Guía de seguridad online

Jorge Litvin

Guía de Seguridad Online

Jorge Litvin*

LOS RIESGOS DE LA DIGITALIZACIÓN.

Estamos transitando una nueva revolución digital que fue apresurada por el contexto que vivimos en la actualidad. Si eran pocas las actividades que desarrollábamos en el mundo real, ahora fueron plenamente reemplazadas por el entorno virtual. Desde vernos con la familia, hasta estudiar y trabajar, prácticamente todo pasa a través de una pantalla en el escenario actual. Sabíamos que esto iba a suceder, pero desconocíamos lo intempestivo que iba a ser, lo cual nos privó del tiempo necesario para prepararnos y aprender ¿Qué se supone que debíamos aprender? A cómo cuidarnos en Internet.
Así como cuando transitamos por la calle tomamos determinados recaudos para que nada malo nos pase, lo mismo debe hacerse extensivo en los espacios digitales, donde somos aun más vulnerables. Suplantaciones de identidad, estafas por ingeniería social, ataques de ransomware, interceptación de correos y acceso ilegítimo a información privada o confidencial son sólo algunos de los muchos peligros a los que nos enfrentamos en este entorno virtual.

¿Cómo los podemos enfrentar? Evitando tener un problema que solucionar, esto se logra mediante lo que llamaremos "higiene digital", que no son otra cosa que una serie de hábitos que debemos tomar para prevenir ser víctimas de un cibercriminal.

PAUTAS BÁSICAS DE CIBERSEGURIDAD

En este acápite, mediante una serie de preguntas, lo invitamos a auto evaluar su nivel de ciberseguridad, a cada interrogante se le agrega una acción cuya implementación se recomienda para mitigar riesgos en su ámbito personal y laboral.

CONTRASEÑAS

Antes de empezar, piense a los password como llaves, su función es trabar puertas digitales, de modo que sólo puedan ser abiertas por el genuino propietario de esa clave.

A) *¿UTILIZA LA MISMA CONTRASEÑA PARA ACCEDER A VARIAS DE SUS CUENTAS ?*

Si la respuesta es afirmativa se recomienda renovar sus claves, asegurándose de que cada cuenta tenga una propia. Así como las puertas de su hogar, de su auto y de su oficina se abren con llaves distintas, a cada "puerta digital" esta lógica también aplica.

B) *¿RECUERDA CUÁNDO FUE LA ULTIMA VEZ QUE MODIFICÓ UNA CONTRASEÑA?*

*Abogado especialista en cibercrimen y evidencia digital. Se desempeña como Director de Legales en Resguarda y, en paralelo, es consultor integrante del Laboratorio de Ciberseguridad de la OEA (Organización Estados Americanos). Es conferencista y docente en materias vinculadas al cibercrimen, ciberseguridad, protección de datos personales e inteligencia artificial".

[1]Ejemplos de "cuentas" digitales son cada perfil en redes sociales (Facebook, Instagram, LinkedIn, Twitter, etc.), también correos electrónicos (Gmail, Microsoft, etc.),

Si la respuesta es afirmativa se recomienda renovarla. ¿Por qué? Porque a diferencia de una llave material, como la que utiliza para abrir su hogar, si la pierde o se la roban no necesariamente se va a enterar. Es habitual que se filtren nuestras contraseñas en Internet, ya sea por un breach o leak de datos de las plataformas que habitualmente utilizamos. Es aconsejable programar renovaciones semestrales de claves.

C) ¿SU CONTRASEÑA ES FÁCIL DE RECORDAR?

Si la respuesta es afirmativa es probable que también sea fácil de "adivinar" (no solo por humanos, hay programas que prueban combinaciones comunes a gran velocidad).
Recomendamos **passwords alfanuméricos alternados con caracteres especiales, mayúsculas y minúsculas** (Por ej; 7h$D-@r23t) no utilizar números o letras consecutivas ("12345678" o "abcdefgh"), fechas de cumpleaños, domicilio, fragmentos de su nombre o de allegados, la patente del auto, entre otra información con la que podamos ser vinculados.
Para facilitar la higiene digital de sus claves recomendamos utilizar **"gestores de contraseñas".** Son programas que crean, almacenan y completan passwords por el usuario. Algunos ejemplos son Dashlane, Keeper, Lastpass y 1Password; también hay plataformas que lo incorporan como un extra (Dropbox, Google, iOS/MacOS, varios software de antivirus, etc.).

D) ¿DEJA SUS CONTRASEÑAS A LA VISTA O LAS COMPARTE CON FAMILIARES EN MENSAJES?

Evite compartir sus claves por medios que se puedan interceptar, tampoco las deje anotadas en su escritorio o pegadas en la pantalla de la computadora.

¿TENES UN PROGRAMA ANTIVIRUS?

