Recursos y materiales

Tarjetas para recortar

A

Mensaje de correo electrónico para descargar actualizaciones o certificados digitales (firma electrónica) de una página web.

B

Mensaje de correo electrónico con faltas de ortografía y gramaticalmente incorrecto debido al uso de traductores automáticos.

C

Mensaje de correo electrónico de la Agencia Tributaria.

D

Mensaje de correo electrónico con amenazas si no haces lo que te indica.

E

Mensaje de correo electrónico que te remite a la web de tu banco a través de un enlace.

F

Mensaje de correo electrónico en el que figuran direcciones webs con caracteres o fórmulas poco comunes.

G

Mensaje de correo electrónico encadenado para reenviar a 10 personas.

H

Mensaje de correo electrónico en el que se solicitan datos personales y datos bancarios para actualizar las bases de datos.

La Administración, víctima de ataques de phishing

4
Actividad

Desarrollo

1. Se trabajará en grupos de 4 mujeres como máximo y cada grupo elegirá a una relatora.
2. El equipo facilitador entregará a cada grupo un juego completo de tarjetas.
3. Una vez leídas las tarjetas por parte de todos los grupos, se abrirá una ronda de preguntas por si algún texto presenta dificultades entre las participantes.
4. Cada grupo deberá identificar qué mensajes son sospechosos de phishing y cuáles no lo son, elaborando una breve justificación de su respuesta.
5. Al finalizar, todos los grupos expondrán sus conclusiones.
6. Nota para el equipo facilitador: SÍ son sospechosas de phishing: b, d, e, f, h / NO son sospechosas de phishing: a, c, g
7. A continuación, el equipo facilitador expondrá un caso basado en un hecho real que sucedió con la Agencia Tributaria:

CASO BASADO EN UNA HISTORIA REAL

La Agencia Tributaria no se libra de los ataque de phishing. El atractivo gancho del fraude se encuentra en el propio asunto del correo electrónico: "Datos a conocer sobre el reembolso del impuesto para el año 2012". En el cuerpo del texto se puede leer un texto con extraña redacción: "Después del último cálculo sobre las actividades fiscales, hemos decidido que le corresponde un reembolso del impuesto en valor de 384,56 €. Para recibir dicho reembolso, completar y mandar el formulario del impuesto a devolver". Después se mostraba un enlace en el que se solicitaban datos personales como el número de DNI, NIF o pasaporte, la fecha de nacimiento así como los números y claves de una tarjeta de crédito.

Recuerda que

- Debes prestar atención al contenido de los mensajes de correo electrónico que recibes en tu bandeja de entrada y ante la menor sospecha eliminarlo.
- Si recibes un mensaje sospechoso desde una Administración Pública, ponte en contacto telefónicamente con la institución antes de facilitar los datos personales que te solicitan.

Fraude en la Red / Phishing

Consejos y buenas prácticas

Recomendaciones para prevenir ataques de phishing:

- No abras enlaces que vienen en correos electrónicos que no conoces: si tienes que verificar o suministrar algún tipo de información personal o financiera, proporciónala directamente a través del sitio web de la entidad, y se tú la persona que escriba la dirección web (URL) en la barra de navegación.
- Recuerda que cuando tengas que facilitar información confidencial (tarjetas de crédito, seguridad social, claves bancarias), ninguna entidad te lo va a solicitar por mail.
- Existen indicadores que te pueden dar pistas de la veracidad del sitio web:
  - -La dirección web comienza con las letras "https" (la "s" corresponde a "seguro") en lugar de HTTP.
  - -Barra de direcciones del navegador de color verde, aunque esto varía según el navegador que se utilice.
  - -Barra de direcciones con símbolo de candado cerrado para páginas que incluyan transacciones económicas.
- Intenta mantener activos los filtros de correo no deseado (antispam) que ofrecen los servicios de correo electrónico para reducir el riesgo de sufrir ataques de phishing.
- Utiliza un antivirus y actualízalo con frecuencia.
- En el caso de que tengas que enviar obligatoriamente información confidencial (cuentas bancarias, tarjetas de crédito o claves de acceso), procura dividir la información en dos correos por si alguno es interceptado por hackers.
- Extrema la precaución a la hora de descargarte los archivos que te envíen por correo electrónico ya que pueden contener virus u otro programa malicioso que reduzcan el nivel de seguridad de tu ordenador. Antes de descargar el fichero, analízalo con un antivirus.
- Vigila los movimientos de tu cuenta bancaria regularmente, no se suelen defraudar grandes cantidades de dinero, sino más bien pequeños movimientos difíciles de detectar.

Consejos si eres víctima de un fraude de phishing:

- Si sospechas que has sido víctima del phishing, cambia inmediatamente todas tus contra señas y ponte en contacto con la entidad bancaria o empresa a la que supuestamente han suplantado para avisarles de lo acontecido.
- Ponte en contacto[1] con la **Brigada de Investigación Tecnológica** de la Policía Nacional o el **Grupo de Delitos Telemáticos** de la Guardia Civil y formula la denuncia.

Fraude en la Red / Phishing

Datos de interés

Phishing: Fraude consistente en el robo de información personal o financiera mediante ingeniería social simulando una identidad de terceros.

Las identidades o los servicios[2] más frecuentes que se simulan para los ataques de phishing son:

- Entidades bancarias.
- Plataformas de pago online (PayPal, Mastercard, Visa, etc.).
- Redes sociales (Facebook, Twitter, Tuenti, Instagram, Linkedin, etc.).
- Páginas de compra/venta y subastas (Amazon, eBay, etc.).
- Juegos on-line.
- Soporte técnico y de ayuda (helpdesk) de empresas y servicios (Outlook, Yahoo!, Apple, Gmail, etc.).
- Servicios de almacenamiento en la nube (Google Drive, Dropbox, etc.).
- Servicios o empresas públicas.
- Servicios de mensajería.
- Falsas ofertas de empleo.

Fraude en la Red / Phishing

Evaluación

Para reforzar los contenidos aprendidos, piensa si son verdaderas o falsas las siguientes afirmaciones:

Como mantengo actualizado mi antivirus, no corro el riesgo de sufrir phishing	*verdadero*	*falso*
Para evitar ser víctima de phishing bancario escribe directamente la dirección web en la barra de direcciones (URL)	*verdadero*	*falso*
Mi banco puede solicitarme mis claves personales a través del mail que yo les he facilitado	*verdadero*	*falso*
Es fácil detectar un ataque de phishing, sólo es cuestión de sentido común	*verdadero*	*falso*
Entre los trucos que utiliza la ciberdelincuencia para estafar mediante phishing está la petición de pronta respuesta por parte de quien lo recibe	*verdadero*	*falso*

Fraude en la Red / Phishing

Palabras Clave

Referencias

[1] La Brigada de Investigación Tecnológica está encuadrada en la Unidad de Delincuencia Económica y Fiscal (UDEF) que es el órgano de la Dirección General de la Policía y de la Guardia Civil encargado de la investigación y persecución de las actividades delictivas, de ámbito nacional e internacional, en materia de delincuencia económica y fiscal, así como la coordinación operativa y apoyo técnico a las respectivas Unidades Territoriales.

- Brigada de Investigación Tecnológica de la Policía Nacional: http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html
- Grupo de Delitos Telemáticos de la Guardia Civil: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

[2] Información elaborada a partir de la documentación contenida en el portal de la Oficina de Seguiridad del Internauta (2014) *"Aprendiendo a identificar los 10 phishing más utilizados por ciberdelincuentes*.
Disponible en: http://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen
[Consultado 16/07/2014]

Materiales didácticos **"Confianza y seguridad de las mujeres en la Red"**

Correo no deseado / Spam

Actividades didácticas

Objetivos generales

Al acabar las actividades, las participantes serán capaces de:

- Reconocer los tipos de correo no deseado (spam) que recibimos en nuestras cuentas de correo electrónico y las medidas de prevención.
- Establecer los pasos a seguir cuando recibimos correo no deseado (spam).
- Saber qué hacer si nuestra cuenta personal queda clasificada como emisora de correo no deseado (spam).

¿Dónde sucede?

Correo electrónico

SMS

1 Actividad
Saturan mi cuenta de correo

2 Actividad
¿Quién tiene mi correo?

MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
SECRETARÍA DE ESTADO DE SERVICIOS SOCIALES E IGUALDAD
INSTITUTO DE LA MUJER Y PARA LA IGUALDAD DE OPORTUNIDADES
Unión Europea
Fondo Social Europeo

Saturan mi cuenta de correo

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Reconocer las consecuencias que supone el envío de correos masivos.
- Tomar conciencia de los riesgos que suponen los archivos adjuntos en los correos no deseados (spam).

