Unidad de Contenido

[Protección de datos personales en redes sociales]

Proyecto: B-SAFE
Número: 2018-1CZ01-KA204-048148
Nombre del autor: EDIT VALUE®
Última fecha de procesamiento: 02.09.2020

Funded by the
Erasmus+ Programme
of the European Union

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."

Co-funded by the
Erasmus+ Programme
of the European Union

Protección de datos personales en redes sociales

Introducción

En 2010, el famoso programa de comedia Saturday Night Live hizo una representación sobre las redes sociales. En él, un actor que se hace pasar por Julian Assange (fundador de la plataforma WikiLeaks) declaró, de manera alegre y sarcástica, "Te doy información privada sobre corporaciones de forma gratuita, y soy un villano. [El creador de Facebook, Mark] Zuckerberg da su información a las corporaciones, por dinero, y es el Hombre del Año [de la revista Time] ". ¿Ves una conexión de esta representación cómica y la realidad? ¿Cómo te sientes al proporcionar tus datos a una empresa de forma gratuita, mientras esto le permite ganar dinero? ¿Están seguros nuestros datos mientras utilizamos las redes sociales?

Obviamente, en estos días, la protección de datos personales en las redes sociales es un tema muy importante. El uso de las redes sociales está creciendo exponencialmente y ahora es una parte esencial de la vida cotidiana de la mayoría de las personas en todo el mundo. Desde nuestro compañero de trabajo hasta nuestra dulce abuela, casi todos usan las redes sociales para compartir fotografías, videos y conversaciones con amigos o familiares, publicar información personal en general y crear una sensación de cercanía.

Sin embargo, como el uso de las redes sociales está tan arraigado en nuestros hábitos como individuos y en la sociedad, la mayoría de las personas bajan la guardia cuando se trata de ciberseguridad, lo que puede tener serias consecuencias a largo plazo.

¿Quién más verá estos datos?

Por lo tanto, hay mucho que aprender sobre la protección de datos e información personal al usar las redes sociales, como verás en esta unidad de contenido.

Relevancia práctica: esto es para lo que necesitarás el conocimiento y las habilidades

Después de trabajar a través de esta unidad de contenido, podrás identificar los riesgos de privacidad más relevantes asociados con el uso de las redes sociales y sabrás cómo protegerte en consecuencia.

1. Construye conocimiento - Protección de datos personales en las redes sociales

Definición

Co-funded by the Erasmus+ Programme of the European Union

Las **redes sociales** son tecnologías interactivas mediadas por ordenador que facilitan la creación o el intercambio de información, ideas, intereses profesionales y otras formas de expresión mediante la creación de comunidades y redes virtuales. El propósito de las redes sociales es conectar y compartir información con cualquier persona en la Tierra o con muchas personas simultáneamente. Puede ser utilizado como una forma de interactuar con amigos y familiares o como una herramienta de marketing por parte de las empresas. Las redes sociales son cualquier herramienta digital que permite a los usuarios crear y compartir contenido rápidamente con otras personas.

En el cuadro anterior se presenta una definición amplia de las redes sociales. La realidad es que, como hay 3.500 millones de usuarios activos de redes sociales en todo el mundo, las redes sociales evolucionaron de una manera que, actualmente, se divide en diferentes categorías, en términos de intereses e intenciones del usuario. A continuación, se presenta una lista de 10 tipos de redes sociales, según su objetivo:

	Propósito	Ejemplo
Social Networks	Para conectarse con personas (y marcas) en línea	Facebook; Twitter; LinkedIN
Redes de intercambio de medios	Para buscar y compartir fotos, videos, videos en vivo y otros medios en línea	Instragram; Youtube; Tik Tok
Foros de debate	Para buscar, debatir y compartir noticias, información y opiniones	Reddit; Quora
Red de curación de contenido	Para descubrir, guardar, compartir y debatir contenido y nuevas tendencias	Pinterest; Flipboard
Red de opinión del consumidor	*Para buscar, revisar y compartir información sobre marcas, productos y servicios, así como restaurantes, destinos de viaje, etc.*	Yelp; Zomato, Tripadvisor
Red de blogs y publicaciones	Para publicar, descubrir y comentar contenido en línea	Wordpress; Tumblr
Red social de compras	Para detectar tendencias, seguir marcas, compartir grandes hallazgos y realizar compras	Etsy
Red basada en intereses	Para conectarse con otros en torno a un interés o pasatiempo compartido	Goodreads; Last.Fm
Red de "economía compartida"	Para anunciar, encontrar, compartir, comprar, vender e intercambiar productos y servicios entre pares	Airbnb; Uber; Glovo

Co-funded by the
Erasmus+ Programme
of the European Union

Red social anónima	Para cotillear, desahogarse y husmear	Whisper; Ask.fm

No hay duda de que estamos viviendo en la era de las redes sociales. Por ello, existen múltiples problemas legales en las redes sociales que surgen cuando las personas comparten contenido en línea a través de diferentes plataformas como Instagram, Pinterest, Facebook, etc. Los derechos más importantes de las redes sociales están relacionados con quién posee el contenido que se comparte, cuándo y dónde es apropiado compartir y qué límites pueden imponerse. A menudo generan problemas relacionados con la infracción de marcas comerciales, la infracción de derechos de autor, el marketing en redes sociales, las relaciones laborales y más. Encontrarás una breve lista sobre los derechos de redes sociales más importantes para Instagram, Whastapp, Youtube y Facebook.

