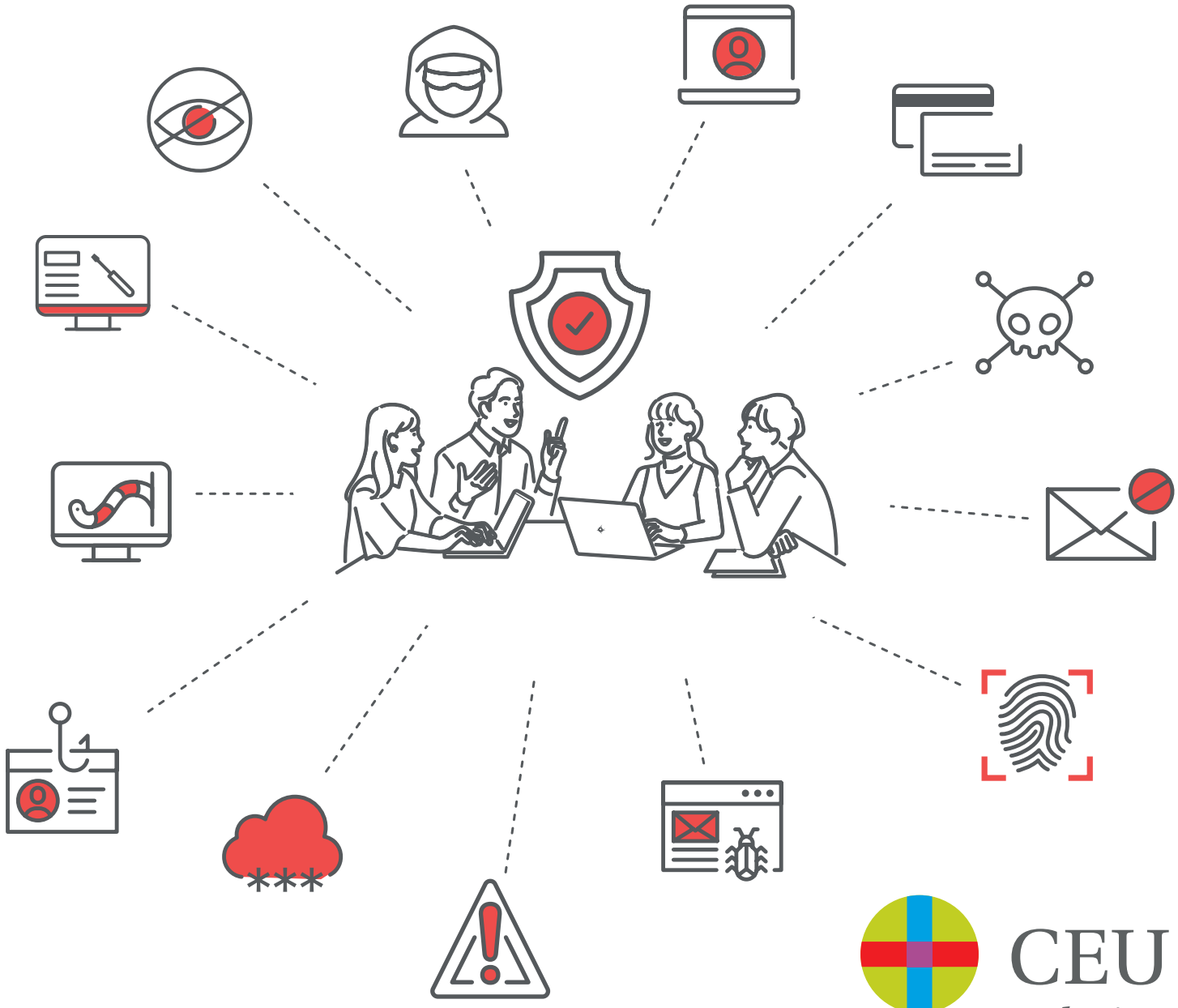
Familias conectadas

Guillermo Cánovas

Ciberseguridad familiar

Ciberinteligencia e Ingeniería Social



CEU Colegios

Guías Familias Conectadas

Ciberseguridad familiar. Ciberinteligencia e ingeniería social

Queridas familias:

Desde el Área de colegios CEU continuamos trabajando para mejorar la salud digital de todos nuestros alumnos, familias y personal. En esta segunda guía de “Ciberseguridad familiar”, elaborada conjuntamente con Guillermo Cánovas, trataremos temas de ciberinteligencia e ingeniería social con el objetivo de mostraros la importancia que tiene el saber manejarnos con seguridad en el entorno digital. Al igual que educamos ante las situaciones ordinarias de la vida cotidiana, también debemos educar a nuestros hijos respecto al modo de actuar y relacionarse en la red.

Con esta guía queremos facilitaros la información para poder comprender el entorno digital y saber actuar ante los posibles peligros que hay en internet: la ciberdelincuencia. Ésta no se trata únicamente de fraudes económicos, sino de amenazas o ciberdelitos que afectan también a la privacidad y seguridad de las personas a las que queremos o con las que nos relacionamos en nuestro entorno familiar, de amistades y laboral.

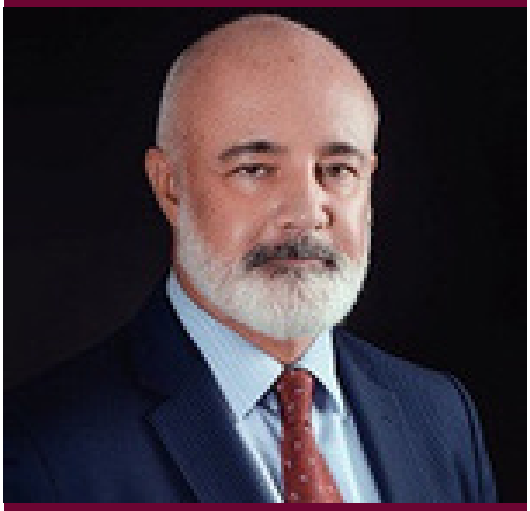
Os queremos acompañar en este aprendizaje digital para continuar educando y protegiendo a los nuestros.

Esperamos que sea de vuestro interés.

Saludos cordiales,

Raül Adames

Director Área de Colegios CEU



GUILLERMO CÁNOVAS

PERFIL DEL AUTOR

Director del Observatorio para la Promoción del Uso Saludable de la Tecnología “Educalike”.

Director del Centro de Seguridad en Internet para los Menores en España, integrado en el Safer Internet Programme de la Comisión Europea (2002-2014).

Profesor y escritor.

RECONOCIMIENTOS

Premio UNICEF en 2013.

Condecorado con la Cruz de la Orden del Mérito.

LIBROS

Entre otros: “Autorregulación Digital” | “Cariño he conectado a los niños” | “Adolescencia y drogas de diseño” | “Acoso Escolar” | “Adolescentes y alcohol”

SUMARIO

CEU Colegios

INTRODUCCIÓN

La seguridad en los entornos digitales es algo que tienes que tomarte muy en serio, tanto si te interesa la informática como si te interesa muy poco. Ya no estamos hablando de virus que pueden estropear el ordenador de casa o de fraudes a través de internet, sino de **situaciones que suponen una amenaza real para ti como adulto, para tu familia y para tu trabajo.** No se trata "únicamente" de cuestiones económicas, sino que afectan también a la privacidad y seguridad de las personas a las que quieres o con las que te relacionas en el entorno familiar, social y laboral.

