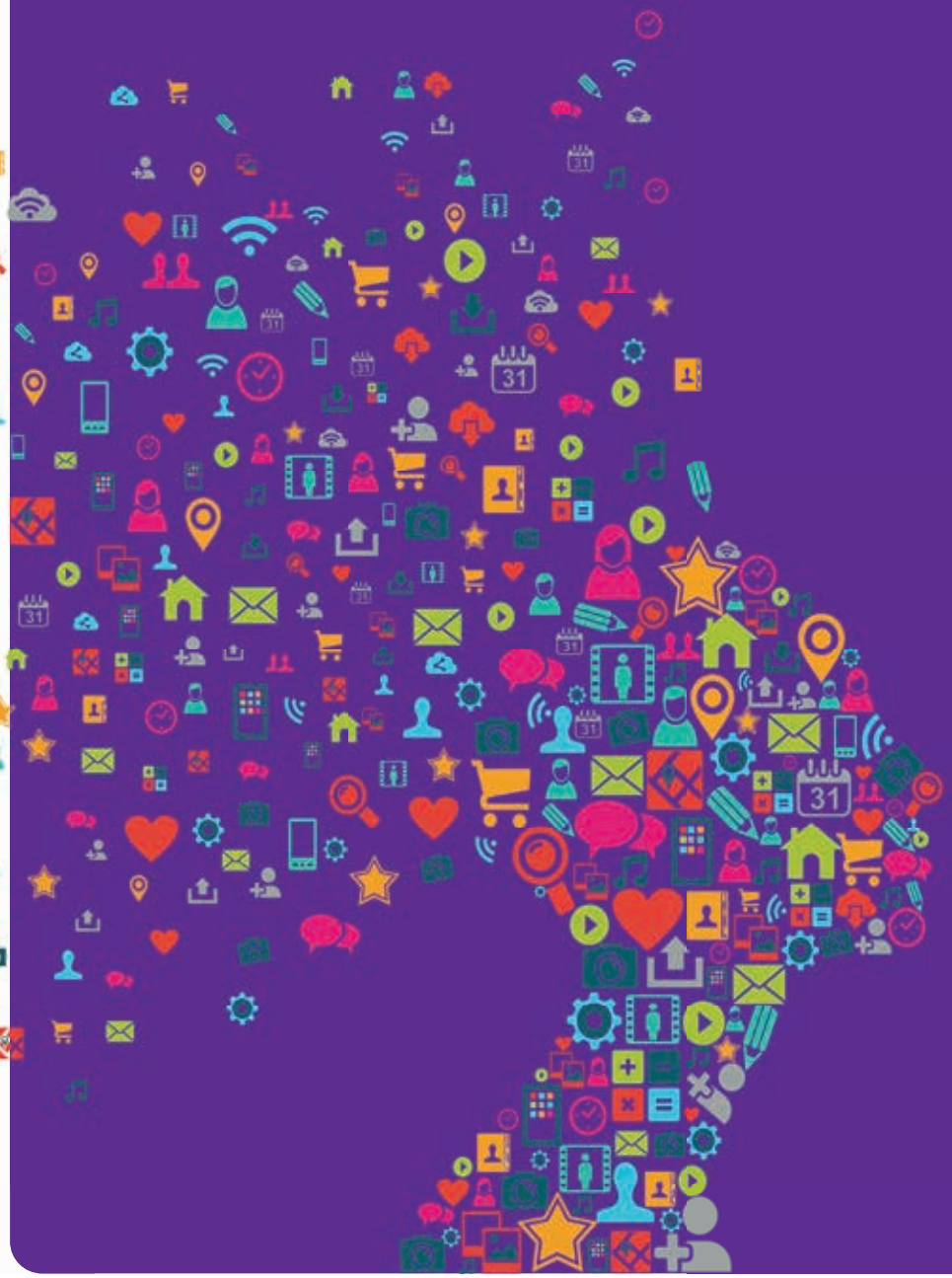


Guía
Confianza y seguridad de las mujeres en la Red

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

Índice

Presentación

Esta guía 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. Trata sobre algunos de los posibles riesgos que pueden encontrarse en Internet. Incluye una serie de recomendaciones y consejos para prevenirlos , además de algunos datos de interés.