1. Oficialmente, eres dueño de cualquier foto y/o video que publiques, pero otras personas pueden pagar para usarlos e Instagram no te pagará por ello
2. Eres responsable de todo lo que hagas con Instagram y de todo lo que publiques
3. Aunque eres responsable de la información que publicas en estas redes sociales, Instagram puede guardar, usar y compartir información personal con compañías conectadas a Instagram
4. Puedes cerrar tu cuenta de Instagram. Si lo haces, tus fotos, publicaciones y perfil desaparecerán de tu cuenta, pero si alguien ha compartido tus fotos o detalles personales, o si alguien usa este tipo de información por algún motivo, aún podrían aparecer en esta red social.

1. Puedes cambiar tu nombre de perfil, imagen y mensaje de estado cuando lo desees
2. Cualquier persona que use WhatsApp puede ver tu número de teléfono móvil, nombre de perfil, foto, estado, mensaje de estado, estado visto por última vez y recibos. Puedes cambiar esto si lo deseas y también puedes usar tu configuración para bloquear personas y controlar con quién chateas
3. Una vez que se entregan tus mensajes, los eliminamos de nuestro sistema y solo se almacenan en tu propio teléfono o dispositivo. Tus mensajes están "encriptados", lo que significa que la empresa propietaria de WhatsApp no puede leerlos
4. No se permite a otras compañías colocar anuncios en tu pantalla de WhatsApp a menos que estés conectado con ellos.

1. Cuando creas una cuenta de YouTube, Google recopila tus datos. Puedes decidir si Youtube debe recopilar parte de esta información yendo a los "controles de actividad" de tu cuenta de Google. Además, tu información personal permanece dentro de las empresas de Google sin tu consentimiento.
2. Puedes pedirle a Youtube la información que tiene sobre ti y puedes pedirle a la compañía que la corrija o elimine
3. Si deseas presentar una queja sobre tu aparición en un video de Youtube, puedes darle a Youtube la URL del video, indicar la hora exacta en la que aparece tu información o tú y explicar por qué destacas sobre otras personas en el video

4. Si alguien se queja de un video que tienes en tu canal y Youtube está de acuerdo con él, se te notificará que debes quitar el video o editar los datos personales.

1. Incluso si tu perfil es privado, recuerda que las personas pueden ver y compartir información que otros publican sobre ti. Otras personas también pueden guardar la información que has publicado sobre ti en sus propios teléfonos y dispositivos.
2. Algunas compañías compartirán información sobre ti con Facebook y Facebook compartirá información con ellas.
3. Si aceptas usar una aplicación en Facebook, esa aplicación podría usar, compartir y mantener la información que publica en Facebook
4. Si eliminas tu cuenta, las cosas que has publicado se eliminarán, pero no las cosas que otras personas han compartido sobre ti.

1. Aplica conocimiento

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Protección de datos personales en redes sociales_01_01

Situación: ¿Qué son las "redes sociales"?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Sitios web y aplicaciones que permiten a las personas enviar mensajes y fotos.
- Las redes sociales son una forma de comunicación electrónica (como sitios web para redes sociales).
- Sitio web y programas informáticos que permiten a las personas comunicarse y compartir información en Internet utilizando una computadora o un teléfono móvil.
- Las redes sociales se refieren al sitio web y las aplicaciones que están diseñadas para compartir contenido rápidamente.

Ejercicio ELECCIÓN ÚNICA

Objetivo específico asociado: OE_Protección de datos personales en redes sociales_01_02

Situación: ¿Qué derechos de protección de datos personales se aplican en WhatsApp?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es falsa.

- Tienes derecho a tener mensajes cifrados, lo que significa que WhatsApp no puede leer los mensajes que envías a otras personas.
- Tienes derecho a eliminar tu cuenta de WhatsApp y con eso no se enviarán los mensajes que se han enviado a otras personas.
- Si solo eliminas la aplicación WhatsApp en tu dispositivo pero no eliminas la cuenta, la información se mantendrá.
- WhatsApp guarda y mantiene información sobre ti, pero no puede usar tu información en ningún lugar del mundo.

Co-funded by the
Erasmus+ Programme
of the European Union

1. Construye conocimiento - Los riesgos más comunes en las redes sociales

Hoy en día, es de conocimiento común que las redes sociales integran nuestros intereses y actividades diarias. Sin embargo, ¿compartimos los hábitos y comportamientos con respecto al uso de las redes sociales? Para comprender la relevancia de las redes sociales en nuestra sociedad, es importante que nos mantengamos al tanto de las últimas estadísticas de redes sociales. A continuación, presentamos las 10 estadísticas más relevantes para las redes sociales:

10 ESTADÍSTICAS MÁS RELEVANTES PARA MEDIOS SOCIALES

e los especialistas en marketing creen que el marketing en redes sociales ha sido muy efectivo para su negocio (Buffer, 2019)

illones de usuarios activos de redes sociales en todo el mundo, equivalente al 45% de la población (Emarsysm, 2019) arsys, 2019)

arios de historias activas diarias de Instagram aumentaron de 150 millones en enero de 2017 a 500 millones de historias activas diarias en todo el mundo en enero de 2019 (Buffer, 2019)

Facebook sigue siendo la plataforma de redes sociales más común (Pewinternet, 2018)

e todos los usuarios de redes sociales acceden a los canales sociales a través de dispositivos móviles (Buffer, 2019)

% de los consumidores quieren que las marcas impulsen las plataformas sociales para proteger mejor sus datos personales (Edelman, 2008)

todos los usuarios de redes sociales acceden a canales sociales a través de dispositivos móviles (Buffer, 2019)

sumidores digitales pasan casi 3 horas al día en redes sociales y aplicaciones de mensajería (Globalwebindex, 2018)

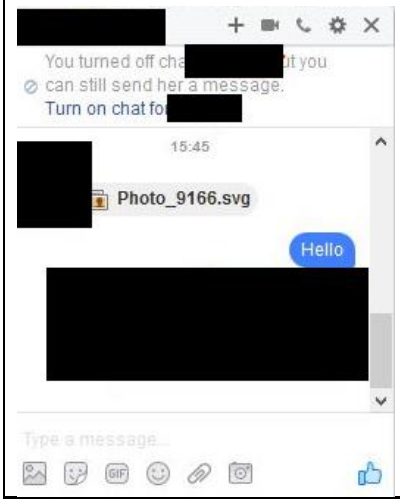
% de las pequeñas y medianas empresas utilizan actualmente las redes sociales para impulsar el crecimiento empresarial y el 9% tiene previsto utilizarlas en el futuro (LinkedIN, 2014)

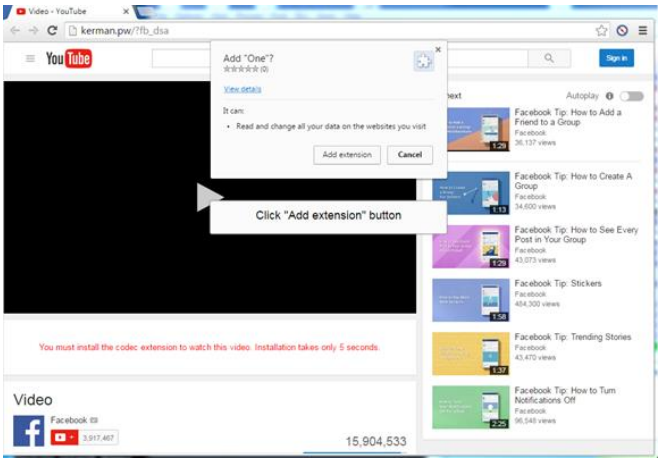
En promedio, las personas tienen 7.6 cuentas de redes sociales (Clement, 2019)

Con este tipo de estadísticas, no es de extrañar que las redes sociales se estén convirtiendo en las plataformas más famosas para recopilar datos de los usuarios, ya sea perpetuada por la propia red de manera legal o por piratas informáticos con intenciones maliciosas.
El riesgo más preeminente de las redes sociales es el malware que puede comprometer todos tus datos. Existen diferentes tipos de malware con diferentes propósitos, como puedes ver a continuación:

1. **Ransomware- software que utiliza cifrado para deshabilitar el acceso de un objetivo a sus datos, como fotografías o documentos, hasta que se pague un rescate. Este malware se activa cuando el usuario hace clic en un hipervínculo publicado en una plataforma de redes sociales o en una imagen que lo redirige a un sitio web externo que difunde el código malicioso.**

Ejemplo de Ramsomware
Las aplicaciones de chat como WhatsApp o Facebook Messenger son medios comunes para los ataques de ransomware. En este ejemplo, los cibercriminales enviaron mensajes engañosos con archivos adjuntos de imágenes SVG a través de Facebook Messenger. Los usuarios que hicieron clic en la imagen se encontraron a sí mismos en un sitio web con una ventana emergente para instalar una extensión de navegador o complemento para ver un video. Más tarde, después de que el código malicioso infectara el sistema de los usuarios, apareció otra ventana emergente que exigía el pago para desbloquear los archivos del usuario.





2. Troyano - Tipo de código o software malicioso que parece legítimo pero que puede tomar el control de tu ordenador. Un troyano está diseñado para robar datos (inicios de sesión, datos financieros, incluso dinero electrónico), instalar más malware, modificar archivos, monitorear la actividad del usuario (observación de pantalla, registro de teclas, etc.), usar el orenador en botnets y anonimizar la actividad de Internet del atacante . Un troyano actúa como una aplicación o archivo legítimo para engañarte y que descargues e instales malware. Una vez instalado, puede desempeñar la acción para la que fue diseñado.
Por lo general, un caballo de Troya está oculto en publicidad falsa o se envía a los usuarios por mensajería instantánea.

3. Virus - Form of malware that is capable of copying itself and spreading to other computers. Viruses often spread to other computers by attaching themselves to various programs and executing code when a user launches one of those infected programs. Viruses can also spread through script files, documents, and cross-site scripting vulnerabilities in web apps. Viruses can be used to steal information, harm host computers and networks, create botnets, steal money, render advertisements, and more.