En términos generales, lo que necesita un ciberdelincuente es que te descargues un archivo que ha preparado, o pinches en un enlace que te llevará a un sitio en el que se producirá la descarga de ese archivo. En otras ocasiones necesita que le facilites tus datos, y para conseguirlo crea una página falsa que parece oficial. Es decir, **necesita que caigas en una trampa.** Te dejará un caramelo para que lo cojas pero, si no lo haces, difícilmente podrá entrar en tu móvil, tablet u ordenador. **La inmensa mayoría de los ataques solo tienen éxito si cometes un error.** Aquí es donde surge lo que denominamos ingeniería social. Si no eres fácil de engañar, el ciberdelincuente necesita entonces investigar más sobre ti y saber más cosas, para conseguir que cojas su caramelo y caigas en su engaño.

> La inmensa mayoría de los ataques en línea tienen éxito gracias a errores humanos, y no por sofisticados sistemas informáticos.

No cometas el error de pensar que este tema no va contigo, o que es muy minoritario. **Los ciberdelitos se han duplicado en los últimos 4 años.** En 2020 se denunciaron 260.000 delitos de este tipo en España, según datos del Ministerio del Interior. Esto supone 712 ciberdelitos diarios, **más todos aquellos que no llegan a denunciarse.** Se trata ya del segundo delito común más denunciado en España. Y no estamos hablando solo de estafas económi-

cas, sino también de situaciones que afectan a la privacidad y a la seguridad de las personas, de las familias y de las empresas.

> 2020 > 712 CIBERDELITOS DIARIOS
>
> 2022 > 1.054 CIBERDELITOS DIARIOS

Veamos un caso. Luis es un trabajador de una pequeña empresa. Sabe muy bien que debe borrar directamente correos electrónicos de remitentes extraños y nunca abre archivos adjuntos sin saber qué contienen. Sabe lo que es el spam y lo que es el phishing, y nunca ha caído en uno de esos mensajes en los que te piden que entres en la web de tu banco para confirmar tus datos. Es decir, tiene algo de formación en ciberseguridad y es cuidadoso. Sin embargo, esta mañana ha pinchado en un enlace que le ha llegado en un correo y se ha descargado un virus sin saberlo. El virus se ha extendido rápidamente y ha encriptado el contenido de los ordenadores de su empresa. Alguien les pide ahora un rescate en bitcoins para poder recuperar todos los archivos de los ordenadores. Mientras tanto **la empresa está paralizada.** ¿Cómo ha caído Luis en la trampa?

Resulta que un ciberdelincuente se ha tomado la molestia de buscar a familiares de Luis en la red social de moda, y ha dado con su hija. Revisando las publicaciones de la adolescente, ha encontrado una en la que aparece una foto con la frase *"Deseando veros en Villabotijo de Arriba".* Resulta que es el lugar al que acude su familia cada año para celebrar las navidades. **Una vez que el ciberdelincuente obtiene un dato interesante lo utilizará.** Sabe que si envía a Luis un correo electrónico sospechoso no tendrá éxito, pero puede aprovechar la información que acaba de conseguir. En este caso redacta y envía un correo electrónico que lleva por título: *"Ubicación de los nuevos radares que el ayuntamiento ha puesto en Villabotijo de Arriba".* El correo incluye un enlace al mapa en el que se especifica dónde están situados los radares. Cuando Luis ha recibido este correo, lo ha abierto alarmado y ha pinchado en el enlace. En cuestión de segundos ha caído en la trampa.

Esto es ingeniería social. **Saber cosas sobre ti para conseguir que hagas algo,** que hagas clic sobre un botoncito o que pinches en un enlace. Y **cuanta más información exista en la red, publicada por ti o por tus familiares, más vulnerable serás.** Esto afectará a otras personas o entidades con las que te relaciones a través de ese dispositivo que ha sido infectado. Luis podría ser también un abogado en una asesoría o en su despacho, un médico en su consulta privada, un cargo intermedio de una sucursal bancaria o cualquier otro profesional.

En esta guía pondremos más ejemplos y explicaremos con más detalle en qué consiste cada sistema utilizado. Las amenazas a las que nos vamos a referir son bastante variadas, aunque siguen unos patrones que nos permitirán llegar a una serie de conclusiones fáciles de entender y de aplicar. Explicaremos los sistemas a los que hay que prestar más atención. Explicaremos de forma amena, clara y con ejemplos lo que es el phishing, el smishing o el ransomware, entre otros, para que cualquier persona pueda educar a sus hijos sobre estas amenazas.

Hablaremos también sobre las usurpaciones de identidad, y el riesgo que conllevan. En las formaciones con alumnos de colegios suelen surgir frases como: *"Mis datos no le interesan a nadie", "Yo no soy famoso, así que en mí nadie se va a fijar", "Yo no he hecho nada malo y no tengo nada que ocultar", "Si quieren mi información solo para ponerme anuncios me da igual",* etc. Es necesario hacerlos conscientes de que **toda persona y toda información es muy importante en internet.**

Entre otras razones, conseguir tus datos es importante para poder usurpar tu identidad y actuar en tu nombre. Crear una cuenta o un perfil en una red social, con tus datos, puede hacerse fácilmente, y con distintos objetivos. Por ejemplo: para **cometer delitos desde tu perfil, hacer compras o ventas fraudulentas** utilizando tu identidad, publicar **mensajes de odio o contrarios a algún gobierno o entidad** en tu nombre, o hacer que formes parte de una *red zombie* y **participes en ciberataques sin que seas consciente de ello.**

Al margen de las usurpaciones de identidad, hablaremos además de fenómenos como el cibergrooming o **acoso sexual a menores** en internet, que son mucho más efectivos y dañinos cuanta más información encuentra el ciberdelincuente. Asociados a este fenómeno están los problemas de sextorsión y el sexting, que también explicaremos.

En definitiva, niños y adolescentes pueden ser objeto de acoso sexual, usurpaciones de identidad y otras situaciones, pero pueden convertirse también en el objetivo de ciberataques de ingeniería social para poder llegar, a través de ellos, a los adultos de su entorno.

Recuerda siempre una cuestión: **un grupo, una familia o una empresa es tan fuerte como su eslabón más débil.** El eslabón débil permite fácilmente el acceso a toda la cadena, por lo que hay que fortalecerlo, y eso significa formarte sobre cuestiones básicas de ciberseguridad.

Esta guía te permitirá contar con información actualizada, protegerte correctamente y formar a tus hijos, familiares, amistades y entorno laboral. No plantearemos solo los problemas, sino también estrategias preventivas y soluciones.

USURPACIONES DE IDENTIDAD

Identificar y reaccionar

Se trata de un fenómeno creciente especialmente en el entorno de las redes sociales.

La mayoría de los adolescentes tienden a pensar que las usurpaciones de identidad son algo que solo afecta o debe preocupar en todo caso a personas famosas, pero esta percepción en absoluto responde a la realidad. En función del objetivo del ciberdelincuente, **cuanto más anónima sea la persona, mejor.**

Para empezar, hay que aclarar que **solo hablamos de suplantación de identidad cuando alguien se hace pasar por otra persona que existe.** Es decir: crearse un perfil en una red social inventándose un nombre y apellidos o utilizando un *nickname* o nombre inventado, no es un delito. No obstante, algunas redes sociales exigen a sus usuarios que utilicen sus datos reales, por lo que podrían eliminar una cuenta que no responde a ninguna identidad.

En España, la figura legal que contempla esta circunstancia es lo que se conoce como «usurpación de estado civil», recogida en el Artículo 401 del Código Penal, que puede conllevar penas de prisión de hasta 3 años.