1
Actividad

Recursos y materiales

Cuadernillo Correo no deseado / Spam

Tiempo

10 min.

Saturan mi cuenta de correo

1
Actividad

Desarrollo

1. El equipo facilitador leerá el siguiente caso y lanzará unas preguntas para la reflexión colectiva, conduciendo el debate hacia las posibles estrategias y acciones que eviten, en la medida de lo posible, la recepción de spam en nuestras cuentas de correo electrónico:

CASO

Una asociación de mujeres enviaba todas sus comunicaciones a sus socias a través del correo electrónico. Un día, una de las socias comprobó que los correos que recibía de la asociación, iban a parar a la carpeta de "Correo no deseado". En ese momento la asociación no entendía bien porque sus correos eran catalogados como Spam (correo basura o no deseado). Tiempo atrás, esta asociación había estado realizando campañas a través de correo electrónico para captar y fidelizar socias, pero el resultado fue que el 80% de sus correos fueran clasificados como Spam y no llegaron a sus destinatarias.

2. Preguntas para dinamizar el debate grupal:

a) ¿Recibís habitualmente correos que se quedan guardados en la carpeta "No deseados"?
b) ¿Conocéis los pasos a seguir para indicar en el correo electrónico que determinadas direcciones sean considera das como spam?
c) ¿Alguna vez habéis realizado envíos de correo masivos a vuestros contactos?

Saturan mi cuenta de correo

1
Actividad

Recuerda que

- Los spam son mensajes de correo electrónico no deseados ni solicitados, que con frecuencia tienen fines publicitarios y comerciales. En la mayoría de las ocasiones son enviados por personas desconocidas de forma masiva, realizando lo que se conoce como "spamming".
- Aunque el correo electrónico suele ser la vía más utilizada para enviar spam, los teléfonos móviles son también objetivo de estos mensajes basura. Si quieres evitar que tus envíos de boletines o newsletter sean catalogados como spam, sigue estos consejos:
  - Mantén actualizada la base de datos de e-mails para evitar envíos innecesarios, eliminando correos incorrectos.
  - Si haces envíos masivos envía a tus suscriptoras un mensaje en el que solicitas confirmación de que desean recibir tus correos y diseña un sistema sencillo y rápido para facilitar la baja en la suscripción
  - Presta atención al contenido del asunto y cuerpo del correo para evitar filtros antispam (no escribas en mayúsculas el asunto, evita expresiones exageradas, signos de admiración y frases redundantes).
  - Evita incorporar imágenes, ya que en muchos correos electrónicos no se pueden visualizar.
  - Da seguimiento al envío de tus correos para ver si hay caída en los ratios de entrega.
  - Recuerda que el envío masivo e indiscriminado de correos a personas que no lo han solicitado, puede tener un efecto negativo para ti en caso de que tu cuenta quede catalogada en una lista negra (blacklist), dañando tu imagen y pudiendo acarrearte incluso problemas legales.
- En caso de que tú seas la receptora de correos masivos:
  - Si hay correos que te interesan y los dejas de recibir, es posible que se estén archivando automáticamente en la carpeta de spam. Búscalos allí y avisa a la persona o institución emisora para que corrija la situación.
  - Si recibes correos no deseados puedes catalogarlos tú directamente como spam desde tu proveedor de correo electrónico (Outlook, Webmail, etc.) de esta manera ya no volverás a visualizarlos en siguientes envíos.

Saturan mi cuenta de correo

1
Actividad

Recuerda que

- Entre las consecuencias que supone la recepción y emisión de spam están:
  - Pérdida de productividad: Tener que borrar correos que no son de nuestro interés supone emplear tiempo.
  - Consumo de espacio: Utiliza tu ancho de banda, reduce el espacio de tu disco y satura tu correo.
  - Pérdida de información valiosa: Hay veces que dada la cantidad de correos que recibes, puedes eliminar por error correos que son de tu interés.
  - Sufrir un virus informático: Cuando el correo spam lleva un virus asociado puede llegar a atacar tu equipo.
  - Ser catalogada como remitente de spam: Tu cuenta de correo pasa a ser clasificada como cuenta spam, y serán bloqueados tus correos por muchos servidores.

¿Quién tiene mi correo?

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Comprobar en la web si nuestros correos electrónicos son accesibles para quienes generan spam.
- Tomar conciencia de los riesgos asociados a hacer pública nuestra dirección de correo electrónico.

2
Actividad

Recursos y materiales

PC

Tiempo

20 min.

¿Quién tiene mi correo?

2
Actividad

Desarrollo

1. Cada participante entrará de manera individual en: www.google.es y tendrá que escribir en la barra de búsqueda del navegador, el nombre de su cuenta de correo personal y comprobar qué sucede después. Si se tiene más de una cuenta de correo, repetir el ejercicio con todas.
2. En caso de que obtengan algún resultado, entrarán en las páginas propuestas por el buscador, con el fin de saber los contenidos a los que se vinculan sus correos electrónicos en la Red y responderán individualmente a las siguientes preguntas para compartirlo después en plenario:

    a) En caso de tener varias cuentas de correo, ¿has detectado diferencias en los resultados de la búsqueda?
    b) ¿Esperabas obtener esos resultados?
    c) ¿Qué es lo que más te ha sorprendido al comprobar las páginas a las que te redireccionaba el buscador?
    d) ¿Por qué crees que a veces resulta sencillo que otras personas obtengan nuestras cuentas de correo para enviarnos spam?, ¿cómo crees que se puede evitar?

Recuerda que

Las técnicas que utilizan las personas que se dedican profesionalmente a enviar spam son variadas[1]:

- Bases de datos: La venta o compra de ficheros con datos personales, tanto de particulares como de empresas, sin consentimiento de las personas interesadas, es una práctica ilegal.
- Uso de robots: Programas automáticos que rastrean Internet en busca de direcciones de correos electrónicos públicos, grupos de noticias, weblogs, etc.
- Generan automáticamente direcciones de correo electrónico pertenecientes a un dominio específico, y envían mensajes a las mismas hasta averiguar cuáles son las correctas, por ejemplo, mail@dominio.es o webmaster@dominio.es

Correo no deseado / Spam

Consejos y buenas prácticas

Recomendaciones para combatir y prevenir el spam[2]:

- Antes de facilitar tu dirección de correo electrónico, piensa bien quién te está solicitando esta información y solamente facilítala cuando sean personas o empresas que te generen confianza.
- Crea varias cuentas de correo electrónico. Utiliza una dirección exclusivamente si necesitas facilitar la dirección y no tienes confianza en la fuente solicitante, y otra dirección personal que sea conocida únicamente por tus amistades, familiares y personas o instituciones conocidas y de confianza.
- Recuerda que los robots emisores de spam compilan listas de direcciones de correo electrónico mediante la combinación de nombres, palabras y números obvios, así que procura cear direcciones de correo que resulten complicadas de adivinar, incluyendo algo más que tú nombre y apellidos.
- Cuando envíes correos en los que aparezcan muchas direcciones, utiliza la copia oculta (CDO). Asimismo, si reenvías un correo, elimina las direcciones del resto de personas destinatarias.
- Si necesitas facilitar la dirección de correo en alguna Web que te genere desconfianza, escribe 'at' o 'arroba' en lugar de @.
- Lee detenidamente las Políticas de Privacidad y las Condiciones de Cancelación de tus suscripciones, y no dudes en ejercer tus derechos de acceso y cancelación sobre tus datos personales cuando quieras dejar de recibir sus notificaciones.
- No contestes correos de personas desconocidas que no esperas recibir, ni hagas clic en los vínculos ni abras los archivos adjuntos. Incluso si quien te lo manda te inspira confianza, verifica que no están infectados antes de abrir los archivos; ¡puede ser un virus!.
- Utiliza filtros de correo. Los programas de gestión de correo electrónico y muchas páginas Web ofrecen la posibilidad de activar filtros que separan el correo deseado del spam.
- Mantén al día tú equipo con programas antivirus, software antispam, actualizaciones y parches que corrigen los problemas detectados en los programas de tu equipo. Además, es muy recomendable la instalación de cortafuegos para monitorizar lo que ocurre en el ordenador.