4. Greyware –forma de malware que realmente no hace ningún daño físico a tus datos como lo hace otro malware, y se presenta en un asunto más molesto, como el adware y el spyware. Tiene una alta prevalencia en las redes sociales, generalmente en forma de "cebo de clic", donde un artículo atractivo te llevará a un sitio web que te pide que realices una acción, como instalar un complemento falso de redes sociales o completar un mensaje rápido o encuesta antes de acceder a los medios. Esa información se recopila y se vende a otros ciberdelincuentes y se puede usar para intentar hackear tus cuentas personales.

Ejemplo de Greyware
A lo largo de los años, los estafadores han utilizado muertes de celebridades reales y falsas para convencer a los usuarios de que hagan clic en los enlaces y realicen acciones. Un ejemplo infame siguió a la muerte del actor Robin Williams, en 2014. Solo 48 horas después de su muerte, comenzó a circular un video en Facebook que decía vincular a un supuesto video de despedida de Williams. Los usuarios que hicieron clic en el enlace al supuesto video fueron llevados a un sitio web falso de BBC News. Luego, se les indicó que compartieran el video en Facebook antes de verlo. Después de compartir la página según lo solicitado, apareció una segunda página falsa y solicitó que se completara una encuesta en línea. Se recopiló información personal y luego se vendió a compradores de Internet sin escrúpulos.

5. Gusanos – Los gusanos se encuentran entre los tipos más comunes de malware. Los gusanos pueden modificar y eliminar archivos, robar datos, instalar una puerta trasera y permitir que un hacker obtenga el control de un ordenador y la configuración de su sistema. Incluso pueden inyectar software malicioso adicional en el ordenador. Los gusanos se pueden transmitir a través de vulnerabilidades de software o pueden llegar como archivos adjuntos en correos electrónicos no deseados o mensajes instantáneos. Una vez abiertos, estos archivos podrían proporcionar un enlace a un sitio web malicioso o descargar automáticamente el gusano informático. Una vez que está instalado, el gusano silenciosamente se pone a trabajar e infecta la máquina sin el conocimiento del usuario. Los gusanos a menudo se propagan enviando mensajes instantáneos masivos con archivos adjuntos infectados a los contactos de los usuarios.

Como puedes observar, todo este malware utiliza la misma estrategia para atraer al usuario, es decir, estafas o ataques de phishing. Los ataques de phishing utilizan fuentes maliciosas para recopilar información personal y financiera o infectar la máquina del usuario con malware.

El primer paso de un archivo adjunto de phishing es siempre el mismo: en tus redes sociales o en tu aplicación de mensajes instantáneos aparece un enlace, foto, video, un artículo o un anuncio. Esto podría parecer de cualquiera: una fuente de noticias, una celebridad, un negocio, la red social o incluso un contacto de confianza. La mayoría de las veces esas fuentes son suplantadoras de cuentas reales o usuarios cuya cuenta de redes sociales ha sido comprometida o su identidad ha sido robada.

Ejemplo de una cuenta de imitador
Twitter tiene una herramienta que verifica las cuentas para reducir la actividad fraudulenta, llamada "Twitter Verified". Esta es la verdadera cuenta para ello:

No pasó mucho tiempo hasta que apareció una cuenta clonada, afirmando ser la cuenta de ayuda de verificación auténtica y dirigiendo a los usuarios a todo tipo de cargas maliciosas.

El phishing de las redes sociales juega con las emociones y necesidades humanas básicas, como la confianza, la seguridad, el duelo, el miedo a perder dinero, obtener algo por nada, el afán de encontrar una ganga o el deseo de encontrar amor o popularidad/estatus. En general, también indican o implican la necesidad de una acción urgente para evitar un problema o aprovechar una oferta.

Ejemplos de Estafas de phishing
¡DIOS MIO! ¿Viste esta foto tuya? ¡Detalles secretos sobre la muerte de Michael Jackson! ¡Solo el 1% de las personas puede resolver este problema! ¡Responde el cuestionario ahora! Adidas regala 3.000 pares de zapatos gratis para celebrar su 93 aniversario. ¡Consigue tus zapatos gratis ahora! Estas son estafas de phishing muy comunes que involucran una pregunta, una celebridad, una marca o un hecho que despierta el interés del usuario y luego le dirige a una pantalla de inicio de sesión falsa para obtener información de inicio de sesión o instalar automáticamente malware en un ordenador.

El segundo paso de un ataque de phishing es redirigir al usuario a un sitio web que solicita detalles confidenciales o causa la infección del ordenador o dispositivo móvil con malware. Este malware se puede instalar automáticamente o después de solicitar la descarga de un programa, extensión de navegador o aplicación.

Alternativamente, la publicación, el tweet o el mensaje pueden indicarte que realices una llamada telefónica a un número específico. Esto puede provocar que se soliciten detalles confidenciales o que se agreguen cargos exorbitantes a tu factura telefónica.