> Para demostrar la usurpación de estado civil, tiene que quedar claro que otra persona está intentando hacerse pasar realmente por nuestro hijo, con el objetivo de obtener un beneficio o causar algún daño.

En algunos casos las usurpaciones de identidad las llevan a cabo amigos o conocidos, y suelen iniciarse como una broma. Pero si no es así, la persona que lo hace puede terminar causando muchos problemas.

Problemas que puede causar

En función de las intenciones que tenga el ciberdelincuente, podemos hablar de cuatro grupos de problemas:

- **De reputación digital.** El ciberatacante puede utilizar el perfil del adolescente como altavoz para decir cosas que no quiere decir con su identidad real, por ejemplo para apoyar a grupos radicales, colgar imágenes o vídeos, y que parezca que quien los difunde es el adolescente cuya identidad ha robado. Si lo hace públicamente, puede acarrear un problema importante para la imagen y reputación del menor.
- **Problemas de convivencia.** Es posible que utilice el perfil para generar conflictos entre el adolescente y las personas con las que se relaciona. Si conoce a sus amistades, compañeros del colegio, profesores o vecinos, puede insultarlos, enviar imágenes desagradables, etc. Si los demás creen que ese perfil es real del adolescente, será necesario dar muchas explicaciones para convencerles de que no es así.
- **Problemas de seguridad.** Si el objetivo del ciberdelincuente es causar daño, puede utilizar ese perfil falso para amenazar o provocar a personas peligrosas. Por ejemplo, podría insultar a un grupo problemático de otro centro escolar y citarlo a la salida de clase; o contratar en nombre del adolescente servicios por los que no pague y generar una posible deuda con individuos poco recomendables.
- **Problemas legales.** También es posible que utilice la cuenta falsa para difundir mensajes ilegales o contenidos delictivos: desde pornografía infantil hasta manuales de elaboración de explosivos. También existe la posibilidad de que la utilice para cometer estafas, engañar a otras personas o incluso participar en ataques informáticos a otros usuarios.

Dos formas de usurpación de identidad

En algunas usurpaciones de identidad, el ciberdelincuente **se apodera de la cuenta real del adolescente en lugar de crear una nueva.** Esto sucede cuando el atacante consigue el usuario y la contraseña, y accede sin dificultad. Esta situación suele ser consecuencia de errores cometidos por el propio usuario. Es muy importante que transmitas a tus hijos una serie de normas básicas sobre el uso de contraseñas:

1. **Las contraseñas son privadas y no se comparten con los amigos bajo ninguna circunstancia.** En ocasiones se las dicen como muestra de confianza, o utilizan los dispositivos de sus amigos para acceder en una situación puntual y después dejan la sesión abierta. Si un amigo tiene que ver su contraseña por alguna razón, deben cambiarla en cuanto tengan ocasión.
2. **Las contraseñas no pueden ser fáciles.** Deben ser como mínimo alfanuméricas, con letras y números, incluyendo además alguna mayúscula en algún sitio. Si pueden utilizar símbolos (por ejemplo +, %, $) mejor aún.
3. **No se puede utilizar la misma contraseña para todo.** Es importante tener varias contraseñas para utilizar en las distintas herramientas.
4. **Es importante cambiar las contraseñas de vez en cuando.** No se recomienda estar durante años utilizando la misma contraseña.
5. **Las contraseñas se apuntan.** Pero no se escriben en un post-it que luego se lleva en el estuche, en la funda del teléfono móvil o pegado en el ordenador. Ese papel se deja en casa, dentro de un libro o similar.
6. **También es interesante utilizar llaveros de contraseñas,** que pueden crear y cambiar nuestras contraseñas de forma aleatoria. Existen diversos gestores de contraseñas descargables tanto del Apple Store como desde Google Play.

La segunda forma de usurpación de identidad es la señalada anteriormente, en la que un ciberdelincuente crea **un perfil nuevo utilizando los datos y fotos que ha encontrado en el perfil real.** Es importante concienciar a los

adolescentes sobre la importancia de proteger su privacidad y actuar en caso de detectar una usurpación. Tus hijos deben saber que pueden contar contigo también para estos temas, y que harás todo lo que esté en tus manos.

En caso de que se efectúe la usurpación, haz lo siguiente:

1. **Comunica el hecho a la propia red social,** tal y como se especifica a continuación para las dos redes más utilizadas.
2. **Denuncia ante las fuerzas y cuerpos de seguridad,** tanto para proteger la identidad y privacidad de tus hijos, como para advertir sobre la posible comisión de delitos desde esa cuenta. Seguramente no será utilizada para nada lícito. Para denunciar deben dirigirse preferiblemente a las unidades de Policía y Guardia Civil especializadas en delitos tecnológicos.

PARA DENUNCIAR:

Brigada Central de Investigación Tecnológica de la Policía:

https://bit.ly/3fFa6VF

Grupo de Delitos Telemáticos de la Guardia Civil:

https://bit.ly/3rXvc49

3. **Denuncia ante la Agencia Española de Protección de Datos (AEPD)** la utilización de fotos y datos personales de tus hijos sin autorización. La AEPD puede imponer sanciones importantes.

DENUNCIAR EN INSTAGRAM

1. Entrar en el perfil propio y pinchar en Opciones (tres rayitas o puntitos arriba a la derecha).
2. Pinchar en CONFIGURACIÓN.
3. Pinchar en AYUDA.
4. Pinchar en AYUDA SOBRE PRIVACIDAD Y SEGURIDAD.
5. Pinchar en DENUNCIAR CUENTAS Y PUBLICACIONES.

Para ir directamente al formulario sobre suplantación de identidad pinchar en:
https://help.instagram.com/contact/636276399721841

DENUNCIAR EN TIKTOK

- Si la cuenta real ha sido robada:
  1. Iniciar y pinchar en ¿OLVIDASTE TU CONTRASEÑA?
  2. Elegir el CORREO o TELÉFONO que tenga vinculado.
  3. Se recibe un email con un enlace y una contraseña.
- Si la cuenta es falsa:
  1. Ir a la página de perfil del usuario en cuestión.
  2. Pulsar sobre los tres puntitos y selecciona DENUNCIAR.

Como forma de prevención, recomendamos a los adolescentes que practiquen de vez en cuando el *egosurfing,* es decir, **buscarse a sí mismos en internet.** Esto puedes hacerlo también desde la familia, por tres razones básicas:

- Saber qué información circula sobre tus hijos por internet y las redes sociales, e identificar a la persona que la haya publicado.
- Averiguar si existen otras cuentas creadas con su nombre y apellidos para hacerse pasar por tus hijos.
- Evitar que se cometan delitos utilizando su nombre o datos personales.

El *egosurfing* sirve para cuidar su reputación en internet, pero también para prevenir situaciones graves que podrían meterles en un problema legal e incluso impedirles el acceso a otros países.

EL PHISHING

En qué consiste

Podríamos definir el phishing como el conjunto de técnicas que se desarrollan para **lograr, mediante el engaño, datos sensibles de usuarios de internet,** desde su número de tarjeta de crédito, a claves de acceso a distintos servicios. Estos ataques son una verdadera amenaza para la seguridad de las personas, las familias, las empresas y todo tipo de entidades, y están aumentando de forma exponencial y haciéndose cada vez más sofisticados.

Los ataques a personas son habitualmente más comunes y sencillos, y suelen llevarse a cabo de forma masiva. **La inmensa mayoría de los ataques de phishing tienen éxito gracias a errores humanos:** personas que abren un documento adjunto que no deberían haber abierto o que pinchan en un enlace que lleva a un sitio desconocido.