Correo no deseado / Spam

Datos de interés

Spam: Mensajes de correo electrónico no deseados, ni solicitados, que con frecuencia tienen fines publicitarios y comerciales.

¿Cómo son estos mensajes?

- La dirección que aparece como remitente del mensaje no suele ser conocida y la mayoría de las veces es falsa.
- El asunto del mensaje suele ser comercial y atractivo.
- El spam puede buscar desde publicidad hasta actividades ilegales (fraudes económicos). Así, son múltiples y variados los tipos de mensajes: Anuncios de sitios web, productos milagro, ofertas inmobiliarias, casinos, loterías y apuestas, servicios de alojamientos gratuitos en la nube, ofertas de trabajo con altas remuneraciones, listados de productos con precios en promoción, ayuda espiritual, etc.
- La mayor parte del correo no deseado está escrito en inglés y se origina en Estados Unidos o Asia, pero empieza a ser común también en castellano.

Regulación legal

Las leyes que regulan el envío no solicitado de comunicaciones comerciales electrónicas son:

- Ley 34/2002 de Servicios de la Sociedad de la Información (LSSI) (artículos 19, 20, 21, 22, 38 y 43).
- Ley 32/2003 General de Telecomunicaciones (LGT) (artículos 38, 53.z, 54.r, 58.b y Disposición Adicional Novena de la Ley 32/2003).
- Ley 15/1999 de Protección de Datos de Carácter Personal (artículos 3.a, 4, 5, 6, 37.1.n y 44 y 45).

La Ley de Servicios de la Sociedad de la Información (LSSI) en su artículo 21.1 prohíbe de forma expresa el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por las personas destinatarias de las mismas.

Correo no deseado / Spam

Datos de interés

La Directiva sobre Privacidad en las Telecomunicaciones de 12 de julio de 2002 (Directiva 58/2002/CE) transpuesta en la Ley 32/2003 General de Telecomunicaciones que modifica varios artículos de la Ley 34/2002, introdujo en el conjunto de la Unión Europea el principio de "opt in", es decir, el consentimiento previo de la persona para el envío de correo electrónico con fines comerciales. De este modo, cualquier envío con fines de publicidad queda supeditado a la prestación del consentimiento, salvo que exista una relación contractual previa y la persona no manifieste su voluntad en contra[3].

Además la LSSI establece que la Agencia Española de Protección de Datos es responsable para imponer las sanciones pertinentes en el caso de que se cometan infracciones por el envío masivo de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o equivalentes.

Correo no deseado / Spam

Evaluación

Para reforzar los contenidos aprendidos, piensa si son verdaderas o falsas las siguientes afirmaciones:

Cuando recibo spam en mi correo, tengo que contestar para solicitar que me den de baja	*verdadero*	*falso*
Es conveniente contar con un software antispam en nuestro equipo informático	*verdadero*	*falso*
Son más vulnerables de cara al spam las cuentas de correo que se componen de nuestros nombres y apellidos	*verdadero*	*falso*
Cuando me solicitan mi cuenta de correo es conveniente enmascararla, por ejemplo poner: "lauraarrobayahoopuntoes" en vez de laura@yahoo.es	*verdadero*	*falso*
Es seguro publicar mi dirección de correo electrónico en chats y foros de acceso público	*verdadero*	*falso*

Correo no deseado / Spam

Palabras Clave

Referencias

[1] Información elaborada a partir de la documentación contenida en el portal web de Panda Security *"Spam: mensajes de correo no solicitados"*.
Disponible en: http://www.pandasecurity.com/spain/enterprise/security-info/types-malware/Spam/
[Consultado: 16/07/2014]

[2] Información elaborada a partir de la documentación contenida en el portal web de la Agencia Española de Protección de Datos, *"Decálogo de recomendaciones para combatir el Spam"*.
Disponible en : http://goo.gl/NWmLwI
[Consultado 16/07/2014]

[3] *Ibíd*., p.3

Bulo / Hoax

Actividades didácticas

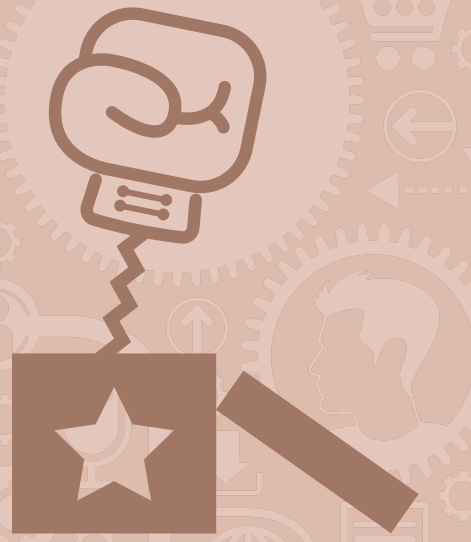
Objetivos generales

Al acabar las actividades, las participantes serán capaces de:

- Reconocer las características que definen y diferencian un bulo de una noticia veraz.
- Prevenir la reproducción de cadenas masivas de bulos (bromas, engaños) tanto en la Red como en dispositivos de mensajería instantánea.

¿Dónde sucede?

Correo electrónico | Redes sociales | Foros | Mensajería instantánea



1 Actividad
"Más vale prevenir..."

2 Actividad
"Rumores, rumores..."

3 Actividad
Hagamos nuestro propio bulo

MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
SECRETARÍA DE ESTADO DE SERVICIOS SOCIALES E IGUALDAD
INSTITUTO DE LA MUJER Y PARA LA IGUALDAD DE OPORTUNIDADES
Unión Europea
Fondo Social Europeo

“Más vale prevenir...”

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Reflexionar sobre la importancia de contrastar la información que obtenemos de Internet.

.

1
Actividad

Recursos y materiales

PC

Tiempo

15 min.

"Más vale prevenir..."

1
Actividad

Desarrollo

1. Se trabajará en grupos de 3 mujeres como máximo y cada grupo elegirá una relatora.
2. El equipo facilitador dará la siguiente consigna:

   "Imagina que una buena amiga te ha llamado para contarte que ayer, mientras se estaba duchando, se ha encontrado un pequeño bulto en el pecho izquierdo. Está muy asustada y te ha pedido que busques información en Internet para saber qué le pasa."

3. Tendrán 10 minutos para buscar información sobre el caso de la amiga, debiendo anotar lo siguiente:

   a) Dónde localizo la Información. URL (sólo dominio)
   b) ¿Qué puede estar pasando?
   c) ¿Qué puede hacer mi amiga?

4. Una vez que haya pasado el tiempo estipulado, las relatoras irán exponiendo los resultados de su grupo.
5. En paralelo, el equipo facilitador irá anotando en la pizarra o papelógrafo las coincidencias y las diferencias que han ido surgiendo en la dinámica, poniendo de manifiesto la importancia de contrastar la información que encontramos.

Recuerda que

- Los bulos ("hoax"- "engaño" en inglés-) son noticias falsas que circulan de manera masiva a través de la Red. Son similares a lo que conocemos coloquialmente como "rumores", que muchas veces se convierten en correo no deseado (Spam).
- Es necesario asegurarnos de la fiabilidad de las webs que visitamos, procurando consultar páginas oficiales y de confianza.
- Las mujeres somos las que nos ocupamos mayoritariamente de los cuidados y la salud de las personas que nos rodean, siendo las que principalmente buscamos información sobre salud en Internet. Si te preocupa algo en relación a tu salud o de las personas que están a tu cargo, puedes buscar información en las webs de los servicios de salud de tu comunidad y/o acudir a tu centro de atención primaria para que te orienten.

"Rumores, rumores..."

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Identificar y reconocer las características que nos hacen pensar que estamos ante un bulo.
- Saber qué hacer en caso de sospechar que se ha recibido un bulo.

2 Actividad

Recursos y materiales

Textos con los 4 bulos

Papel

Bolígrafos

Tiempo

20 min.

"Rumores, rumores..."

2
Actividad

Desarrollo

1. Se trabajará en grupos de 5 mujeres y cada grupo elegirá una relatora.
2. Se entregará aleatoriamente a cada grupo uno de los bulos seleccionados que han circulado por Internet, para que analicen qué características tiene la noticia que les hacen pensar que se trata de un bulo. Después tendrán que elaborar un listado de claves y pautas para reconocerlos.
3. En plenario cada grupo expondrá el listado elaborado con las principales claves propuestas.