2. Aplico conocimiento

Ejercicio ELECCIÓN ÚNICA

Objetivo específico asociado: OE_Protección de datos personales en redes sociales_02_01

Situación: ¿Qué hecho es falso?
Tarea: Elige la opción correcta siguiendo el principio de opción múltiple: solo una opción es correcta.

- Las redes sociales son una herramienta de marketing efectiva para las empresas.
- Facebook es la plataforma de redes sociales más utilizada
- La mayoría de los usuarios de redes sociales acceden a canales sociales a través de dispositivos móviles
- Las pequeñas y medianas empresas utilizan actualmente las redes sociales para impulsar el crecimiento empresarial
- Los usuarios tienden a elegir una red social, usándola todos los días

Ejercicio ELECCIÓN ÚNICA

Objetivo específico asociado: OE_Protección de datos personales en redes sociales_02_02

Situación: te estás desplazando por Facebook y ves la siguiente publicación:

¿Qué harías?

Tarea: Elige la opción correcta siguiendo el principio de opción múltiple: solo una opción es verdadera.

- Dios mío, ¡hoy es mi día de suerte! Hago clic en "CONTINUAR" y les doy todos los datos necesarios para ganar la tarjeta de regalo. ¡Después de eso, comparto la oportunidad con todos mis amigos cibernéticos!
- ¡Solo tengo 4 minutos para reclamar mi premio! Hago clic en "CONTINUAR" y les doy todos los datos necesarios para ganar el premio. Pero después de ver que debo dar detalles bancarios, me rindo. Demasiado trabajo.
- Tengo curiosidad y hago clic en "CONTINUAR". Después de ver que es necesario darles datos personales, cierro la pestaña. Creo que es una estafa.
- No hago clic en la publicación. ¡No puedo ganar una lotería que nunca jugué! Señalo la publicación en Facebook como "estafa".

Co-funded by the
Erasmus+ Programme
of the European Union

2. Construye conocimiento - Algunos consejos de seguridad utilizando cuentas de redes sociales

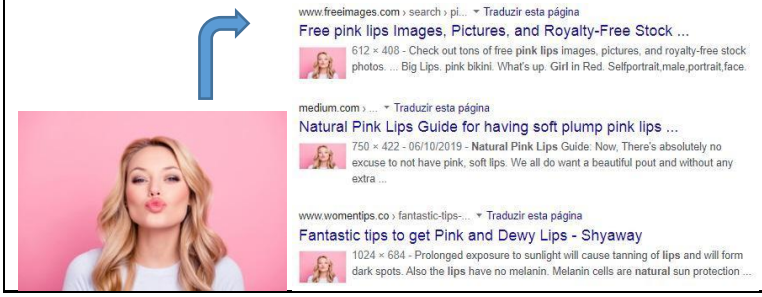
Ahora que conoces la amplia variedad de riesgos del uso de las redes sociales, ¡no sientas que la única solución para garantizar tu seguridad y privacidad es eliminar tus redes sociales! El secreto es utilizarlas mientras se entienden los riesgos y se sabe cómo actuar en consecuencia.
Hay algunos comportamientos comunes de estafadores y piratas informáticos que pueden alertarnos sobre la posibilidad de una estafa de phishing. Mientras navegas por tu red social favorita, ten siempre en cuenta estas señales de alerta que indican que esa publicación es una estafa de phishing:

Bandera roja # 1: Solicitudes de amistad de extraños

¿Recibiste una solicitud de amistad de un extraño? ¿Alguien que no reconoces te envió un mensaje privado? ¿Una empresa o una figura pública te pidió que comenzaras a seguirles?
Plataformas como Facebook, Instagram y Twitter están llenas de perfiles falsos con la intención engañar a los usuarios. No aceptes ninguna solicitud de amistad sin verificación. Si alguien te molesta, es bueno informar y bloquear dichos perfiles.

Consejo rápido

Haz una búsqueda de imagen inversa de la fotografía de perfil. La mayoría de las veces, los hackers usan fotos de archivo. Si tiene resultados para diferentes sitios web que usan esa foto para diferentes propósitos, es una cuenta falsa.



Consejo rapido

¿Alguna vez te diste cuenta de la marca de verificación azul junto a los nombres de altos perfiles o empresas en las plataformas sociales? Se parece a esto:

Twitter: Stephen King
Facebook: adidas
Instagram: cristiano

Esta marca de verificación está disponible en casi todas las plataformas de redes sociales y significa que la cuenta se verifica como auténtica y pertenece a una celebridad o líder de la industria.
Por ejemplo, si obtienes un MD de la cuenta "Verificado de Twitter" sin la marca de verificación, ten cuidado: ¡es probable que sea falso!

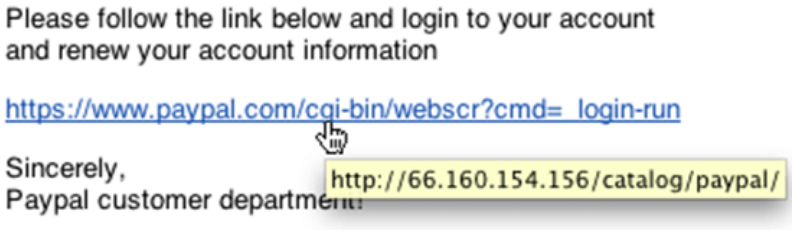
Redflag # 2: ¡Haz clic en este enlace!