> Un alto porcentaje de los internautas españoles, que hace unos años se situaba ya en el 25%, ha sido objeto de un ataque de phishing masivo.
>
> España es en la actualidad uno de los principales objetivos de los individuos y grupos que se dedican a realizar ciberataques, habiéndose convertido en su tercer objetivo favorito a nivel internacional, solo por detrás de Estados Unidos y Alemania.

El sistema más habitual que utilizan los ciberdelincuentes es el envío masivo de correos electrónicos con archivos adjuntos, o con enlaces a sitios supuestamente oficiales. De hecho, en la actualidad el 93% de los ciberataques comienzan con un simple correo. Veámoslos por separado.

1. CORREOS CON ARCHIVOS ADJUNTOS

El virus que permite al ciberdelincuente acceder al contenido de tu dispositivo y manejarlo, se encuentra en el archivo adjunto. Normalmente se trata de **un troyano, que se instala en cuanto lo abres. Suele ir camuflado como un archivo común:** un ZIP o un RAR, un PDF, incluso aparentes archivos de Microsoft Office: documentos de Word (DOC, DOCX), hojas de cálculo de Excel (XLS, XLSX, XLSM), o presentaciones y plantillas (PPT, PPTX).

Los mensajes variarán en función de la creatividad de los ciberdelincuentes. Una vez introducidos en tu ordenador, podrán hacer lo que quieran: desde instalar un ransomware o "secuestro de datos" para pedir después una cantidad de dinero a cambio del desbloqueo, hasta acceder a los datos personales de tu familia.

Estos mensajes resultarán aún más efectivos en función de cómo vayan vestidos, por ejemplo, si incluyen **palabras como "urgente", o "importante", fijan plazos muy cortos** para descargarse el documento o advierten de **consecuencias graves** si no se realiza la acción solicitada.

La mayoría de los correos de phishing **son bastante genéricos.** No saben a qué tipo de entidad, empresa o particular van a terminar llegando, por lo que suelen incluir mensajes que puedan ser asumidos por el mayor porcentaje posible de personas.

Veamos ejemplos de correos con los que es fácil que alguien llegue a abrir el archivo adjunto y se descargue el virus:

- El remitente puede parecer de **cualquier empresa de compra en internet,** tiendas de tecnología, grandes almacenes, etc. Comunican que han **actualizado las condiciones de uso** de su servicio, adjuntan un documento informativo que contiene el archivo malicioso.
- Mensaje informando que **se han localizado algunas cuentas tuyas que parecen inactivas,** por ejemplo de correo electrónico, videojuegos o tiendas de ropa; y que, si no indicas lo contrario, procederán a su eliminación.

- **Mensaje de Correos o de alguna empresa de mensajería express** diciendo que tienen un paquete tuyo y adjuntan un formulario para poder retirarlo o recibirlo en casa, por ejemplo un formulario de aduana.
- **Correo en el que te dicen que el pedido que has hecho ya ha salido y será entregado en los próximos días.** Te adjuntan un documento con la información y detalles del pedido.
- **Comunicados de tu banco con todo tipo de excusas:** problemas de seguridad, confirmación de datos, etc. Como en los casos anteriores, el archivo contiene el virus.

2. WHATSAPP O PRIVADOS EN REDES SOCIALES

En estos casos los mensajes no contienen virus alguno, pero **enlazan a sitios fraudulentos que usurpan la identidad de sitios reales u oficiales.** En esos sitios te pedirán tu usuario y contraseña para acceder, y quedará registrado para ellos desde ese momento.

El sistema más común suele realizarse a partir del envío de un correo que parece de **nuestro banco,** solicitando que entremos con cierta urgencia con la excusa que sea: un problema de seguridad, una verificación urgente, un cambio en la normativa del banco o de Hacienda, o similares. Al pinchar en el enlace, te lleva a **una web idéntica a la web oficial que conoces.** Entras, escribes tu usuario y contraseña y te da error. Te indica que has metido mal uno de los dos datos, y que vuelvas a intentarlo. Pinchas en el botón para reintentar **y te lleva a la web verdadera.** Escribes tu usuario y contraseña y entras en tu cuenta sin ningún problema. **Piensas que está todo bien y que antes has debido meter mal las claves. Pero no es así:** has dejado tus claves en un sitio fraudulento que después, para que no sospeches, te ha llevado a la web oficial. Te quedarás tranquilo, mientras tus claves ya están en manos de ciberdelincuentes[1].

1. Cánovas, G. (2021). Autorregulación Digital. Cómo educar en el uso responsable de la tecnología. Biblioteca Innovación Educativa. Editorial SM.

Si esto te sucede, **lo primero que debes hacer es cambiar tu contraseña y notificar al banco lo sucedido.** Es probable que tengas que reenviar el mensaje o correo fraudulento y denunciarlo.

Algunos ejemplos:

BANCO XXX (logo e identidad exactas de nuestro banco)

Estimado (a) Cliente
Asunto: Error de sesión
Remitente: Servicio al cliente

Lamentamos comunicarle que su último servicio al Banco XXX en línea no finalizó de manera correcta, así que le pedimos que por su seguridad termine la sesión de inmediato.

Para evitar que su acceso sea manejado por personas ajenas a usted.

Para finalizar su sesión por favor entre AQUÍ.

Ante cualquier consulta puede contactarnos a nuestro servicio de atención a Clientes en el teléfono xxxxxxxx, disponible las 24 horas del día, o a través de nuestra página web xxxxx.

Saluda atentamente a usted
XXX

BANCO XXX (logo e identidad exactas de nuestro banco)

De acuerdo con la nueva legislación europea de Sistemas de Pago, tuvimos que suspender el acceso en línea de su cuenta por razones de seguridad!

Por favor descargue y complete el archivo adjunto a este correo electrónico.

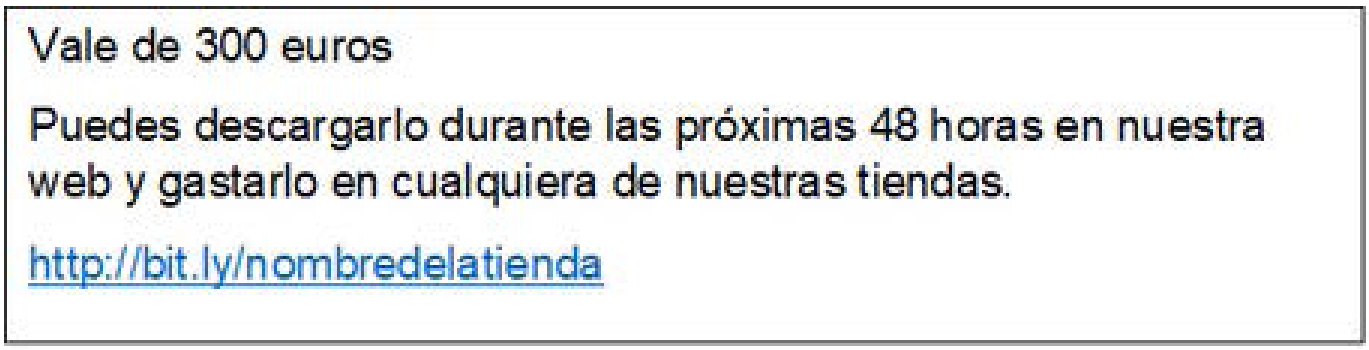
NOTA: su cuenta puede ser automáticamente suspendido hasta que la actualización e hizo a su favor profilo. Si tomar medidas inmediatas.

