

2.2. Amenazas externas

El Phishing

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.

Para saber más, te proponemos ver el siguiente vídeo 

<https://www.youtube.com/embed/uhzV5-iFb5E>

Youtube. ¿Qué es el phishing? INCIBE

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.
- **Si el mensaje te obliga a tomar una decisión de manera inminente o en unas pocas horas, es mala señal**. 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**.

En nuestro trabajo, tendremos que tener **mucho cuidado al revisar nuestras bandejas de entrada del correo corporativo**, por lo que te recomendamos leer la siguiente infografía para poder detectar los correos electrónicos maliciosos:

Cómo identificar un correo electrónico malicioso

Cientos de emails fraudulentos llegan a nuestras bandejas de correo y, aunque muchos son eliminados, otros consiguen su objetivo, ser leídos. **Depende de nosotros saber cómo identificar un correo electrónico malicioso:**

- 1 REMITENTE**
¿Esperabas un email de esta persona/entidad?
Comprueba que el email coincida con la persona o entidad remitente que dice ser o si está suplantando a alguien.
- 2 ASUNTO**
¿Capta tu atención el asunto del correo?
La mayoría de correos fraudulentos utilizan asuntos llamativos e impactantes para captar tu atención. Ten en cuenta esta consideración.
- 3 OBJETIVO DEL MENSAJE**
¿Cuál es el objetivo del correo?
Una entidad de servicios como el banco, suministros del hogar (agua, gas) u otros nunca te pedirá tus datos personales por correo. Además, si es de carácter urgente, amenazante o con ofertas y promociones muy atractivas, es muy posible que sea un fraude.
- 4 REDACCIÓN**
¿Tiene errores ortográficos o parece una mala traducción de otro idioma?
Revisa la redacción en busca de errores de ortografía o gramaticales. Además, si no está personalizado o parece una traducción automática, sospecha.
- 5 ENLACES**
¿Los enlaces llevan a una página legítima?
Sitúa el cursor encima del enlace, o mantén presionado el enlace en dispositivos móviles, podrás ver la URL real a la que redirige. Si no coincide o es una web sin certificado de seguridad (https://), no hagas clic.
- 6 ADJUNTOS**
¿Contiene un archivo adjunto que no estabas esperando o es sospechoso?
Analiza los adjuntos antes de abrirllos, puede tratarse de un malware. Los antivirus y analizadores de ficheros te ayudarán a identificar si están infectados.

Finalmente, **no olvides utilizar el sentido común y aplicar todos los contenidos que se encuentran en la OSI** para convertirte en un usuario ciberseguro.

¡Sigue estas pautas y disfruta de un correo electrónico libre de riesgos!

GOBIERNO DE ESPAÑA
VICERREINADO
TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe
INSTITUTO NACIONAL DE CIBERSEGURIDAD
@INCIBE INCIBE @INCIBE

Mantente al día con nuestras campañas de concienciación para estar informado.
¡Es nuestra mejor defensa!
www.incibe.es | www.osi.es

OSI
Oficina de Seguridad del Internauta
@osiseguridad osiseguridad

Infografía. *Cómo identificar un correo electrónico malicioso.* **INCIBE.**

El 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.



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.

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

Sexting

https://www.youtube.com/embed/s_O1FIEc1xk

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

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:

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

Entre sus **características** encontramos:

- 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
- 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)
- **Ciberbullying o Ciberacoso**
- **Grooming** (forma de acoso en la que un adulto contacta con un menor con el fin 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)

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



Revision #12

Created 18 April 2023 13:28:29 by Meritxell Pradel

Updated 6 October 2023 14:12:29 by Silvia Coscolin Sanchez