Recomendamos descargar uno. No sólo para su computadora, también para teléfonos celulares y tabletas. Las marcas principales ofrecen alternativas para proteger varios dispositivos con la misma licencia. Siempre descárguelos del sitio oficial. Evite buscar el software, generadores de licencias y crackers en redes P2P o foros de Internet, en muchos casos traen escondidos aquello de lo que se quiere proteger. Algunos ejemplos de marcas confiables son ESET, McAffee, Norton, AVG, Kaspersky, BitDefender, Panda.

¿TIENE UNA COPIA DE SEGURIDAD DE SUS ARCHIVOS?

Con los secuestros de datos y sistemas en auge, a través de ataques de ransomware, recomendamos programar un "back-up" semanal para resguardar los archivos y datos más importantes (por ejemplo: todos los martes). Puede ser en un disco rígido externo o en la nube (Dropbox, Google Drive, Microsoft One Drive, etc.).

¿CUENTA CON LA ÚLTIMA VERSIÓN DEL SOFTWARE DISPONIBLE?

Es importante verificar si tenemos la versión más actual del software antes de empezar a utilizarlo ¿Por qué? Porque no todas las fallas de seguridad pueden contemplarse al momento del lanzamiento de un aplicativo, por eso las plataformas van generando "parches" en la medida que van advirtiendo que la versión original deja un margen expuesto a peligro. Configure actualizaciones automáticas para sistemas operativos (Windows, MacOs/iOS, Android y Linux) y también para aplicaciones que utiliza de forma cotidiana (mensajería, videoconferencia, streaming, paquete Office, etc.).

¿CONFIGURÓ LA AUTENTICACIÓN MULTIFACTORIAL?

El MFA[2] (o 2FA, dependiendo de la cantidad de factores de seguridad) es un proceso de seguridad que agrega una barrera extra para verificar que quien pasee una clave es el legítimo titular de un dispositivo o cuenta, evitando que un extraño acceda.
El primer factor de autenticación es la contraseña que asigna cada usuario, mientras que el segundo factor puede ser:

- Algo que solo el usuario sabe. Como un código pin;
- Algo que solo el usuario tiene. Por ejemplo, su Smartphone (al que llega un mensaje o cuenta con una app de autenticación) o un pendrive que actúa de llave física;
- Algo inherente al usuario. Por ejemplo un dato biométrico (reconocimiento facial, de voz o dactilar).
- Servicios que admiten MFA:
- Redes sociales (Facebook, Instagram, Twitter, Tumblr, LinkedIn, TikTok, Snapchat).
- Cuentas de Microsoft, Google, iCloud, Yahoo, Dropbox, Evernote, GoDaddy, Slack.
- Cuentas bancarias (mediante Token).
- Plataformas de Gaming (Playstation, Nintendo, Xbox, Steam).
- Plataformas de comercio electrónico y billeteras digitales (Amazon, Mercado Libre, Mercado Pago, Paypal, Ualá).
- Aplicaciones de mensajería (Whatsapp, Telegram, Signal).
- Etc. (siempre revise en la configuración de seguridad de toda app o plataforma si se puede configurar).

Se recomienda preferir autenticación biométrica cuando este disponible. Las aplicaciones de autenticación son preferibles por sobre el método de recibir un código vía mensaje de texto o llamado a un número celular. Alternativas que puede descargar: Microsoft Authenticator, Google Authenticator, Lastpass, Authy o Duo, entre otros.

¿TIENE CUBIERTA SU CÁMARA WEB?

Es muy usual que los criminales intenten husmear para obtener información, imágenes o videos para cometer escraches o extorsionar.
Si la cámara de su pc se encuentra incorporada, manténgala cubierta hasta que la tenga que utilizar. Si utiliza una cámara externa desconéctela.

¿SABE QUÉ ES EL PHISHING?

Se trata de una modalidad de ataque por ingeniería social (manipulación psicológica) en la que un criminal suplanta una identidad (de otra persona o una empresa) y, haciéndose pasar por ella, engaña a su victima para obtener información o convencerla de que ejecute una acción que le dará acceso al sistema.
Para ilustrarlo piense en el criminal como un pescador, utiliza como caña un correo electrónico o un mensaje de texto, una oferta imperdible o algo importante y urgente como señuelo, un enlace o un archivo adjunto como anzuelo y el pez es... usted. Es muy probable que ya haya recibido muchos de estos ataques y hasta que haya caído en uno sin saber[3] .
La consecuencia de caer ante el señuelo depende del tipo de anzuelo. Si se trata de un enlace, lo más probable es que lo lleve a una página en donde usted entregue datos personales, incluyendo tarjetas de crédito o nombre de usuario y contraseña de redes sociales u organizacionales. Bien podrá imaginar qué pueden hacer con ello los criminales. Si el anzuelo era un archivo el panorama puede ser aun más conflictivo, ese aplicativo es como el caballo de troya, trae escondido al enemigo.

[2]MFA = Multi Factor Authenticationn; 2FA = Two Factor Authentication.

¿CÓMO DETECTARLOS Y PREVENIRLOS?