BULO 1

Asunto: ALERTA DE VIRUS!!!!!!!!!! IMPORTANTE

ATENCIÓN!!! Durante las próximas semanas esté atento y ponga cuidado en no abrir "La Caja de los Truenos" independientemente de quien se lo haya enviado. POR FAVOR HAGA CIRCULAR ESTO ENTRE TODA SU FAMILIA Y AMISTADES. NO ABRIR la " La Caja de los Truenos ". Es un virus que puede borrar todo lo que contiene su disco duro "C". Le llegará como un e-mail proveniente de una persona familiar. Envíe este e-mail a todos los contactos de su libreta de direcciones. Es preferible recibir 25 veces este mensaje que no recibirlo del todo. Si recibe un e-mail llamado "Los Truenos.Com" no lo abra!. Bórrelo inmediatamente! Este virus suprime toda la librería dinámica (.dll files) de su computador.
POR FAVOR HAGA CIRCULAR ESTE MENSAJE!

Recuerda que

Existen una serie de pautas que te pueden ayudar a reconocer los bulos en Internet:

- Son anónimos y no incluyen la fecha de publicación para durar el máximo tiempo posible circulando en la Red.
- Están escritos en un castellano neutro para facilitar la difusión, aunque pueden contener errores de ortografía o gramaticales evidentes ya que a veces se utilizan traductores automáticos.
- Contienen una petición de reenvío masivo y presagian grandes desgracias si no lo haces o, por el contrario, gran felicidad si lo haces.
- Suelen ser mensajes enviados por alguno de nuestros contactos que ha caído en la trampa de la cadena, ya que contienen un "gancho" para atraer la atención de quien lo lee.
- Si el contenido es sobre un falso virus, alertarán sobre una amenaza que ningún antivirus detecta.

"Rumores, rumores..."

2
Actividad

Desarrollo

BULO 2

Asunto: URGENTEEEEEEEEEEEEEEEEEEE!!!!!

¡¡Para todos las madres!! La Compañía JOTA está pidiendo que devuelvan toda la comida de bebé que contenga banana y que expire en el 2013 porque puede tener vidrio!! Por favor, copia esto y pégalo en tu muro para seguridad de todos los bebes... código 7613033089 73,... si no eres madre por favor hazlo también, podrías salvar a alguien!

BULO 3

Asunto: ¡¡ATENCIÓN MUJERES!! ENVIADO POR LA DRA. CUATRO MÉDICA BIOMOLECULAR

No dejen de pasar este mensaje a sus esposas, hijas, amigas, hijas y colegas de trabajo. La Dra. CUATRO emitió un alerta para labiales conteniendo una sustancia cancerígena. Recientemente la marca 'X' disminuyo los precios de 36€ a 5€. Por qué? Porque contenía esa sustancia.

Después de hacer un test en labiales, fue constatado en los labiales de la marca X mayor nivel de la sustancia. Atención para esos labiales que supuestamente tienen una fijación mayor. Si tu labial se fija mas, es debido al alto nivel de la sustancia. Este es un test que puedes hacer: 1. Coloca algún labial en tu mano; 2. Con un anillo de oro pásalo sobre este labial; 3. Si el color del labial cambia para negro, entonces sabes que contiene esa sustancia.

Por favor, envía esta información para todas tus amigas.

Recuerda que

Hace unos años los bulos se propagaban casi exclusivamente por correo, pero ahora es común encontrarlos en los programas de mensajería instantánea y en las redes sociales. La facilidad de combinar texto e imágenes aumenta su impacto.

Ignora las amenazas de virus que te lleguen por correo electrónico, es muy posible que sea un bulo. Si por el contrario haces lo que indican abriendo archivos adjuntos, eliminando archivos de tu PC o pinchando en enlaces asociados, puede que infectes tu equipo.

"Rumores, rumores..."

2
Actividad

Desarrollo

BULO 4

Asunto: Uso correcto del papel de envolver alimentos

Este papel se utiliza ampliamente en los alimentos, pero en la mayoría de los casos se usa incorrectamente. Las usuarias tienden a poner la cara brillante hacia fuera, ya que deja el aspecto del plato más bonito. El lado más brillante es así porque se hace un pulido para crear una barrera y evitar el contacto directo con los alimentos. Debemos poner el lado brillante hacia los alimentos y el lado no brillante hacia fuera. Esta protección, el pulido, no está en ambos lados ya que es un proceso costoso que haría que la comercialización del papel fuera inviable. Pero es altamente tóxico y responsable de complicaciones generales en el funcionamiento de nuestro cuerpo. PROTÉGETE A TI Y A TU FAMILIA

Hagamos nuestro propio bulo

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Tomar conciencia de la facilidad con que se pueden generar y propagar bulos en la Red y sus consecuencias.

3
Actividad

Recursos y materiales


PC


Papel continuo / cartulina


Revistas


Tijeras


Pegamento


Rotuladores

Tiempo

20 min.

Hagamos nuestro propio bulo

3
Actividad

Desarrollo

1. Se trabajará en grupos de 5 mujeres como máximo y cada grupo elegirá a una relatora.

2. Cada grupo debe elegir un tema para construir su propio bulo: Falsas advertencias de virus, invención sobre una marca concreta, cadena solidaria de ayuda o de la suerte, un método milagroso para perder peso o ganar grandes sumas de dinero, etc. Se podrá construir el bulo a través de la imaginación de las participantes, pudiendo utilizar información que encuentren en la Red. La consigna es que debe parecer lo más real posible. Para conseguirlo deberán:

    a) Escribir el bulo en el papelógrafo utilizando los elementos distintivos respecto a su redacción.
    b) Acompañarlo si lo desean con una imagen que encuentren en las revistas.

4. Una vez finalizados los trabajos, se colgarán los papelógrafos a modo de murales y las relatoras leerán el bulo de su grupo.

5. El resto de participantes deberá identificar qué elementos hacen de esa historia un bulo.

6. Por último, el equipo facilitador leerá el siguiente bulo relacionado con la aplicación "WhatsApp":

Recuerda que

Los bulos se aprovechan de la sensibilidad, el interés económico, la superstición o creencias de las personas. Buscan confundir, manipular o incidir en la opinión pública.

Cuando reenvías correos en cadena, estas colaborando con quienes se dedican a enviar profesionalmente (spammers) correo no deseado (spam) y a configurar una base de datos con miles de direcciones de correo electrónico para mandar publicidad o archivos de contenido malintencionado (malware).

Consecuencias de los bulos

- Atentan directamente contra la credibilidad de Internet, siendo actualmente la primera herramienta de búsqueda de información para la población.
- Hacen perder valor a los mensajes de personas o instituciones verídicas que recibimos a través de la Red.

Hagamos nuestro propio bulo

3
Actividad

Desarrollo

CASO DE BULO BASADO EN UNA NOTICIA REAL

Asunto: Mensajería instantánea pasará a ser de pago!
"Hola, soy Germán X, director de Mensajería instantánea. Este mensaje es para informarles a todas nuestras personas usuarias de que sólo nos quedan 530 cuentas disponibles para nuevos teléfonos, y que nuestros servidores han estado recientemente muy congestionados, por lo que estamos pidiendo su ayuda para solucionar este problema. Necesitamos que las personas usuarias activas reenvíen este mensaje a cada una de las personas de su lista de contactos a fin de confirmar quienes utilizan Mensajería instantánea, si usted no envía este mensaje a todos sus contactos de Mensajería instantánea, entonces su cuenta permanecerá inactiva con la consecuencia de perder todos sus contactos. El símbolo de actualización automática en su teléfono (SmartPhone), aparecerá con la transmisión de este mensaje. Su SmartPhone se actualizará dentro de las 24 horas siguientes, contará con un nuevo diseño, un nuevo color para el chat y su icono pasará de ser verde a azul. Mensajería instantánea pasará a tarifa de pago a menos que lo uses frecuente. Mañana empiezan a cobrar los mensajes por Mensajería instantánea a 0,37 céntimos. Reenvía este mensaje a más de 9 personas de tus contactos y te será gratuito de por vida"

Recuerda que

- Reducen el ancho de banda y saturan los servidores y la bandeja de entrada de tus contactos.
- Si reenvías este tipo de mensajes contribuyes a generar correo basura (spam), y a difundir publicidad no deseada .
- En ocasiones persiguen infectar los equipos, averiguar datos personales o contraseñas de quienes continúan con la cadena, dando paso a la comisión de estafas o robos.

Cuando dudes sobre la veracidad de un mensaje que te genere sospecha, recuerda lo poco que te ha costado crear tu propio bulo.