El objetivo de un ataque de phishing suele ser que descargues un archivo adjunto (por ejemplo, una foto enviada en un mensaje directo) o hagas clic en un enlace. A veces, los delincuentes se hacen pasar por fuentes confiables para que hagas clic en un enlace (o descargues una aplicación) que contenga malware. Lo que parece un hipervínculo legítimo puede ser un enlace encubierto a un sitio web criminal.

Por lo tanto, no hagas clic en ningún enlace que te redirija a otro sitio web. En su lugar, ve directamente a la fuente (sitio web de la marca, página del banco, etc.) y confirma si ves en las redes sociales que es un verdadero anuncio.

Consejo rápido

Una forma rápida de comprobar si el hipervínculo te redireccionará a una fuente confiable es pasar el ratón sobre el texto del hipervínculo. Debería ver la URL completa, que ayudará a mostrar si conduce a un sitio web legítimo.



¿Cuál es la pista principal que deberíamos buscar en la URL?
Presta atención al comienzo de la URL: las URL seguras comienzan con "https" en lugar de solo "http" para indicar que están encriptadas. La "s" en "https" significa "seguro".
¡Entonces, este hipervínculo es una estafa de phishing!

Consejo rápido

¿Qué pasa si haces clic en un enlace? ¿Qué deberías hacer?
Si ese enlace te redirige a un sitio web, hay algunas señales que puedes buscar para ayudarte a saber si una empresa es real o no.Antes de hacer nada, como ingresar tus credenciales de inicio de sesión o hacer clic en el botón de descarga, busca estas claves:

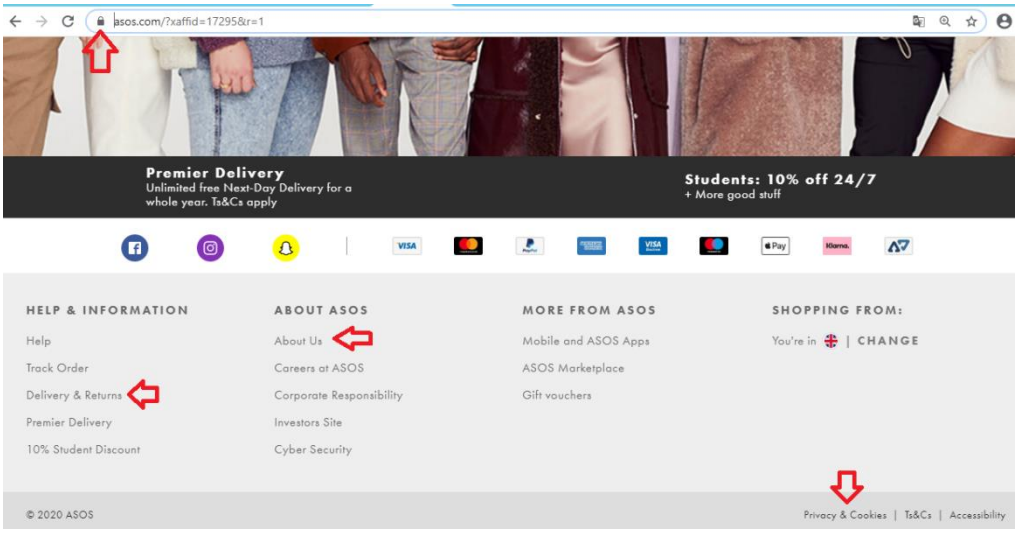
a barra de búsqueda aparece "https" o un símbolo de "candado", eso significa que **el sitio web está egido.**

el dominio - los ciberatacantes son muy astutos. La mayoría de las veces, los dominios son muy similares al, por ejemplo, "as0s.com" o "asos.net".

una dirección física y un número de teléfono - las compañías acreditadas enumerarán su información para puedas comunicarte con ellos si hay un problema.

tica de devolución - los sitios acreditados deben incluir su política de devolución y su política de envío.

aración de privacidad - los sitios acreditados deben informar sobre cómo protegen tu información y si itan tu información a terceros.



Co-funded by the
Erasmus+ Programme
of the European Union

Redflag #3: ¡Promociones y concursos demasiado buenos para ser verdad!

Esta es una estafa de phishing muy común. Al presentar precios muy bajos, ofrecer premios irresistibles o regalar descuentos, los estafadores pueden engañar a los usuarios para que brinden información privada.

Consejo rápido
¿Cuáles son los signos comunes de una estafa de concurso? - La página social tiene un número bajo de seguidores; - Gramática y ortografía pobres; - Piden información muy personal, como el nombre de tu madre, la primera mascota, si tienes hijos, etc. ¡Todo lo que quieren son pistas para descifrar tu contraseña! - ¡Son muy persistentes en su diálogo! Solo quieren que tengas la sensación de "urgencia".

Como puedes concluir, hay formas de detectar estafas de phishing en las redes sociales, evitando convertirte en víctima de un ataque cibernético que comprometa tus datos personales. Pero tener un ojo atento no es suficiente. Con respecto a los ciberataques, el mejor remedio es la prevención. Entonces, ¿qué puedes hacer para estar siempre un paso por delante de los ciberdelincuentes en las redes sociales?