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 esta guía, además de abordar-se riesgos generales como por ejemplo, estafas o robo de contraseñas, se tratarán aquellos relacionados con la violencia de género. También, dado que las mujeres, aun con mucha frecuencia, son las responsables de los cuidados en la familia, abordaremos algunas temáticas relacionadas con menores e Internet.

En definitiva, esperamos que la guía 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

Identidad digital, reputación y privacidad on-line

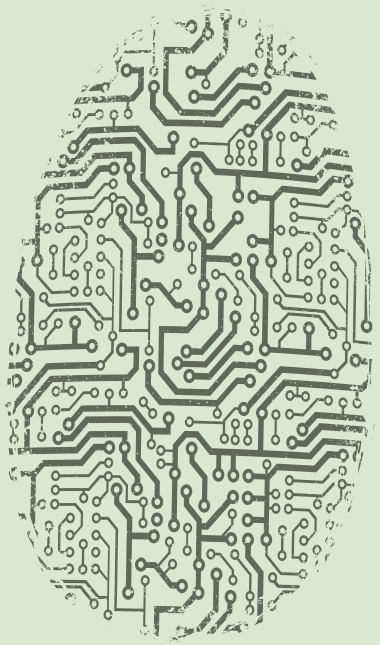
Información que publico + Información que comparto + Información que existe sobre mi [1].

Datos de interés

¿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.



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[2] y canales de denuncia a disposición de las personas usuarias.

Consejos y buenas prácticas

- 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 información 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.

¿Dónde sucede?


Correo electrónico


Redes sociales


Juegos en línea


Chat


Mensajería instantánea

Referencias

[1] 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]

[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.

1. Brigada de Investigación Tecnológica de la Policía Nacional: http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html

2. Grupo de Delitos Telemáticos de la Guardia Civil: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

Contraseñas

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

Datos de interés

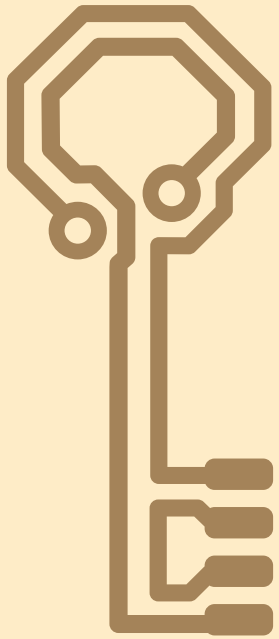
Siguiendo las recomendaciones de Windows, para que una contraseña sea segura[1], ésta ha de cumplir una serie de recomendaciones que nos ayudarán a proteger nuestra información. Deberemos pensar en contraseñas imaginativas y personales que además sean:

- **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 adelante.
- **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.



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 minúscuslas).
- 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

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: G53tlrr1

  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: 8G53tlrr1 / Foro Motera: 10G53tlrr1
- Utiliza reglas mnemotécnicas, como elegir la primera letra de cada palabras de una frase:
  - No hay mal que 100 años dure: Nhmq100ad

¿Dónde sucede?


Correo electrónico


Redes sociales


Juegos en línea


Redes P2P


Mensajería instantánea


Dispositivos de almacenamiento externo

Referencias

[1] 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]

[2] *Ibid.*

Ciberacoso

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

Datos de interés

En el ciberacoso aunque tanto hombres como mujeres pueden ser víctimas, el porcentaje de víctimas femeninas es siempre mayor que las masculinas[1]. 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[2].

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 ciberacoso:

- 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 desconocida.

Consejos y buenas prácticas

- 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 con las autoridades a través de la Policía Nacional (Brigada de Investigación Tecnológica) o Guardia Civil (Grupo de Delitos Telemáticos) y formula la denuncia.

¿Dónde sucede?


Correo electrónico


Redes sociales


Juegos en línea


Mensajería instantánea

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://goo.gl/pevrFI

[2]Tjaden, P. y Thoennes, N. (1998). Stalking in America: *Findings from the national survey against women violence.* Washington, 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://goo.gl/pevrFI

Sexting

Envío voluntario a terceras personas de imágenes o videos de contenido sexual mediante dispositivos móviles.