Gracias por su cooperación.

Banco XXX

CIF

Otro sistema muy utilizado es el envío de whatsapp o privados en redes sociales en los que te llegan **vales de descuento de comercios conocidos.** Es recurrente el mensaje en el que recibes un vale de descuento de 300 euros de una conocida cadena de tiendas de ropa. Se especifica que tienes que descargar el vale en el móvil y dispones solo de 48 horas para gastarlo. El enlace que se incluye no pertenece a la cadena de tiendas, pero puede parecerlo.



3. APPS MALICIOSAS

Un tercer sistema también utilizado para la distribución de virus es la **creación de aplicaciones con el código malicioso ya incorporado.** Estas apps pueden encontrarse en páginas y sitios diversos: páginas web que aparecen y desaparecen al poco tiempo y que ofrecen increíbles descuentos o premios de todo tipo, sitios de pornografía y contenidos para adultos, sitios de piratería, o incluso en algunas ocasiones en plataformas oficiales como el Google Play Store. **No es recomendable la descarga de aplicaciones fuera de las plataformas oficiales,** y en las mismas debemos tener mucho cuidado cuando se trate de aplicaciones que no conocemos o que **llevan muy poco tiempo en circulación.**

Cómo actuar ante el *phishing*

Antes de hablar de las pautas a seguir para prevenir o actuar ante un ataque de phishing, es importante recordar que en estos momentos es básico y fundamental utilizar en nuestros dispositivos programas anti-malware y spyware: **como mínimo un buen antivirus**. Existen antivirus para todo tipo de herramientas, incluso gratuitos. Es importante actualizarlo constantemente. **Si no lo actualizas no podrás protegerte de los virus nuevos que comienzan a**

circular cada día. Del mismo modo debes actualizar siempre el sistema operativo, programas y aplicaciones que tengas instaladas.

> Algunos de los antivirus más reconocidos: Bitdefender, Panda, Kaspersky, Norton, McAfee, Avast, ESET, BullGuard, Avira y AVG.

Antes de abrir un archivo adjunto o pinchar en un enlace debes:

1. CONFIRMAR LA PROCEDENCIA. Si no conoces al remitente, no abras el archivo. Selecciona el correo y bórralo directamente. Si conoces al remitente, es aconsejable ponerte en contacto con él para **confirmar que te ha enviado un correo y qué contiene el archivo adjunto**, en especial si no estabas esperando nada, ya que algunos **ciberdelincuentes envían correos con remites que han obtenido previamente,** para que la víctima confíe y los abra. Esto, como casi cualquier otra cosa en internet, puede hacerse sin demasiado problema.
2. VERIFICAR LA DIRECCIÓN DEL SITIO. Si el mensaje o correo te remite a una dirección web, **verifica que es la dirección oficial.** Si se trata de un banco no accedas **desde el mensaje,** sino desde el navegador o medio que ya hayas utilizado en otras ocasiones. Si nunca has accedido, utiliza un buscador, como Google, y teclea el nombre de la entidad. El primer resultado que te dé el buscador será la dirección oficial.
3. REPASAR LA ORTOGRAFÍA Y LA REDACCIÓN. Los textos que acompañan a los mensajes de phishing suelen estar mal redactados, con incongruencias de número, por ejemplo, o con erratas o faltas de ortografía.
4. DESCONFIAR DE VALES Y REGALOS EN INTERNET. Con frecuencia se trata de señuelos para que entres en sitios o facilites datos personales.

Smishing

Una de las formas de phishing más efectiva suele ser el desarrollado **a través de mensajes SMS** en lugar de correos electrónicos o mensajes de whatsapp. Tendemos a considerar que los mensajes de texto son más serios, y suelen ser utilizados por algunas entidades para comunicarse con sus clientes, como compañías de telefonía móvil.

Pero, cuando una entidad conocida realiza un envío de SMS, **no pide la confirmación de datos personales a sus clientes.** Normalmente se trata de promociones, ofertas o recordatorios que no requieren de una interacción con el mensaje. Esto no siempre es así, como ha sucedido por ejemplo con las notificaciones de fechas para la vacunación por COVID en las que se pedía incluso una confirmación; pero dichos mensajes ya llevan incluidos tus datos, **no requieren que facilites otros** y utilizan enlaces a sitios oficiales.

Spear phishing

Hasta ahora hemos visto las técnicas más utilizadas para el phishing masivo, o poco selectivo, pero cuando los ciberdelincuentes **seleccionan a una persona o tipo de trabajador en concreto,** desarrollan otra serie de técnicas. Una de ellas es la llamada spear phishing.

Esta técnica requiere de un conocimiento previo del objetivo, que puede haber sido **seleccionado por su relación con informaciones o datos muy sensibles o interesantes, o directamente por un encargo.**

Es un trabajo de ingeniería social, que implica estudiar a las entidades que se relacionan con la que va a ser atacada, sus proveedores, clientes, etc. Esa información será utilizada para **crear un correo que resulte absolutamente creíble para la persona que lo vaya a recibir.** Puede crearse un mensaje que parezca provenir de un cliente, por ejemplo, notificando que ha procedido a demandar a la empresa y que adjunta una copia de la demanda. Puede ser un proveedor enviando sus novedades de servicio, o utilizarse una vía más personal.

Catphishing

Bajo esta modalidad, el ciberdelincuente **crea una cuenta en una red social adoptando una identidad falsa que pueda resultar atractiva para el objetivo,** en función de sus características y de la información previa de la que ya disponga. Puede ser desde un perfil de alguien que ha estudiado en el colegio o instituto en la misma época que la víctima, hasta un perfil de alguien que muestra los mismos gustos musicales o ideología política.

En función del tiempo de preparación que quiera dedicarle el ciberdelincuente, puede alimentar ese perfil con información diversa, fotografías que habrá obtenido de otros perfiles en otras redes sociales, **o incluso haber contactado previamente con personas conocidas por la víctima** para que vea que comparten amistades.

Uno de los sistemas empleados consiste en crear perfiles falsos en **redes sociales de contactos y servicios para establecer relaciones de pareja.**

Una vez creado el perfil con las fotos y las características adecuadas, basta con mantener conversaciones sobre gustos, inquietudes y demás temas. Esas conversaciones, además de para obtener nueva información o verificar la que ya se posee, permitirán **obtener finalmente el correo electrónico del objetivo o su número de móvil** para continuar la relación por mail o por whatsapp. Una vez ganada la confianza todo es tan sencillo como enviar un mensaje con un enlace diciendo algo como: “no te puedes perder esto… luego me dices qué te parece”, o un correo electrónico con un archivo o un zip que lleve por título: “esas fotos mías”. El texto que acompañe el mensaje será determinante para conseguir que la víctima se lo descargue.

Una persona que caiga en esto puede comprometer la privacidad y la seguridad de sus familiares, la de sus compañeros de trabajo y la de toda la empresa. En cuanto el virus tenga acceso al listado de contactos o correos electrónicos y llegue a los ordenadores de las demás personas, el ciberdelincuente dispondrá de un enorme abanico de posibilidades.

> Es llamativa la facilidad con la que muchos adolescentes, y también adultos, facilitan su número de móvil o su correo electrónico a personas que acaban de conocer. Cuando el contacto se inicia en un entorno digital es necesario extremarse las precauciones.

