# 1.5.3. Amenazas externas

## Phishing, qué es y cómo evitarlo

> El **phishing es una de las estafas con mayor trayectoria** y mejor conocidas de Internet. Es un tipo de fraude que se da en las telecomunicaciones y que emplea trucos de ingeniería social para obtener datos privados de sus víctimas. La diferencia entre Spam y Phishing es clara: el Spam es correo basura, no es más que un montón de anuncios no deseados. **El phishing por otro lado, tiene como finalidad robar tus datos y utilizarlos contra ti.**

La **mayor parte del phishing puede dar como resultado el robo de identidades o de dinero, y también es una técnica eficaz para el espionaje industrial y el robo de datos**. “Algunos hackers llegan incluso a crear perfiles falsos en redes sociales, invierten un tiempo en desarrollar una relación con las posibles víctimas y esperan a que exista confianza para hacer saltar la trampa”.

Un ataque de phishing tiene 3 componentes:

1. El ataque **se realiza mediante comunicaciones electrónicas, como un correo electrónico, un SMS o una llamada de teléfono.**
2. El atacante **se hace pasar por una persona u organización** de confianza.
3. El **objetivo es obtener información personal confidencial**, como credenciales de inicio de sesión o números de tarjeta de crédito.

> Como a veces es difícil detectarlo, aquí te dejamos una serie de **características y trucos que pueden funcionar** para **detectar** un intento de **phishing:**

- Sé **precavido ante los correos** que aparentan ser de entidades bancarias o servicios conocidos (Dropbox, Facebook, Google Drive, Apple ID, Correos y Telégrafos, Agencia Tributaria, etc.) con mensajes que no esperabas, que son alarmistas o extraños.
- **Sospecha si hay errores gramaticales en el texto,** pueden haber utilizado un traductor automático para la redacción del mensaje trampa. Ningún servicio con cierta reputación enviará mensajes mal redactados.
- Si recibes **comunicaciones anónimas del tipo “Estimado cliente”, “Notificación a usuario” o “Querido amigo”,** es un indicio que te debe poner en alerta.

Copyright 2026

- **Si el mensaje te obliga a tomar una decisión de manera inminente o en unas pocas horas, es mala seña**l. Contrasta directamente si la urgencia es real o no directamente con el servicio o consultando otras fuentes de información de confianza: la OSI, Policía, Guardia Civil, etc.
- **Revisa si el texto del enlace que facilitan en el mensaje coincide con la dirección a la que apunta,** y que ésta corresponda con la URL del servicio legítimo.
- **Un servicio con cierto prestigio utilizará sus propios dominios para las direcciones de email corporativas**. Si recibes la comunicación desde un buzón de correo tipo @gmail.com, @outlook.com o cualquier otro similar, sospecha.
- Aplica la **ecuación: solicitud de datos bancarios + datos personales** = fraude.

## Ciberacoso

UNICEF lo define como:

> Ciberacoso es acoso o intimidación por medio de las tecnologías digitales. Puede ocurrir en las redes sociales, las plataformas de mensajería, las plataformas de juegos y los teléfonos móviles. Es un comportamiento que se repite y que busca atemorizar, enfadar o humillar a otras personas.
>
> - **Difundir mentiras o publicar fotografías** o videos vergonzosos de alguien en las redes sociales.
> - **Enviar mensajes, imágenes o videos hirientes**, abusivos o amenazantes a través de plataformas de mensajería
> - **Hacerse pasar por otra persona** y enviar mensajes agresivos en nombre de dicha persona o a través de cuentas falsas.

Y por último, en el caso de que nuestro alumnado reciba el tan temido ciberacoso hay que enseñarles a gestionarlo:

- En un primer momento hay que **crear un clima de confianza con el menor** en el que entienda que se le escucha y se le apoya, evitando culpabilizar a nadie.
- Hay que **guardar evidencias** de la situación generada mediante capturas de pantalla de los mensajes, fotografías o vídeos.
- **Contactar con las Fuerzas y Cuerpos de Seguridad** en caso de reiteración, gravedad o ilegalidad del comportamiento.

Copyright 2026




IS4K de INCIBE. Ciberacoso escolar.

> INCIBE es el Instituto Nacional de Ciberseguridad y tiene una web específica para el uso seguro en menores (IS4K). En ella se puede obtener más información sobre ciberacoso escolar en el siguiente enlace.

## Sexting

Etimológicamente proviene de los anglicismos SEX (sexo) y TEXTING (mensajería de texto) y hace referencia a la producción y difusión de contenido sexual mediante aplicaciones de mensajería digital.

Estudios nacionales afirma que el 31% de los menores de entre 11 y 16 años ha recibido ha recibido mensajes sexuales de algún tipo principalmente por servicios de mensajería instantánea, habiendo aumentado exponencialmente frente al 10% del año 2010.
Entre sus características encontramos:

Copyright 2026

- Uso de medios digitales para la producción.
- Contenido erótico/sexual
- Protagonistas identificables en el contenido difundido.
- Naturaleza privada en su origen.

Pero pese a ser contenidos privados, pueden ser difundidos debido a:
- Pérdida del dispositivo
- Fallo de seguridad
- Haber sido enviado a un destinatario erróneo
- O difusión posterior por parte del receptor del mensaje sin estar autorizado.

Esto puede acarrear consecuencias como:
- **Sextorsión**: Utilización de material privado de contenido sexual para chantajear.
- **Ciberbulling o Ciberacoso**
- **Grooming**: Forma de acoso en la que un adulto contacta con un menor con el fín de ganarse su confianza para posteriormente involucrarle en una actividad sexual.
- **Pornovenganza**: difusión de contenido íntimo en redes sociales o servicios de mensajería sin consentimiento del protagonista.

Todas estas actuaciones conllevarán a la exigencia de
-**Responsabilidad en materia de protección de datos** por difusión de datos sensibles sin consentimiento.
-**Responsabilidad civil**: por daños y perjuicios materiales y morales, con su consecuente sanción administrativa e indemnización
**-Responsabilidad penal**: la grabación y difusión de imágenes o vídeos sin consentimiento podrá ser constitutiva de delito, sancionable con penas de hasta 5 años de prisión. Y de **uno a tres meses para quienes difundan, revelen o cedan a terceros sin consentimiento de la víctima**.

https://www.youtube.com/embed/s_O1FlEc1xk

Youtube. No puedes compartirlas sin su consentimiento #RevengePorn. Pantallas Amigas

> Para saber más, échale un ojo al libro de "*Convivencia segura en la red, ciberayudantes*"

Revision #4
Created 2023-02-28 22:00:08 CET by Javier Anzano
Updated 2023-04-17 10:09:40 CEST by Javier Anzano

Copyright 2026