Datos de interés

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[1] 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.

Datos de interés

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.

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)[2].

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 vírica.
- 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 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.

Consejos y buenas prácticas

- 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[3] 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

¿Dónde sucede?


Correo electrónico


Redes sociales


Juegos en línea


Mensajería instantánea

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"*. Ministerio de Sanidad, Servicios Sociales e Igualdad. Delegación del Gobierno para la Violencia de Género.

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

[3] 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.

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

Extorsión sexual / Sextorsión

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

Datos de interés

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).

Consejos y buenas prácticas

Recomendaciones para prevenir situaciones de sextorsión

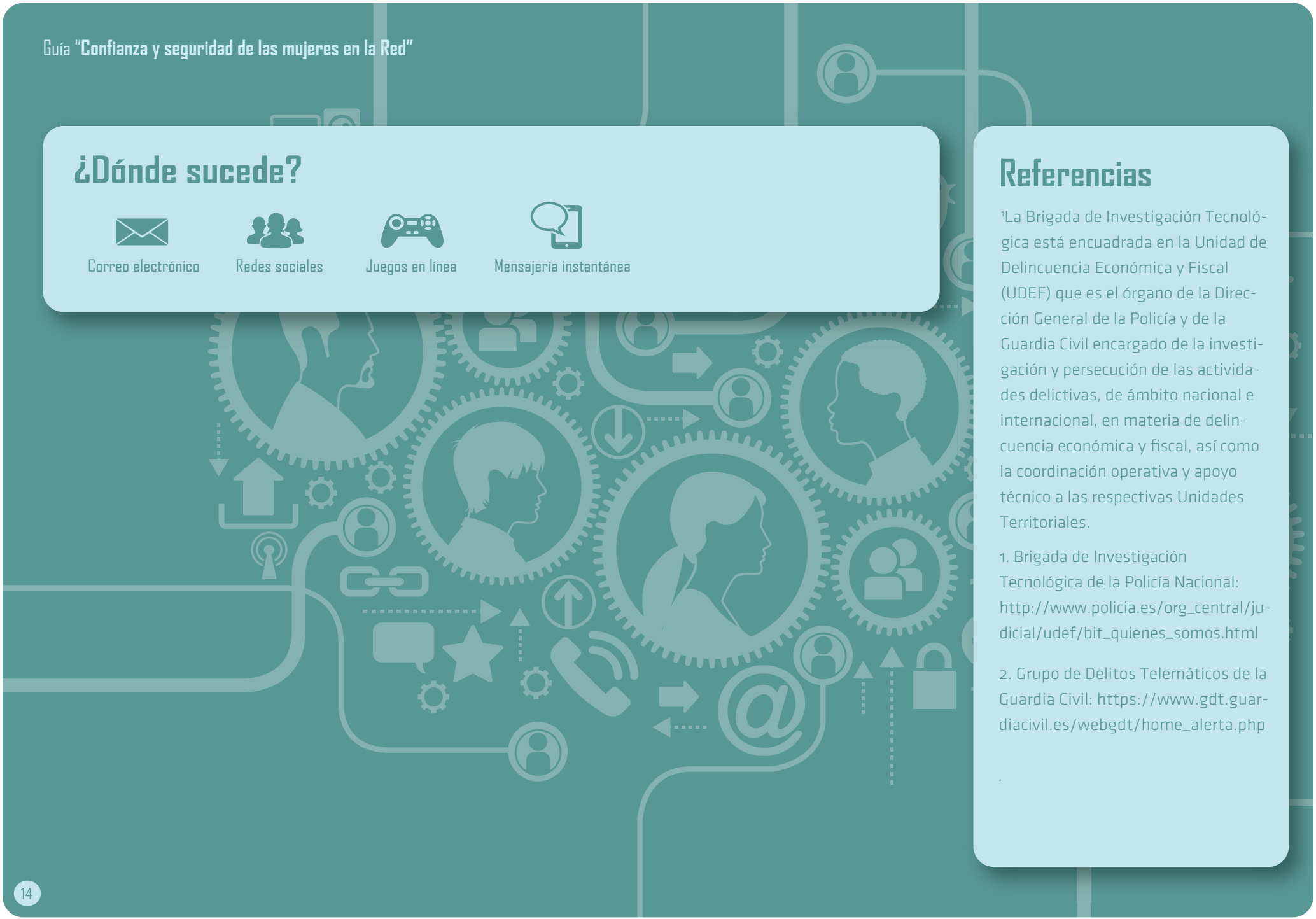
- Sé consciente del riesgo que corres si compartes material de contenido íntimo con personas de tu círculo de confianza o incluso con parejas sentimentales, ya que en el caso de ruptura, pueden ser quienes difundan los materiales o incluso te chantajeen.
- Intenta mantener tus dispositivos (Smartphone, 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.