Vishing

Se trata de una variante del phishing, pero en la que se utiliza la voz humana. Suele llevarse a cabo **mediante una llamada telefónica,** en la que una persona se identifica como responsable de la seguridad de nuestra cuenta bancaria, de nuestra compañía telefónica o de cualquier otra entidad. Necesita realizar comprobaciones o ayudarnos a **solucionar un supuesto problema,** y a lo largo de la conversación va obteniendo los datos personales que le interesan. Puede también redirigirnos a una dirección web, o pedirnos acceso remoto a nuestro dispositivo para ayudarnos con cualquier cuestión.

En ocasiones, este sistema puede ir **precedido de un SMS** en el que se nos advierte sobre el problema que tenemos o vamos a tener. Después nos dicen que se pondrán en contacto con nosotros vía telefónica para solucionarlo.

Ingeniería social

Ingeniería social es el término que utilizamos al trabajar sobre ciberinteligencia, para referirnos a la **labor de investigación que se lleva a cabo para obtener información sobre una persona con el objetivo de hacerla más accesible.** Implica además el posterior desarrollo de **técnicas y estrategias personalizadas de engaño,** para lograr que dicha persona facilite sin quererlo el acceso a su dispositivo o a información más personal. La víctima puede incluso no ser consciente en ningún momento de la situación que se está desarrollando.

En la introducción veíamos el ejemplo de Luis, un trabajador cualquiera de una pequeña empresa de transporte - en España, el 94% de las empresas son PYME- que se encarga de temas administrativos, pagos de facturas, etc. Se trata de una persona con ciertos conocimientos, **sabe lo que es el phishing y nunca abre archivos adjuntos sin saber qué contienen, ni pincha en enlaces sin saber dónde terminan.** Pero, un día pincha en un enlace que le ha llegado en un correo y se ha descargado un virus sin saberlo. El virus se ha extendido rápidamente y ha encriptado

el contenido de los ordenadores de su empresa. Alguien les pide un **rescate en bitcoins para poder recuperar todos los archivos de los ordenadores. Mientras tanto la empresa está paralizada.** Luis ha sido víctima de un ataque de ingeniería social.

Como explicábamos en la introducción, un ciberdelincuente se había tomado la molestia de buscar a familiares de Luis en la red social de moda, y había dado con su hija. Revisando las publicaciones de la adolescente, una foto había puesto a su disposición una información muy interesante: el sitio habitual en el que la familia pasa las navidades. Utilizando este dato había creado un correo electrónico con una noticia falsa alertando sobre los nuevos radares colocados por el ayuntamiento en la población. Un archivo adjunto o un enlace al sitio web específico habían completado la jugada.

Es muy importante el texto y la información que facilita después el ciberdelincuente. Los nuevos radares en la población son un buen tema, pero otro podría serlo la presencia de agua contaminada, por ejemplo. El ciberdelincuente podría haber mandado otro correo con el siguiente titular: “El agua del grifo de Villabotijo de Arriba podría estar contaminada”. En el mismo correo, en el sitio creado para colgar la notica falsa, podría incluir un texto como este:

> *“En algunas zonas de la población se han identificado concentraciones elevadas de contaminantes peligrosos para la salud como los trihalometanos (THM) —entre ellos cloroformo, bromoformo, bromodiclorometano o el dibromoclorometano-. El ayuntamiento ha publicado un listado con las calles que se están viendo afectadas y recomendaciones para los vecinos, o para los visitantes que se alojen en casas de la zona”.*

El correo, o el enlace, pueden facilitar el acceso al supuesto listado en un sencillo formato PDF. En ese archivo puede encontrarse el código malicioso que permitirá después al ciberdelincuente acceder al terminal y a la información que desee.

El problema añadido de los ataques de ingeniería social es que **no son fáciles de detectar, y la víctima puede no llegar a ser consciente de lo que está sucediendo.** Sus datos pueden ser utilizados directamente por quien los obtuvo o **vendidos en la dark web** a cambio de poco dinero.

RANSOMWARE

El secuestro de datos

El ransomware es un software malicioso que, al entrar en tu dispositivo, cifra por completo el sistema operativo o solo algunos de los archivos. A continuación **pide un rescate a cambio de facilitarte la forma de descifrar y recuperar toda tu información.**

El rescate varía en función de que se trate de un ataque a particulares, a pequeñas o a grandes empresas, pero **el mínimo suele estar en unos 3.000 euros.** Se paga normalmente en criptomonedas como los bitcoins.

Esta forma de ataque se ha duplicado en los últimos años. En 2018, por ejemplo, se detectaron 851 millones de ataques ransomware en el mundo. Se produce una infección cada pocos segundos. Algunos de los ataques más

dañinos sufridos por empresas importantes se han realizado mediante este sistema.

El DarkSide, por ejemplo, fue empleado en mayo de 2021 para bloquear uno de los oleoductos más importantes de Estados Unidos, el Colonial Pipeline, que abastece a 50 millones de personas de la costa este. Las autoridades norteamericanas ofrecen una recompensa de 10 millones de dólares a quien facilite información que permita identificar a los desarrolladores de este tipo de ransomware.

Más de la mitad de las infecciones con ransomware tienen lugar por medio de ataques de ingeniería social. Es decir, se parte de una información previa que permite después engañar al usuario y provocar que se descargue el virus. De ahí la importancia de educar a todos los miembros de la familia con acceso a la descarga de archivos, o que utilicen el navegador de tu dispositivo. Dejar en sus manos el dispositivo en el que tienes todos los correos, archivos y documentos de tu trabajo no es una buena idea.

Cómo actuar

Lo último que se recomienda en caso de ataque de ransomware es pagar el rescate, por dos razones: primero, nada te garantiza que el ciberdelincuente vaya a facilitarte después las claves que permitan desencriptar tus archivos. En ocasiones puede que ni tan siquiera exista dicha clave. Segundo, nada impide al ciberdelincuente pedirte otro rescate más adelante. De hecho, ser víctima de un ciberataque exitoso multiplica las posibilidades de que te vuelvan a atacar. **Lo más recomendable es aislar el dispositivo infectado para evitar que se extienda y acudir a ayuda profesional** para afrontar la situación.

> En sitios web como NO MORE RANSOM puedes encontrar información sobre cómo afrontar un ransomware reversible:
>
> https://www.nomoreransom.org/es/index.html

Lo más importante en estos casos es sin duda la prevención:

- **Realiza copias de seguridad de todos tus archivos importantes.** Es recomendable realizarlas en discos duros externos u otros dispositivos, pero no en la nube. Si tus archivos se sincronizan con los que tengas en la nube, algunos tipos de ransomware podrían infectarlos también.
- **Ten siempre actualizado tu navegador y tu antivirus.**
- **Utiliza una VPN,** o máquina virtual, para que todo su tráfico de datos se transmita a través de un túnel virtual cifrado

MÁS SISTEMAS

Ventanas emergentes

En ocasiones no es necesario pinchar en un enlace malicioso o descargarse un archivo infectado por un virus. Los ciberdelincuentes pueden salir a tu encuentro y aparecer en páginas web mediante **ventanas emergentes** -pop ups- o incluso anuncios. Veamos los sistemas más empleados.

- ROGUES

El rogue software es un tipo de programa malicioso que te pretende engañar **haciéndote creer que tienes un virus en tu dispositivo.** Se trata de una ventana emergente, o un mensaje que aparece al acceder a una web, que incluye un texto alarmante como el siguiente: “Hemos identificado tres virus en su aparato. Debe descargarse urgentemente un antivirus que proteja su información”. Suele ir acompañado de un botón de descarga y, en efecto, al pinchar sobre el botón se produce la descarga, solo que del virus informático.