Bulo / Hoax

Consejos y buenas prácticas

Para evitar caer en los bulos que circulan por la Red, el mejor sistema es que hagas una lectura reflexiva y crítica de los mensajes que recibes. Además, debes tener en cuenta algunas recomendaciones como:

- Confirma y contrasta la veracidad de la información que recibes antes de enviarla a tus contactos.
- Nunca reenvíes un correo en cadena que contenga información sospechosa de ser falsa, simplemente bórralo.
- Comprueba que los correos y mensajes que recibes como "historias reales" y que apelan a tu compasión y solidaridad, estén fechados y con remitente identificable. Si no es así, suelen ser falsos.
- Nunca hagas caso de mensajes en cadena que te indiquen que modifiques archivos de tu ordenador, aunque vengan de alguien que conoces.
- No abras los archivos adjuntos que incluyan los mensajes en cadena, pueden contener virus que infecten tus equipos.
- Nunca facilites tus contraseñas, claves de acceso o número de teléfono móvil a personas o entidades desconocidas.

Bulo / Hoax

Datos de interés

Bulos: Noticias faltas que circulan de forma masiva a través de la Red.

La "Asociación de Internautas" realizó un estudio[1] en 2012, concluyendo que el 97,29% de quienes utilizan Internet han recibido una cadena de correos de autoría anónima, con información alarmista sobre un servicio o producto con la petición de ser reenviado. Los contenidos suelen tratar de temas relacionados con salud y alimentación (32,5%), tecnología (13%) y economía (11%). Sobre la veracidad de los contenidos en las cadenas de correos, al 88% de internautas no le parece creíble ese contenido, dando credibilidad al mismo el 9% . El 83,26% confía igual en los contenidos leídos en Internet que en los medios convencionales. El 14,48% sólo se fía de los convencionales.

Nota para el equipo facilitador: Podría reflexionarse en plenario que todavía un 9% de las personas encuestadas por la "Asociación de Internautas" otorga veracidad a las cadenas de emails con contenido alarmista.

Bulo / Hoax

Evaluación

Para reforzar los contenidos aprendidos, piensa si son verdaderas o falsas las siguientes afirmaciones:

Las noticias que van acompañadas de imágenes y datos estadísticos son siempre ciertas	*verdadero*	*falso*
Las cadenas masivas de correo tienen como objetivo recabar direcciones electrónicas para el uso de spammers	*verdadero*	*falso*
Los mensajes alertando sobre virus y malware me ayudan a mantener seguro mi equipo si sigo las instrucciones que indican para eliminarlos	*verdadero*	*falso*
La mejor opción para reenviar mensajes es copiar el contenido en un nuevo correo y poner las direcciones en copia oculta (CCO)	*verdadero*	*falso*
Los bulos se caracterizan por no incorporar la fecha de su publicación y ser anónimos	*verdadero*	*falso*

Bulo / Hoax

Palabras Clave

cadenas
spam
spammers
hoax
virus
falsedad
malware
bromas
de
engaños
mensajes
atemporalidad
anonimato
bulo

Referencias

[1] Asociación de Internautas (2012) *"III Estudio sobre bulos y fraudes en Internet"*.
Disponible en: http://www.internautas.org/graficos/PPT_IIIEstudioBulosyFraudes13sept.pdf
[Consultado 16/07/2014]

Materiales didácticos **"Confianza y seguridad de las mujeres en la Red"**

Virus informáticos y malware

Actividades didácticas

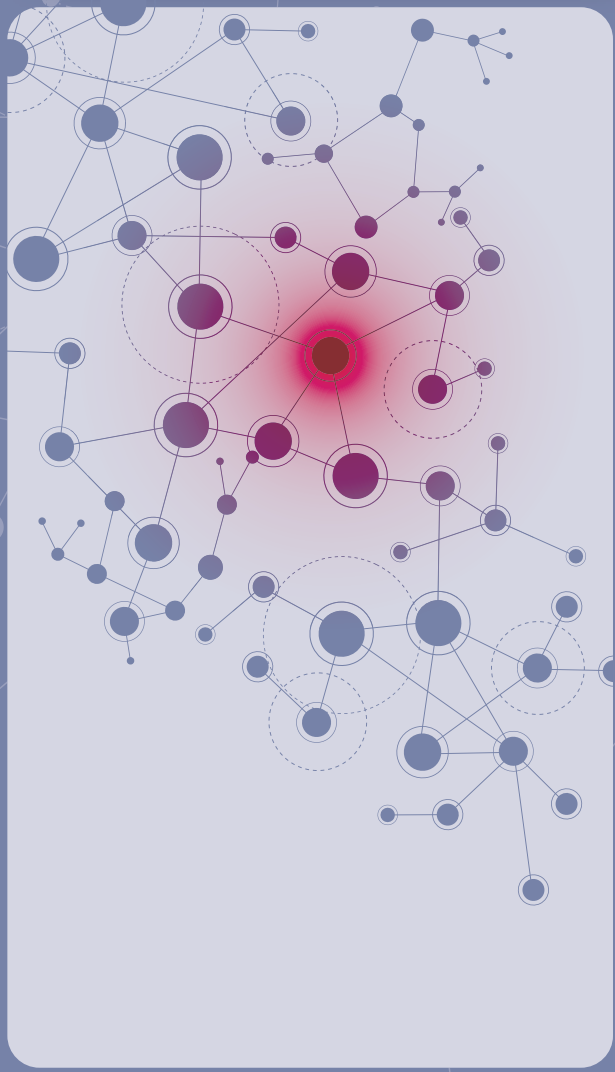
Objetivos generales

Al acabar las actividades, las participantes serán capaces de:

- Reconocer los diferentes tipos de virus informáticos existentes.
- Identificar las situaciones de vulnerabilidad para prevenir el contagio de virus en nuestros equipos informáticos.
- Identificar los signos de sospecha que presentan los equipos cuando contienen virus informáticos.

¿Dónde sucede?

Correo Electrónico | Redes sociales | Juegos en línea | Redes P2P | Mensajería instantánea | Dispositivos de almacenamiento externo



1 Actividad
Virus informáticos - Virus Biológicos

2 Actividad
Dime que virus eres

3 Actividad
Actualizando la versión de juego on-line

4 Actividad
Detectives en la Red

MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
SECRETARÍA DE ESTADO DE SERVICIOS SOCIALES E IGUALDAD
INSTITUTO DE LA MUJER Y PARA LA IGUALDAD DE OPORTUNIDADES
Unión Europea
Fondo Social Europeo

Virus informático - Virus biológico

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Entender cuál es el funcionamiento de los virus informáticos.

1
Actividad

Recursos y materiales


Boligrafos


Tarjetas

Tiempo

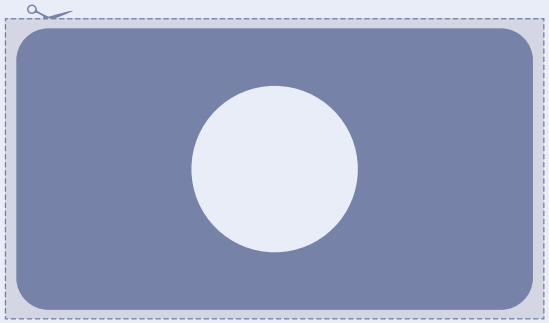
20 min.

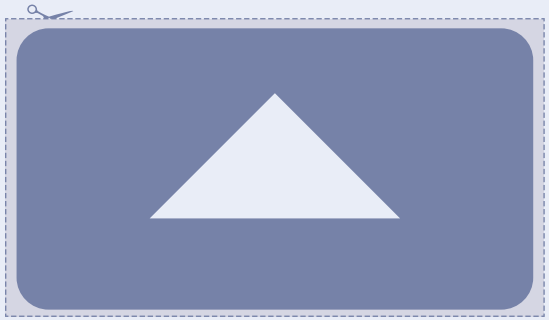
Virus informático - Virus biológico

1
Actividad

Recursos y materiales

Ejemplo de tarjetas para recortar





Nota para el equipo facilitador:

- El 70% de tarjetas estarán marcadas con un cuadrado (significa que las personas que tengan esta tarjeta no utilizan en su equipo informático ningún tipo de herramienta de protección contra los virus informáticos -antivirus, antimalware, antispam, etc.).
- El 20% de las tarjetas estarán marcadas con un círculo (significa que las personas que tengan esta tarjeta, sí utilizan para su equipo informático una herramienta de protección contra los virus informáticos).
- El 10% de las tarjetas estarán marcadas con un triángulo (significa que las personas que tengan esta tarjeta, tienen su equipo infectado de virus informáticos y además no utilizan ningún tipo de herramienta de protección).