Co-funded by the
Erasmus+ Programme
of the European Union

Verifique su configuración de privacidad
Las redes sociales fiables le permiten establecer la configuración de privacidad al nivel que desees. ¿Qué tipo de información quieres hacer pública? ¿Tus fotos? ¿Tus pasatiempos? ¿Y con quién quieres compartir esa información? ¿Tus amigos de las redes sociales o todos?
La modificación de la configuración de privacidad puede permitirte bloquear a extraños y personas que no son tus amigos para que no vean tu perfil y la información que compartes.
Para hacer esto, debe verificar las "definiciones" de su cuenta.

Mantenga actualizado el software de seguridad
Tener el software de seguridad, el navegador web y el sistema operativo más recientes es la mejor defensa contra virus, malware y otras amenazas en línea.
También puede instalar en su navegador una extensión que bloquee los anuncios no deseados.

Cree contraseñas seguras
La creación de una contraseña segura evitará que los piratas informáticos accedan a su cuenta y la utilicen para publicar spam o ataques maliciosos. Una contraseña segura tiene no menos de 8 caracteres y consta de letras y números. También debe cambiarse cada 3 meses y debe ser exclusiva para cada cuenta.
Truco: use una frase de contraseña en lugar de una contraseña, por ejemplo, "IAte27P0tat0s"

Guarda tus secretos
Evita compartir información personal en línea porque tu información, incluida tu dirección de correo electrónico, número de teléfono y número de seguridad social, valen mucho dinero para los piratas informáticos y las empresas de extracción de datos. Esos datos podrían usarse para pedir rescates, robos de identidad o como una pista para adivinar sus contraseñas.
Eche un vistazo a sus perfiles en las redes sociales y trate de mantenerlos estériles; las personas que necesitan saber su fecha de nacimiento, dirección de correo electrónico y número de teléfono ya los tienen.

Debido a que los datos están encriptados, los piratas informáticos, los gobiernos e incluso los proveedores de servicios de Internet no pueden ver ni obtener el control de su información mientras está conectado a un servidor

Don't forget to log out

Keep in mind this golden rule: always log out of all of your social media platforms when you are done using them. If you don't log-out you're allowing anyone with access to your computer, legally or not, to open the browser or application and have instant access to your accounts on such

2. Aplica conocimiento

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Protección de datos personales en redes sociales_03_01 y OE_Protección de datos personales en redes sociales_03_02

Situation: What are the signs of a possible phishing scam that you must always be alert while browsing social media?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Gramática y ortografía de la publicación.
- La presencia de hipervínculos: solo una fuente creíble puede publicar un enlace a su sitio web.
- El hipervínculo no coincide con la URL.
- Si un amigo me envía una foto para descargar, no hay peligro de hacerlo.
- La cuenta de una marca famosa debe ser verificada para ser confiable.

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Protección de datos personales en redes sociales_03_01 y OE_Protección de datos personales en redes sociales_03_02

Situación: ¿Qué debes hacer para garantizar la utilización de tu plataforma de redes sociales de manera segura?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Es más seguro usar la misma contraseña para todas mis cuentas. De esa manera nunca lo olvidaré.
- Antes de aceptar una nueva solicitud de amistad, debo verificar la autenticidad de su perfil y cuenta.
- Nunca debo revelar los detalles de dónde estoy de vacaciones, de compras o de viaje, así como cuándo se espera que me vaya o regrese a casa.
- Está bien utilizar un ordenador con acceso a Internet sin instalar software anti-malware y antivirus.
- **Para realizar un seguimiento de todas las actividades sociales de mis amigos cibernéticos, debo mantener mi sesión iniciada en todo momento.**

Fuentes

Akilawala, T. (August 16, 2014) *Fake Robin Williams goodbye video on Facebook is a scam.* Retrieved from https://www.bgr.in/news/fake-robin-williams-goodbye-video-on-facebook-is-a-scam-321750/

Crowdstrike (October 15, 2019) *The 11 most common types of malware*. Retrieved from https://www.crowdstrike.com/epp-101/types-of-malware/

Constanza, T. (August 19, 2019) *Scam on Facebook exploits Robin Williams' suicide.* Retrieved from https://www.siliconrepublic.com/enterprise/scam-on-facebook-exploits-robin-williams-suicide

DuPaul, N. (October 12, 2012) *Common Malware Types: Cybersecurity 101.* Retrieved from https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101

Foreman, C. (June 20, 2017) *10 Types of Social Media and How Each Can Benefit Your Business*. Retrieved from https://blog.hootsuite.com/types-of-social-media/

Get Safe Online (n. d.) *Social Media Phishing. https://www.getsafeonline.org/social-networking/social-media-phishing/*

GMA News Online (August 15, 2014) *Beware of Robin Williams goodbye video scam.* Retrieved from https://www.gmanetwork.com/news/hashtag/content/375009/beware-of-robin-williams-goodbye-video-scam/story/

Kietzmann, J. H. and Hermkens, K. (2011) *Social media? Get serious! Understanding the functional building blocks of social media*. Business Horizons (Submitted manuscript). 54 (3): 241–251. doi:10.1016/j.bushor.2011.01.005.