La prevención en el caso de los rogues es clara: **nunca debes fiarte de una web o un pop up que te advierte sobre la presencia de virus en tu dispositivo.** Una web no puede saberlo, y es un sistema clásico para provocar su descarga.

En todo caso, si tienes la menor duda, sal de dicha web y **busca antivirus accediendo directamente desde las búsquedas de Google o desde el Apple Store o Google Play.**

Los rogues son un tipo de scareware que pretenden asustarte para que hagas algo que no deberías hacer.

Ante una pantalla que **te alarma, amenaza o intenta asustarte** para que descargues un supuesto antivirus, **cierra tu navegador** haciendo lo siguiente:

- Pincha sobre la «X» que aparece arriba a la derecha de tu navegador.
- Si no aparece y usas Windows, pulsa las teclas Alt + F4 y así se cerrará la ventana activa.
- Si no lo consigues, pulsa las teclas Ctrl + Alt + Supr para abrir el Administrador de tareas de Windows y cerrar desde allí el navegador.

- MALWERTISING O MALVERTISING

Se trata de **anuncios publicitarios con código malicioso** que pueden aparecer en cualquier sitio, aunque con más frecuencia en páginas de contenidos pirateados, pornografía y similares. En ocasiones, este código puede infectarte **sin necesidad de que pinches sobre el mismo.** Puede tratarse de banners publicitarios de cualquier tema.

Para evitar este tipo de ataques es importante tener actualizado el **sistema operativo** del aparato que estés utilizando y también del **navegador**. El malwertising aprovecha las brechas de seguridad de las versiones obsoletas de distintos tipos de software, que aún mantienen aquellas personas que no hacen las actualizaciones.

Cebo o baiting

Esta práctica **aprovecha tu curiosidad** para entrar en tus dispositivos y puede tener como objetivo final tanto a empresas como a particulares.

Imagina que te encuentras un pendrive en una parada de autobús o en el metro, en los servicios de la biblioteca, en tu empresa o en el suelo junto a una máquina de bebidas… ¿qué harías? Seguramente después de leer todas estas páginas pensarías que puede contener un virus; pero si no tuvieras conoci-

mientos sobre estos temas es probable que lo introdujeras en tu ordenador de casa o del trabajo. Tu curiosidad te habría llevado a introducir un archivo malicioso que permitiría a otra persona acceder a toda tu información, encriptarla o hacer lo que quisiera con ella.

Como sucede con las técnicas de ingeniería social, **se puede dar un empujoncito si la persona es algo recelosa o desconfiada.** Bastará, por ejemplo, escribir sobre el pendrive con un rotulador indeleble frases como: “mis fotos”, “mejores vídeos” o cualquier frase similar. En función del “público” al que vaya dirigido puede llevar incluso el logo de una prestigiosa marca de videojuegos, coches o motos, de tal forma que pueda parecer un pendrive publicitario; u otro tipo de frases como: “wifi universal”, “mejores promociones”, etc.

Las wifis públicas

Muchos adolescentes buscan redes wifi gratuitas para conectarse a internet cuando salen de sus casas, para ahorrar datos o navegar más rápido si la wifi que encuentran es potente. Esta práctica no está exenta de riesgos que afectan tanto a su seguridad como a su privacidad.

Con los conocimientos necesarios, un ciberdelincuente puede habilitar su proprio dispositivo para **facilitar la conexión de otras personas bajo la apariencia de una wifi legal.** Si se encuentra en una cafetería, por ejemplo,

puede crear una conexión con el nombre de la cafetería. Quienes busquen un acceso a internet gratuito y abierto se conectarán a su dispositivo, sin saber que están accediendo a internet a través de la conexión de alguien que no tiene nada que ver con el establecimiento. El ciberdelincuente podrá, a partir de ese momento, acceder a los dispositivos conectados.

Los adolescentes deben respetar tres pasos para conectarse a una posible red wifi pública:

1. Preguntar al responsable del establecimiento, bibliotecario, camarero o encargado, si en dicho establecimiento hay wifi gratuita para los clientes. Lo habitual además es que esto esté indicado en diversos carteles.
2. Si es así debe preguntar a continuación el nombre de la red wifi. Puede que no sea el que pensamos en un principio, o pueden aparecer varios similares.
3. Solicitar la clave para acceder a la red inalámbrica.

No obstante, es conveniente también respetar una serie de pautas al conectarse a una wifi gratuita:

- **No abrir ninguna sesión en servicios a los que accedas con usuario y contraseña,** ya que estos datos podrían verse comprometidos. Evita especialmente el acceso a cuentas bancarias y compras.
- **Deshabilitar la sincronización entre dispositivos,** para evitar que algo que pueda entrar llegue al resto de aparatos que utilizas.
- **Utilizar una VPN,** o máquina virtual, para que tu tráfico de datos circule a través de un túnel virtual cifrado.
- **Eliminar los datos que hayan podido quedar tras la sesión** en tu dispositivo y, por supuesto, tener tu antivirus y cortafuegos actualizado.

Bluetooth: bluesnarfing

El bluetooth también puede convertirse también en la vía de entrada para los ciberdelincuentes. Permite el intercambio de datos a distancias muy cortas, lo que hace necesario que el ataque se produzca desde otro aparato situado muy cerca de donde estés.

El bluesnarfing no es otra cosa que el **robo de información desde un dispositivo inalámbrico a través de una conexión bluetooth.** Por esta vía se puede acceder a tus mensajes, agenda de contactos y demás información, con un problema añadido: no lo detectas y difícilmente quedará una evidencia del ataque.

Para prevenir el bluesnarfing se recomienda:

- **No activar el bluetooth mientras no se vaya a utilizar.**
- **No aceptar solicitudes de emparejamiento de dispositivos desconocidos.**
- **Tener actualizados los dispositivos con las últimas versiones de seguridad.**

CIBERGROOMING O ACOSO SEXUAL

Denominamos grooming o cibergrooming al acto de **acosar a un menor a través de internet con una finalidad claramente sexual.** El objetivo puede ser desde la obtención de imágenes de tipo pornográfico hasta el intento de concertar un encuentro en persona. Para alcanzar su objetivo, el acosador desarrolla toda una serie de estrategias entre las que se incluye el hacerse pasar por otro menor de edad.

No siempre es fácil reconocer a un acosador en internet. En ocasiones son personas que dicen claramente lo que están buscando, y a los pocos minutos de conversación ya están hablando sobre cuestiones sexuales y pidiendo fotografías. **En otros casos esconden muy bien sus objetivos,** no llaman la atención, manipulan y dedican tiempo a conseguir lo que quieren. Es muy importante aprender a identificarlos.

El grooming se distingue por estas cuatro características:

- **La persona que acosa es un adulto** y la víctima un menor de edad.
- **El objetivo del acoso es sexual,** y puede abarcar desde la obtención de fotografías inapropiadas del menor hasta el intento de concertar un encuentro físico.
- El adulto emplea estrategias para engañar al menor y manipularlo, y **normalmente se hace pasar por otro menor.**
- Los primeros contactos se establecen **a través de internet.**

¿Cómo actúan los acosadores en internet?

Los individuos que acosan a menores de edad en internet pueden ser más o menos anárquicos en ocasiones, pero con frecuencia son metódicos y pueden llegar a acosar a docenas de adolescentes al mismo tiempo. Alguno de los detenidos por este tipo de delito en España estaba acosando a más de 200 menores en el momento de su detención, y tenía toda la información e imágenes de sus víctimas perfectamente organizada en carpetas.