Virus informático - Virus biológico

1
Actividad

Desarrollo

1. Tomando como base las semejanzas entre un virus biológico, por ejemplo el virus de la gripe, y un virus informático[1]. El equipo facilitador distribuirá aleatoriamente las tarjetas entre las participantes sin explicarles el significado de las marcas (cuadrado, círculo y triangulo).
2. A continuación, se pedirá a las participantes que escriban en su tarjeta tres cualidades personales que las identifiquen, como por ejemplo: "soy alegre", "soy inteligente", "soy divertida".
3. Después, se les explica que comienza una fiesta durante la cual se tienen que levantar de su silla y compartir lo que han escrito con el resto de personas. Si están de acuerdo con lo que las distintas participantes han escrito sobre sí mismas, pondrán su nombre en la otra cara de la tarjeta mostrada y dirán en voz alta "copiado", de tal manera que al final, cada una tendrá en su tarjeta el nombre de varias participantes. Tras 5 minutos, se da por finalizada la fiesta y se sientan de nuevo.
4. Ahora es cuando se les explica que los nombres que hay en sus tarjetas son los de las personas con quien se supone que han compartido información a través de un pendrive (USB). Además se les explica el significado de los símbolos.
5. Se elige a una participante para que se levante y diga:

    a) Si utiliza o no antivirus (tarjeta con círculo o cuadrado).
    b) Si tiene algún virus informático (tarjeta con triangulo).
    c) Y qué personas ha anotado en el reverso de la tarjeta. Estas personas también se levantan y hacen lo mismo.

    Al final casi todas las participantes estarán de pie, y de forma directa o indirecta se observará que casi todo el mundo ha estado en contacto con el virus.

Recuerda que

- Los virus informáticos son programas maliciosos (malware) que pretenden infectar a otros archivos del sistema con el objetivo de dañarlos, incrustándose en el interior del archivo al igual que los virus biológicos.
- Los virus informáticos, al igual que los virus biológicos, pueden reproducirse a sí mismos. En el caso de los virus informáticos, se hacen copias de sí mismos para infectar los equipos.
- El tamaño de un virus biológico es pequeño en comparación con las células que infectan. Con los virus informáticos sucede lo mismo; por ejemplo un virus informático no debería ocupar más de 1 MB.

Virus informático - Virus biológico

1
Actividad

Desarrollo

6. El equipo facilitador abrirá una lluvia de ideas con las siguientes preguntas:

a) ¿Os ha sorprendido la velocidad con la que se ha propagado el virus?

b) ¿Habéis percibido semejanzas entre un virus biológico y uno informático?

c) ¿Alguna vez habéis tenido algún virus en vuestros equipos? ¿cómo os llegó?

Recuerda que

- Ambos virus (biológico e informático) inician su actividad en forma oculta y sin conocimiento del huésped (organismo-dispositivo) y suelen detectarse cuando ya los daños están causados.
- Ambos tipos de virus son propagados de diversas formas. En el caso de los virus biológicos su medio de propagación es el aire, el agua, el contacto directo, etc. Los virus informáticos pueden propagarse introduciendo una llave USB infectada en un ordenador sano; o a través de internet por medio de un mail o archivo infectado, de mensajería instantánea, etc.

Dime que virus eres

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Entender las diferencias entre los tipos de virus más comunes.
- Tomar conciencia de las consecuencias cuando nuestros dispositivos están infectados con virus.

Recursos y materiales


Tijeras


Papel


Tarjetas

El equipo facilitador aportará 24 cartas para realizar la actividad. Habrá tres tipos de cartas: cartas con el nombre del virus; cartas con el texto de la pista que permitirá descubrir el nombre del virus y cartas con la definición del virus. El contenido de cada una de las cartas se encuentra en la siguiente ficha para recortar.

2
Actividad

Tiempo

30 min.

Dime que virus eres

2
Actividad

Recursos y materiales[2]

Cartas para recortar

 **Bomba Lógica** Nombre de virus o malware	Estás es una ceremonia egipcia que se hacía en el templo de Abu Simbel cuando el sol entraba por un largo pasillo e iluminaba las estatuas de Nefertaris y Ramses II — Pista misteriosa	Es un tipo de virus dentro de un programa, que se instala en un ordenador y se ejecuta cuando se cumple una determinada condición (por ejemplo, una fecha concreta relacionada con una persona mundialmente reconocida. Este tipo de códigos ha sido muy usado para la lucha contra la piratería de programas) — Definición del virus o malware
 **Bulo (Hoax)** Nombre de virus o malware	Se extiende el rumor que existe un virus que se contagia por contacto físico. El chisme se propaga por la ciudad y las personas dejan de salir a la calle para no tener contacto con el resto de habitantes. — Pista misteriosa	Son mensajes difundidos a través del correo electrónico con la finalidad de crear confusión y alertar de la existencia de falsos virus. Se presentan como noticas de contenido engañoso que solicitan a quienes las reciben reenviarlas por correo a toda su lista de contactos. — Definición del virus o malware
 **Gusanos** Nombre de virus o malware	María coge una hermosa manzana del campo y la guarda en el frutero de su casa. Al cabo de una semana, cuando se dispone a comerse su manzana, comprueba que la fruta tiene agujeros y no es comestible; sorprendentemente el resto de frutas del frutero no tienen esos agujeros. — Pista misteriosa	Son programas cuya característica principal es realizar el máximo número de copias de sí mismos posible para facilitar su propagación. A diferencia de los virus, no infectan otros ficheros. — Definición del virus o malware

Dime que virus eres

2
Actividad

Recursos y materiales

Cartas para recortar

Troyanos

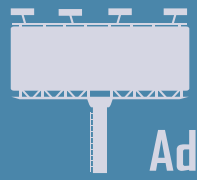
Nombre de virus o malware

Una ciudad recibe un regalo de gran tamaño de un pueblo vecino, agasajados por el obsequio celebran una gran fiesta. Durante la noche, de la fiesta sale un escuadrón de combate desde dentro del regalo que ataca al pueblo de forma desprevenida y lo conquista.

Pista misteriosa

Engañan disfrazándose de programas o archivos legítimos/benignos (fotos, archivos de música, archivos de correo, etc.), con el objetivo de infectar y causar daño. Tienen la capacidad de extraer, copiar y enviar información, así como abrir puertos de comunicación. Aunque no se reproducen, ni infectan archivos, son extremadamente peligrosos por su apariencia inofensiva.

Definición del virus o malware



Adware

Nombre de virus o malware

Una persona tiene que repartir publicidad en la entrada de una estación de metro, pero después de estar mucho tiempo sin que nadie se la acepta, decide poner un torniquete en la salida de la estación de forma que las personas sólo puedan salir si han cogido su publicidad. Al cabo de un rato, comprueba que en las horas punta la gente no puede casi ni entrar ni salir.

Pista misteriosa

Son programas que automáticamente ejecutan o muestran publicidad en nuestro ordenador, animando incluso a instalar falsos programas antivirus. Estos programas rastrean qué tipo de uso hacemos y las páginas webs que visitamos, para mostrarnos una publicidad redirigida y relacionada con esos usos.

Definición del virus o malware

Programa espia (spyware)

Nombre de virus o malware

En los vestidores del gimnasio de un colegio, encontraron una cámara de vídeo. Después se supo que la cámara había sido instalada por unas alumnas del propio colegio.

Pista misteriosa

Son programas que tienen por finalidad la recopilación y envío de información (datos personales, páginas visitadas, contraseñas bancarias) de un ordenador sin conocimiento ni consentimiento, a un servidor remoto. Este tipo de malware es el más extendido. Tambien produce fallos y lentitud en la conección a internet del equipo infectado

Definición del virus o malware

Dime que virus eres

2
Actividad

Recursos y materiales

Cartas para recortar

Broma (Joke)

Nombre de virus o malware

Alguien envió una carta a una agencia de contraespionaje. Se activó un protocolo anti ataque bacteriológico, y después de muchos análisis, se comprobó que simplemente era harina de trigo.

Pista misteriosa

No realiza ninguna acción maliciosa en el ordenador infectado, pero mientras se ejecuta, gasta una "broma" haciéndote pensar que tu ordenador está infectado, por ejemplo, mostrando un falso mensaje sobre que se va a borrar todo el contenido del disco duro, o moviendo el ratón de forma aleatoria.