Mohsin, M. (Frebruary 7, 2020) *10 Social Media Statistics You Need to Know in 2020 [Infographic].* Retrieved from https://www.oberlo.com/blog/social-media-marketing-statistics

NortonLifeLock (n. d.) *What is a Trojan? Is it a virus or is it malware?* Retrieved from https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html

NortonLifeLock (n. d.) *What is a computer worm, and how does it work?* Retrieved from https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html

Obar, J. A. and Wildman, S. (2015) *Social media definition and the governance challenge: An introduction to the special issue.* Telecommunications Policy. 39 (9): 745–750. doi:10.1016/j.telpol.2015.07.014. SSRN 2647377

SNL. 2010. Saturday Night Live. Season 36, Episode 10. First aired December 18. NBC. Retrieved from https://www.youtube.com/watch?v=md3of7O02e4&list=PLS_gQd8UBhLghdS1aaLqVJ74rWi4ffT8&index=14

Woodfield, M. (November 26, 2014) *Should I Buy from This Site? How to Know if a Website is Secure.* Retrived from https://www.digicert.com/blog/how-to-know-if-a-website-is-secure/

ZeroFOX Alpha Team (February 15, 2017) *Social Media Impersonators Go Phishing: 3 Emerging Tactics*. https://www.zerofox.com/blog/social-media-impersonators-phishing/

Afianza conocimiento

Vivimos en un mundo de globalización donde Internet nos permite comunicarnos con todos en cualquier parte del mundo. Las plataformas de redes sociales se han convertido en una parte integral de nuestras vidas y son una excelente manera de mantenerse conectados con los demás.
Las redes sociales como Facebook, Instagram o YouTube son populares entre todas las edades y trabajan constantemente para cautivar corrientes y nuevos usuarios.
Sin embargo, a pesar de todas las ventajas que este tipo de plataformas ofrece a los usuarios, existen muchos riesgos de seguridad y privacidad relacionados con su uso constante y descuidado. De hecho, los estafadores aprovechan los hábitos de los usurarios en las redes sociales para atraerles a estafas de phishing y ataques que comprometen sus dispositivos y datos. Por lo tanto, todos deben reconocer su responsabilidad de mantener un entorno en línea seguro, al tiempo que comprenden los riesgos de una presencia en línea. Ser cauteloso, elegir una contraseña segura o instalar un software antivirus son algunas de las muchas medidas que un usuario debe adoptar para controlar su seguridad mientras usa las redes sociales.
A medida que el mundo evoluciona hacia un mercado digital único, es fundamental que todos conozcan las leyes aplicadas a la protección de datos personales, como el GDPR y cómo se aplica a diferentes escenarios digitales.
En conclusión, el gobierno, la sociedad y los usuarios finales deben trabajar juntos para proteger la privacidad y seguridad de los datos personales en las redes sociales.

Las respuestas correctas están marcadas en negrita

Situación: ¿Qué son las "redes sociales"?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- **Sitios web y aplicaciones que permiten a las personas enviar mensajes y fotos.**
- **Las redes sociales son una forma de comunicación electrónica (como sitios web para redes sociales).**
- **Sitio web y programas informáticos que permiten a las personas comunicarse y compartir información en Internet utilizando una computadora o un teléfono móvil.**
- **Las redes sociales se refieren al sitio web y las aplicaciones que están diseñadas para compartir contenido rápidamente.**

Situación: ¿Qué derechos de protección de datos personales se aplican en WhatsApp?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es falsa.

- Tienes derecho a tener mensajes cifrados, lo que significa que WhatsApp no puede leer los mensajes que envías a otras personas.
- Tienes derecho a eliminar tu cuenta de WhatsApp y con eso no se enviarán los mensajes que se han enviado a otras personas.
- Si solo eliminas la aplicación WhatsApp en tu dispositivo pero no eliminas la cuenta, la información se mantendrá.
- WhatsApp guarda y mantiene información sobre ti, pero no puede usar tu información en ningún lugar del mundo.

Situation: What are the signs of a possible phishing scam that you must always be alert while browsing social media?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Gramática y ortografía de la publicación.
- La presencia de hipervínculos: solo una fuente creíble puede publicar un enlace a su sitio web.
- El hipervínculo no coincide con la URL.
- Si un amigo me envía una foto para descargar, no hay peligro de hacerlo.
- La cuenta de una marca famosa debe ser verificada para ser confiable.

Situación: ¿Qué debes hacer para garantizar la utilización de tu plataforma de redes sociales de manera segura?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Es más seguro usar la misma contraseña para todas mis cuentas. De esa manera nunca lo olvidaré.
- Antes de aceptar una nueva solicitud de amistad, debo verificar la autenticidad de su perfil y cuenta.
- Nunca debo revelar los detalles de dónde estoy de vacaciones, de compras o de viaje, así como cuándo se espera que me vaya o regrese a casa.
- Está bien utilizar un ordenador con acceso a Internet sin instalar software anti-malware y antivirus.
- Para realizar un seguimiento de todas las actividades sociales de mis amigos cibernéticos, debo mantener mi sesión iniciada en todo momento.