Podemos dividir la forma de actuar del acosador en varias fases:

- FASE DE ENGANCHE: Al principio el ciberdelincuente no hace muchas preguntas, las necesarias para saber la edad, sexo, ciudad y gustos básicos del menor, para determinar si se ajusta a lo que busca. A continuación **adapta su identidad;** se presenta como alguien cercano, de la misma edad o uno o dos años más. Comparte gustos musicales, deportivos… buscando establecer puntos en común y temas sobre los que hablar. Se muestra positivo, alegre, divertido y con ganas de ayudar.
- FASE DE FIDELIZACIÓN: El siguiente objetivo es mantener el interés del menor de edad, profundizar en los gustos y ofrecer información: desde trucos para mejorar en su juego favorito, hasta información curiosa o fotos de sus ídolos musicales. El agresor facilita información inventada sobre su persona, y envía fotos de otro menor usurpando su imagen (las obtiene de cualquier red social). Comienza a **tratar temas personales para conocer**

la situación familiar, si hay conflictos con los padres o hermanos y todo lo que pueda serle de utilidad. Intenta convertirse en confidente.

- FASE DE SEDUCCIÓN: Utiliza toda la información y confianza que ha conseguido para intentar seducir al adolescente. Lo manipula y condiciona hasta donde pueda diciéndole cosas como: "solo hablamos de esto si tú quieres", "no tienes por qué contestarme a esta pregunta", etc… Aquí acude ya al tema del sexo, habla de exnovios/as y **pide fotografías más atrevidas, o una videollamada** (aunque su webcam siempre resulta estar estropeada).
- FASE DE ACOSO: El acosador ya sabe lo que puede obtener del menor: si está dispuesto a engañar a sus padres o no, si acudiría a una "cita a ciegas", si le ha contado a alguien lo que han estado hablando, etc. Ahora comienza la presión, utiliza las fotos que ya tenga en su poder o montajes que haya realizado. Intenta además **hacerle cómplice o responsable de todo:** "Tú has querido", "yo no te he obligado a nada", "si cuentas algo de esto sabes lo que la gente va a pensar de ti…"

> En función de la edad que tenga tu hijo no es necesario que le expliques todas estas cuestiones, sino solo las normas básicas a seguir con los desconocidos en internet, que se señalan a continuación. Pero si crees que puede encontrarse ante una situación de cibergrooming, ver estas fases y reconocerlas sí puede ayudar a alertar al menor y activar su sentido crítico. En ocasiones la información realista y aséptica es lo más efectivo.

Hasta aquí hemos visto una forma habitual de actuación de los acosadores sexuales de menores. Otros pueden ser más directos o dedicarle menos tiempo a la manipulación, pero el objetivo es siempre el mismo. Antes o después llegarán exactamente al mismo lugar: les pedirán fotos, que se pongan delante de la webcam o querrán quedar a solas.

Para prevenir el cibergrooming es importante trasladar tres normas básicas a tus hijos:

- **No trates con personas en internet que no sabes realmente quiénes son.** Si por alguna razón has de hacerlo, nunca reveles datos personales que permitan identificarte, saber dónde vives o cuál es tu centro escolar.
- **Nunca envíes una fotografía a alguien que no conoces realmente, ni conectes la webcam con esa persona.**
- **Jamás acudas a una cita con alguien que te ha conocido a través de internet.** Si toda la información que tienes sobre su persona es la que te ha dado él mismo, y si las fotos te las ha enviado él, no puedes confiar. Y eso es lo primero que te pedirá: que confíes en él. Acudir en compañía de un amigo o amiga tampoco garantiza tu seguridad.

Si la situación de cibergrooming ya se ha producido, el menor debe saber que la forma de proceder es la siguiente:

- **No ceder jamás al chantaje.** El acosador amenazará con distribuir la fotografía que tenga si no recibe imágenes nuevas. Ya es un grave error

que haya conseguido esa foto con la que hacer chantaje, pero pensar que enviándole más va a cesar en su acoso es otro error mucho mayor. Nunca será suficiente y cada imagen o vídeo servirá para un nuevo chantaje.

- **Contarlo a los padres.** Los padres deben saber lo que está sucediendo. Una intervención suya a tiempo puede evitar que se produzcan situaciones mucho más graves.
- **Denunciar.** El grooming es un delito recogido en nuestro Código Penal. Debe ser denunciado siempre, tanto para solucionar un caso como para evitar casos nuevos.

PARA DENUNCIAR:

Brigada Central de Investigación Tecnológica de la Policía:

https://bit.ly/3fFa6VF

Grupo de Delitos Telemáticos de la Guardia Civil:

https://bit.ly/3rXvc49

Sexting

El sexting es una práctica que consiste en el envío de mensajes, fotografías o vídeos de contenido erótico o sexual protagonizados por la persona que los envía. Suele circunscribirse a un entorno íntimo, y son enviados con la confianza de que nunca llegarán a mostrarse o compartirse con terceras personas.

El problema surge cuando, como suele suceder, **la imagen termina en los móviles o correos de otras amistades.** En pocos días puede estar circulando de móvil en móvil e incluso terminar haciéndose pública en internet.

Es posible que algunos jóvenes no sean conscientes de los riesgos que supone hacerse y enviar una fotografía de tipo erótico, pero otros sí lo son.

> El sexting es una práctica peligrosa, que puede convertirse en la antesala del ciberbullying, o incluso del *cibergrooming* si las imágenes caen en manos de acosadores sexuales

Diversos estudios ponen de manifiesto que **los adolescentes suelen ser tan conscientes de los riesgos como los adultos, pero le dan mucha mayor importancia a la recompensa.** El problema del sexting es que algunos adolescentes piensan que vale la pena correr el riesgo si consiguen su objetivo. ¿Y cuál es el objetivo? Normalmente llamar la atención de alguien, o buscar aceptación.

Quien lo hace por buscar aceptación está haciéndose una foto que alguien le ha pedido. Alguien que insiste con el tema, y a quien hay que aprender a decir que no. **Una foto sin ropa no es una prueba de confianza, ni de amor, ni de fidelidad.**

Quien lo hace por iniciativa propia, para llamar la atención de otra persona, está utilizando una estrategia equivocada y peligrosa. Es importante que el adolescente entienda que **no es una forma correcta de relacionarse o de ganar la atención de alguien, y que el riesgo de su difusión no compensa en absoluto.**

> IMPORTANTE:
>
> La difusión de fotografías de menores de edad sin ropa es un delito en España. Tener dichas imágenes en el móvil u ordenador, o difundirlas entre otras personas puede acarrear graves consecuencias.

Sextorsión

La sextorsión consiste en **chantajear a la víctima bajo la amenaza de difundir imágenes suyas obtenidas de diferentes maneras.** Estas fotogra-

fías o vídeos pueden proceder de la práctica del sexting, de una acción previa de cibergrooming, o de la intromisión en el dispositivo de la persona chantajeada.

En muchas ocasiones, especialmente cuando se trata de menores de edad, **puede que el ciberdelincuente realmente no disponga de dichas imágenes.** Muchos usuarios de internet reciben con frecuencia correos en los que se afirma que han sido grabados desde la cámara de sus dispositivos mientras consumían pornografía o mientras de desvestían, y se les amenaza con difundir las imágenes si no pagan una cantidad de dinero, normalmente en bitcoins, a cambio del silencio del extorsionador.

> Tu reacción, como en el caso del resto de delitos, debe ser la denuncia inmediata de la situación ante las unidades especializadas de las Fuerzas y Cuerpos de Seguridad del Estado. No cedas nunca al chantaje y sigue las indicaciones que te den.

CEU

Colegios