Definición del virus o malware

Ladrón de contraseñas (PWStealer)

Nombre de virus o malware

Unas delincuentes instalan una cámara de video en un cajero automático para grabar las contraseñas de las personas usuarias. Además, también tienen un dispositivo camuflado que graba la banda magnética de las tarjetas para reproducirla posteriormente.

Pista misteriosa

Son programas que roban nombres de usuario/a y contraseñas del ordenador infectado, generalmente accediendo a determinados ficheros del ordenador que almacenan esta información.

Definición del virus o malware

Dime que virus eres

2
Actividad

Desarrollo

1. Se formarán hasta 8 grupos de 2 y/o 3 mujeres.
2. El equipo facilitador distribuirá las 24 cartas aleatoriamente entre los ocho grupos, dando a cada grupo el mismo número de cartas.
3. El objetivo del juego consistirá en relacionar los tres conceptos (el nombre, la pista y el significado de los virus). Cada grupo deberá encontrar las cartas que le completen una terna, y para ello deberá intercambiar sus tarjetas con los otros grupos.
4. Cuando algún grupo haya logrado encontrar su terna deberá explicar cómo ha llegado a esa conclusión.
5. El juego continuará hasta que se hayan completado las 8 ternas.
6. Durante el desarrollo de la actividad, el equipo facilitador, si ve que hay dificultades, ayudará con más pistas para formar las ternas. Al final, se realizará una puesta en común y se explicarán las diferencias y semejanzas entre los distintos virus, así como las **consecuencias generales** cuando en nuestros equipos informáticos hay virus:

   - Robo o destrucción de nuestra información (vídeos, fotografías, contactos, documentos). Es importante tener copias de seguridad.
   - Denegación de accesos, puesto que a veces no puedes acceder a tus documentos por estar protegidos con contraseñas (cifrado).
   - Pérdida de privacidad y suplantación de identidad.
   - Fraude económico, ya que los virus son capaces de acceder a nuestros datos bancarios, permitiendo a la ciberdelincuencia hacer compras on-line y realizar transferencias.
   - Pérdida de tiempo en la reinstalación y formateo de los equipos.

Recuerda que

- Hay muchos tipos de virus informáticos y pueden clasificarse en función de diferentes criterios, tales como su forma de propagación o el tipo de acciones que realizan en el equipo infectado. Hay que tener presente que cada virus plantea situaciones diferentes.
- Los virus pueden afectar a cualquier dispositivo: ordenadores personales, teléfonos móviles, tablets, videoconsolas, etc.

Actualizando la versión de un juego on line

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Detectar situaciones de riesgo de contagio de virus informáticos.
- Reconocer los síntomas de un dispositivo infectado por virus.

3 Actividad

Recursos y materiales

Texto del caso Actividad 3

Tiempo

15 min.

Actualizando la versión de un juego on line

3
Actividad

Desarrollo

1. El equipo facilitador leerá un caso y abrirá un debate sobre:

    a) Piratería de los juegos en línea.

    b) Búsqueda y actualizaciones de descargas de juegos en línea.

    c) Ficheros sospechosos.

CASO BASADO EN UNA HISTORIA REAL

Lucía, de 19 años, suele jugar con su amiga todos los viernes a los videojuegos en línea. En un descanso, entraron en un chat para intercambiar con otras jugadoras experiencias, actualizaciones y novedades. Aprovechando la ocasión, preguntaron sobre un reto que había en el videojuego, imposible de superar. Inmediatamente, una usuaria del chat les recomendó que descargaran una versión actualizada y mejorada del juego, eso sí, pirateada. A Lucía y a su amiga les pareció una buena idea, y se descargaron la nueva versión. En la descarga había dos ficheros, uno "leeme.txt", donde se detallaban los pasos a seguir, y un ejecutable "dolime.exe". Cuando ejecutó el archivo "dolime.exe" apareció inmediatamente una ventana que le advertía de la existencia de virus en su equipo y le recomendaba solucionar el problema. A Lucía le pareció extraño, ya que los mensajes de su antivirus nunca habían sido de ese tipo; el color era diferente y aparecía todo en inglés, sin embargo ella aceptó. A partir de ese instante, constantemente aparecía el mismo mensaje diciendo que tenía un virus, y su equipo iba cada vez más lento, hasta que le confirmaron en la tienda donde compró su ordenador que tenía un virus troyano, y por tanto la única forma de solucionarlo era formatear el disco duro de su ordenador.

Recuerda que

Los virus son una herramienta del crimen organizado, especializado en todo tipo de delitos informáticos, por tanto:

- Los programas y juegos pirateados pueden contener virus, también las películas, series o canciones que te descargas de manera ilegal. Usa software original.
- En el caso de que hayas tenido que facilitar la tarjeta de crédito para darte de alta en algún servicio on-line, controla tus movimientos bancarios para detectar posibles fraudes.
- Nunca compartas tus contraseñas con otras personas.

Actualizando la versión de un juego on line

3
Actividad

Desarrollo

2. Posteriormente, se preguntará al grupo qué síntomas piensan que tiene un ordenador cuanto está infectado. Las respuestas se anotarán en papelógrafo o pizarra.

   Se orientará al grupo en caso de que no haya respuestas espontáneas, preguntando si piensan que son **síntomas de infección** los referidos a continuación, hasta completar el listado:

Síntomas de infección

- Reducción inesperada del espacio libre en la memoria o disco duro.
- El equipo tarda más de lo habitual en encenderse o apagarse.
- Lentitud en las operaciones rutinarias (conexión a Internet, software).
- El equipo realiza automáticamente acciones que tú no le indicas: Por ejemplo, tus contactos (círculo de amistades, familiares) reciben mensajes de correo que tú no has enviado e incluso encuentras contenidos en el muro de tu facebook que tampoco has enviado tú.
- Apertura de ventanas emergentes (aparecen todo tipo de pop-ups y mensajes en el escritorio) y anuncios, incluso cuando no se está usando un navegador web.

Detectives en la Red

Objetivos de la actividad

Al acabar la actividad, las participantes serán capaces de:

- Identificar los correos que contengan virus en sus archivos adjuntos y las medidas a tomar.

.

4 Actividad

Recursos y materiales

Baraja de cartas por duplicado

Papel continuo / cartulinas

Cinta adhesiva

Tiempo

25 min.

Detectives en la Red

4
Actividad

Recursos y materiales

Cartas para recortar por duplicado

Carta 1

mifoto.exe

Carta 2

verano.bat

Carta 3

tarjetadenavidad.vbs

Carta 4

informe.doc

(con programación: macros)

Carta 5

balance.xls

(con programación: macros)

Carta 6

presentacion.ppt

(con programación: macros)

Carta 7

datos.mdb

(con macros)

Carta 8

protectorpantalla.scr

Carta 9

programas.pif

Detectives en la Red

4
Actividad

Recursos y materiales

Cartas para recortar por duplicado

Carta 10

virus.txt

Carta 11

formato.rtf

Carta 12

infeccion.bmp

Carta 13

imagen.jpg

Carta 14

foto2.tif

Carta 15

Animacion.gif

Carta 16

Pronta entrega - virus.mp3

Carta 17

sonido.wav

Carta 18

La epidemia.mpg

Detectives en la Red

4
Actividad

Desarrollo

1. Se dividirá a las participantes en 2 grupos y cada grupo elegirá una relatora.
2. El equipo facilitador entregará a cada grupo un juego de cartas.
3. Se explicará que cada carta simboliza un archivo adjunto que nos han enviado a nuestro correo electrónico.
4. Cada grupo tendrá una cartulina dividida en dos grandes círculos con los títulos: "puede tener un virus" y "puede no tener un virus" respectivamente. Tendrá que pegar en cada uno de sus círculos los ficheros que crean que puedan contener virus o no.
5. Seguidamente, el equipo facilitador leerá el siguiente caso basado en hechos reales antes de dar paso al plenario:

CASO BASADO EN UNA HISTORIA REAL

Lola, una compañera de trabajo, recibió hace días un correo electrónico de una empresa farmacéutica holandesa en el que la invitaban a probar y adquirir, a precios muy competitivos, una nueva gama de productos de estética muy eficaces. Para poder probar y adquirir los productos, pedían completar un formulario que adjuntaban en el correo. El nombre del archivo adjunto era "estar guapa.exe". Lola abrió el adjunto y el archivo resultó ser un ejecutable que infectó su equipo al tratarse de un virus informático.