¿Dónde sucede?

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



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.

1. Brigada de Investigación Tecnológica de la Policía Nacional: http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html

2. Grupo de Delitos Telemáticos de la Guardia Civil: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

.

Acoso sexual a menores en Internet / Grooming

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

Datos de interés

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.

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.

Consejos y buenas prácticas

- 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.

¿Dónde sucede?


Correo electrónico


Redes sociales


Juegos en línea


Mensajería instantánea

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.

1. Brigada de Investigación Tecnológica de la Policía Nacional: http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html

2. Grupo de Delitos Telemáticos de la Guardia Civil: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

.

Ciberacoso escolar / Cyberbullying

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

Datos de interés

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[1]. 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[2] 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).

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[3] con la Policía Nacional (Brigada de Investigación Tecnológica) o Guardia Civil (Grupo de Delitos Telemáticos).

Consejos y buenas prácticas

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.

¿Dónde sucede?


Correo electrónico


Redes sociales


Juegos en línea


Mensajería instantánea

Referencias

[1] Orijuela 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]

[2] I*bid.,p.*24
[Consultado 18/07/2014]

[3] 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

Tecnoadicciones

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

Datos de interés

Algunas conductas asociadas a las tecnoadicciones:

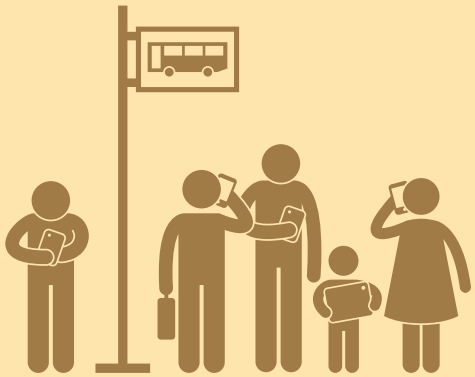
- Puesto que las nuevas tecnologías de la información y la comunicación forman parte ya de nuestra vida cotidiana, es difícil determinar dónde está el límite entre el uso necesario y el uso adictivo.
- El "phubbing" hace referencia al uso del teléfono móvil o la tablet mientras se está en compañía de 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[1].



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 de 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, etc.).
- 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.

¿Dónde sucede?

Referencias

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

Fraude en la Red / Phishing

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

Datos de interés

Las identidades o los servicios[1] 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.

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.

Consejos y buenas prácticas

- 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 hacker.
- 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 contraseñas y ponte en contacto con la entidad bancaria o empresa a la que supuestamente han suplantado para avisarles de lo acontecido.
- Ponte en contacto[2] con la **Brigada de Investigación Tecnológica** de la Policía Nacional o el **Grupo de Delitos Telemáticos** de la Guardia Civil y formula la denuncia.

¿Dónde sucede?


Correo electrónico


Redes sociales


Mensajería instantánea

Webs

SMS

Referencias

[1] 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://goo.gl/7mYRIa [Consultado 16/07/2014]

[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.

1. Brigada de Investigación Tecnológica de la Policía Nacional: http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html

2. Grupo de Delitos Telemáticos de la Guardia Civil: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

Correo no deseado / Spam

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

Datos de interés

¿Cómo son estos mensajes?

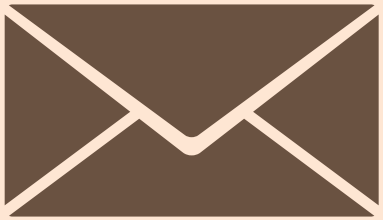
- La dirección que aparece como remitente del mensaje, no suele ser conocida y la mayoría de las veces es falsa.
- El asunto del mensaje suele ser comercial y atractivo.
- El spam puede buscar desde publicidad hasta actividades ilegales (fraudes económicos). Así, son múltiples y variados los tipos de 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.



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.

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 (CCO). Asimismo, si reenvías un correo, elimina las direcciones del resto de personas destinatarias.

Consejos y buenas prácticas

- 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.

¿Dónde sucede?

Correo electrónico

SMS

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

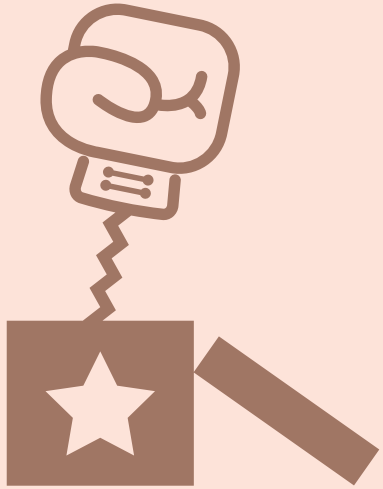
Bulo / Hoax

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

Datos de interés

La "Asociación de Internautas" realizó un estudio' 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.



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.

Consejos y buenas prácticas

- 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.

¿Dónde sucede?


Correo electrónico


Redes sociales


Foros


Mensajería instantánea

Referencias

[11] 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]

Virus informáticos y malware

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

Datos de interés

¿Qué es el malware?

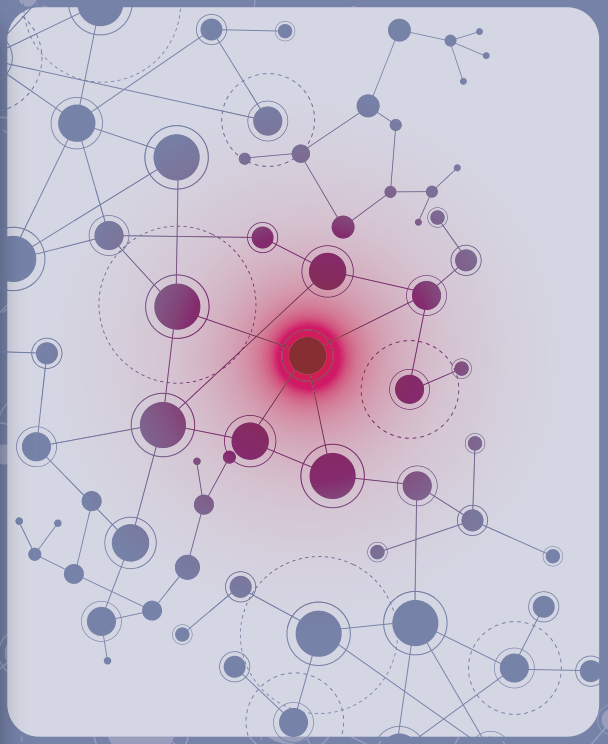
Engloba a todo tipo de programa o código informático malicioso que se instala en nuestro equipo sin consentimiento ni conocimiento, con el objetivo de alterar tanto el funcionamiento del equipo, como la información que contiene, además de pretender un beneficio económico. Normalmente sucede a través 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.



Datos de interés

- **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.

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.

Consejos y buenas prácticas

- 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.

¿Dónde sucede?


Correo Electrónico


Redes sociales


Juegos en línea


Redes P2P


Mensajería instantánea


Dispositivos de almacenamiento externo

Esta guía se complementa con la publicación, "Materiales didácticos. Confianza y seguridad de las mujeres en la Red", editada en el año 2014 por el Instituto de la Mujer y para la Igualdad de Oportunidades.

Las definiciones legales que figuran en ambos materiales, no siempre se corresponden con las definiciones legales desde el punto de vista del Código Penal.

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: 685-14-055-1
Catálogo de publicaciones oficiales de la Administración General del Estado
http://publicacionesoficiales.boe.es