Recuerda que

- No abras archivos adjuntos de remitentes que no conoces, pueden contener virus informáticos y pueden ocasionar daños a tu equipo.
- Comprueba que los adjuntos de todos los correos que recibes no contienen virus antes de abrirlos.
- Cuando ejecutas ficheros que son virus, te conviertes en emisora de nuevos virus, y de manera involuntaria puedes infectar los equipos de tus contactos.

Detectives en la Red

4
Actividad

Desarrollo

7. En plenario se expondrán las conclusiones a las que ha llegado cada grupo. El equipo facilitador abrirá un debate y hará la devolución del juego a partir de las siguiente pregunta:

    a) ¿Por qué habéis pensado que esas extensiones contenían un archivo dañino para el equipo?

    A continuación, se explica el significado de cada una de las extensiones:

    - Ficheros ejecutables de extensión: .exe, .bat
    - Programas de Visual Basic Script: .vbs
    - Documentos de Office con macros: .doc, .xls, .ppt, .mdb
    - Protectores de pantalla: scr
    - Archivos de información de programas: .pif
    - Texto puro: .txt
    - Formato de texto enriquecido: .rtf
    - Imágenes: .bmp, .jpg, .tif, .gif,
    - Videos, sonidos: .mp3, .wav, .mpg

    b) ¿Alguna vez habéis reenviado algún correo con este tipo de archivos?

    Nota para el equipo facilitador: Las cartas del 1 al 9 son archivos que pueden ocultar un virus. Las cartas del 10 al 18, son archivos que no pueden contener virus.

Virus informáticos y malware

Consejos y buenas prácticas

- Instala un antivirus efectivo en tu ordenador, tablet y smartphone. Existen versiones gratuitas y de pago; lo más importante es que te asegures que haya sido desarrollado por una compañía fiable y que directamente descargues el antivirus de la web oficial de la empresa fabricante
- Actualiza regularmente el sistema operativo, programas y navegadores que utilices.
- Realiza con periodicidad copias de seguridad de la información que consideres valiosa y guárdalas en un dispositivo distinto al que contiene la información que vas a copiar, asegurándote de que no está infectada.
- Si necesitas información que esté en dispositivos de almacenamiento externo (pendrive, discos duros, tarjetas de memoria) verifica que tienes activado y actualizado el antivirus.
- Evita utilizar software pirata o no original, ya que muchas veces son la causa directa del contagio; las propias personas que se encargan de desproteger estos programas, muchas veces integran virus o programas espía (spyware).
- Ten en cuenta que las webs de hackeo, adultos, casinos on-line o descargas ilegales, son fuentes muy comunes de propagación de virus.
- Ten activo el programa cortafuegos (Firewall), ya que es un buen mecanismo de seguridad contra ataques que provienen de Internet, evitando así el robo de información. Actualmente varios antivirus ya vienen con firewall.
- Evita ejecutar archivos con extensión VBS o EXE, que vengan adjuntos en correos no esperados o de descargas de sitios Web. Es aconsejable que analices el correo electrónico y los archivos adjuntos con el antivirus antes de abrirlos, aunque conozcas al remitente.
- Configura tu navegador con los niveles de seguridad adecuados, prefiriendo los ítems de alta seguridad que se activan en el menú de herramientas de tu navegador.
- Ten sólo un antivirus instalado, nunca dos o más, ya que puede provocar conflictos entre ellos.
- Los antivirus no son infalibles ya que pueden ser vulnerables a virus de reciente creación para los que no estén preparados. De ahí, la necesidad de tenerlos permanentemente actualizados.

  En definitiva, utiliza el sentido común. La mejor precaución ante los virus, es mantenerte alerta y ser precavida ante cualquier cosa que te parezca sospechosa.

Virus informáticos y malware

Actividades didácticas

Datos de interés

Virus: Código informático malicioso que tiene como objetivo de dañar los equipos informáticos o la destrucción de la información.

¿Qué es el malware?

Engloba a todo tipo de programa o código informático malicioso que se instala en nuestro equipo sin consentimiento ni conocimiento, con el objetivo de alterar tanto el funcionamiento del equipo, como la información que contiene, además de pretender un beneficio económico. Normalmente sucede a través de un archivo ejecutable (cuyas extensiones más comunes son: .exe / .com / .scr y reciben ese nombre porque el ordenador los interpreta como un programa) que pasa a ser portador del virus y por tanto una fuente de infección. El código del virus queda alojado en la memoria RAM del equipo, aun cuando el programa que contenía el virus no esté ejecutándose.

Inicialmente, los virus informáticos fueron creados como juegos o retos intelectuales entre Hackers (personas apasionadas por la seguridad informática). La razón principal para quienes creaban el virus era el reconocimiento público, ya que cuanta más relevancia tuviera el virus, más reconocimiento obtenía la persona creadora.

¿Cómo se distribuyen los virus?

Las principales vías de acceso para infectar tu equipo son:

- **Correos electrónicos no deseados (spam)**: Es la principal y preferida vía de entrada, por lo que hay que estar atentas al contenido de los correos, ya que pueden contener ficheros adjuntos como: programas ejecutables (.exe), ficheros PDF o ficheros comprimido (.zip o .rar) o cualquier otro tipo de archivo que contenga un virus.
- **Redes sociales**: Son también una vía para infectar los equipos debido a la gran cantidad de personas usuarias y por tanto a su potencial de difusión y propagación.
- **Webs fraudulentas**: Los correos que recibimos puede que estén vinculados a páginas web fraudulentas que contienen malware. Un ejemplo frecuente son las falsificaciones de páginas web bancarias.
- **Redes P2P (descargas de ficheros)**: Las descargas mediante programas de compartición de ficheros (P2P) pueden contener algún tipo de virus, por lo que debes extremar la precaución. Muchos virus se cuelan por las descargas ilegales.
- **Dispositivos de almacenamiento externo (pendrive, discos duros, tarjetas de memoria, etc.)**: La infección a través de dispositivos externos se realiza al copiar archivos infectados de un dispositivo externo a nuestros equipos; incluso algunos virus tienen la capacidad de autoejecutarse.
- **Mensajería instantánea:** Dada la popularidad de esta herramienta, suele usarse como una vía de entrada para filtrar virus, al igual que los correos electrónicos.

Virus informáticos y malware

Evaluación

Para reforzar los contenidos aprendidos, piensa si son verdaderas o falsas las siguientes afirmaciones:

Con el uso indiscriminado de la descarga de ficheros a través de redes P2P tendrás más riesgo de sufrir un ataque de virus.	*verdadero*	*falso*
Los "gusanos informáticos" son programas cuya finalidad es infectar otros ficheros.	*verdadero*	*falso*
Existen virus informáticos que te animan a instalar falsos programas antivirus.	*verdadero*	*falso*
Las compañías antivirus son las que desarrollan los virus.	*verdadero*	*falso*
Cuando te instalas un antivirus te garantizan la seguridad máxima.	*verdadero*	*falso*

Virus informáticos y malware

Palabras Clave

malintencionado programas externo ingeniería social directorios troyanos de software macro operativo ejecutables sistema dispositivos ficheros virus adware maliciosos malicioso spyware código almacenamientos piratas gusanos

Referencias

[1] La actividad propuesta es una adaptación de la dinámica *"La fiesta: Cadena de transmisión"* desarrollada en (2007) "*Dinámicas que contemplan las Acciones Educativas de SIDA Studi*" .Área de Salud Pública i Consumo de la Diputació de Barcelona.
Disponible en: http://www.sidastudi.org/resources/doc/091127-10-dinamiques_castella-492606124477994323.pdf
[Consultado 16/07/2014]

[2] Adaptado según las definiciones extraídas del portal web de INTECO, *"Virus y Programas Maliciosos"*.
Disponible en: http://www.inteco.es/Formacion/Amenazas/Virus/
[Consultado: 16/07/2014]

Edita:
Instituto de la Mujer y para la Igualdad de Oportunidades
Ministerio de Sanidad, Servicios Sociales e Igualdad
Condesa de Venadito 34
28027-Madrid

Textos:
Instituto de la Mujer y para la Igualdad de Oportunidades
Ángeles Matesanz Barrios

AMB Piensa S.L.
Mónica Castellanos Torres
Antonio Miguel Baena Cock

Diseño:
AMB Piensa S.L.

NIPO: 685-14-056-7
Catálogo de publicaciones oficiales de la Administración General del Estado
http://publicacionesoficiales.boe.es