- No seguir enlaces ni descargar archivos que provengan de remitentes desconocidos.
- Antes de ejecutar cualquier instrucción de un correo electrónico verifique que el remitente sea genuino, es decir, que sea quien dice ser. Para ello revise el dominio (lo que viene después del @ en una dirección). Este atento a cambios sutiles, por ejemplo: @volkswagen.com/@volksvvawen.com, @cries.org/@cries.net.
- Esté atento a errores en la gramática y redacción del contenido.
- Suelen requerir información personal, de acceso o de pago.
- Suelen incluir una advertencia con consecuencias negativas o un premio que requiere de la intervención del usuario en un plazo muy acotado de tiempo.
- Tenga cuidado con los enlaces acortados, siempre lea a qué dirección lo dirigen antes de presionarlo.

En caso de sospechar que recibió un correo malicioso repórtelo al departamento de seguridad de la organización de inmediato.

Trabajando fuera del entorno laboral

El trabajo remoto no es una novedad, se implementa hace añares en el mundo corporativo e implica exactamente lo que surge de su traducción literal: todo lo que hacíamos en la oficina lo replicamos desde cualquier otro lugar. Esta modalidad acarrea innumerables beneficios, pero también muchos peligros. Suele llevarse a cabo utilizando redes hogareñas –o inclusive abiertas-, que no cuentan con los filtros para que la seguridad de la información esté cubierta. Del mismo modo se suelen utilizar dispositivos personales que no están configurados de forma que el debido resguardo de la información pueda garantizarse. Algunos de esos dispositivos inclusive puede que sean compartidos con compañeros de vivienda o familiares, quienes no siempre están instruidos sobre cómo manejarse en internet de forma segura y responsable. Esto pone de relieve que, aunque sea idéntica la tarea desarrollada, no es igual de seguro llevarla a cabo desde la oficina, desde un café o desde nuestra casa. Se abren múltiples brechas por las que los cibercriminales pueden infiltrarse. Veamos algunos recaudos para evitar que esto pase.

Trabajando desde el hogar

3 Un correo de Netflix indicando que no pudo verificarse su medio de pago, otro de iCloud advirtiendo problemas en su cuenta y que si no actualiza su información será bloqueado, una oferta limitada de un producto a un precio irrisoriamente bajo son algunos ejemplos cotidianos.
Hay una modalidad llamada “Spear Phishing” (“pesca con arpón”). Se utiliza específicamente para ser lanzada contra usted o su organización. Por ejemplo: Usted -o alguien dentro de su empresa- recibe un correo electrónico cuyo remitente aparenta ser de confianza, supongamos de un integrante propio equipo de IT o sistemas. En el mensaje se adjunta un enlace al que se invita a acceder para cambiar una contraseña o rellenar un formulario de la empresa; o bien se adjunta un archivo que se requiere instalar por seguridad.

A) Conexión a la red: Utilice las conexiones previstas por la organización, si se trata de conexión cifrada (VPN[4] o similar) no acceder de ninguna otra manera. De no tener una red de la organización evite tener "abiertas" -sin contraseña- las redes de su hogar.
Lo ideal es modificar la clave con la que viene el router y configurar la red con la seguridad más robusta disponible (WPA2/WPS2). Un recaudo extra es nombrar a la red de forma que no pueda ser vinculada con usted (evitando asignarle su nombre, apellido o el de familiares). Si el router permite configurar dos redes, conecte los dispositivos con los que trabajará a una y utilice la otra para navegar de forma personal, uso de menores de edad o invitados en su hogar.
B) Uso compartido: De ser posible, utilice dispositivos diferentes para trabajar que para uso personal. Caso contrario:
i. Genere usuarios diferentes para un mismo dispositivo. Una configuración posible es crear un usuario administrador, uno para navegación personal de adultos, uno distinto para niños -configurando las restricciones y permisos respectivos- y un cuarto para trabajar.
ii. Asigne a la cuenta que usará para trabajar una contraseña que no compartirá con los demás.
iii. Configure que el dispositivo solicite insertar la contraseña luego de 5-10 minutos en desuso.
C) Correo electrónico laboral: No utilice la cuenta de correo laboral para suscribirse a plataformas, newsletteres, aplicaciones ni eventos. Limite su uso al ámbito organizacional.
D) Plataformas de video conferencia:

- Descargue la aplicación desde el sitio oficial o desde las plataformas propias de cada sistema operativo de sus dispositivos (AppStore en iOS y Google Play Store en Android).
- Si la organización no le provee un usuario, cree una nueva cuenta rellenando el formulario de la página en lugar de utilizar el clásico atajo "iniciar sesión con...". Si se produce una filtración de datos, los criminales tendrán acceso a los que haya completado en ese formulario, no a los de Facebook/Google/LinkedIn, etc.
- No utilice la misma clave que usa para iniciar sesión en otras plataformas.
- Revise si cuenta con la última versión ANTES de cada reunión.
- Configure las sesiones para que sean privadas.
- Establezca una contraseña para que los participantes tengan acceso a la sesión.
- No comparta el link de acceso a una reunión en redes sociales o sitios web, utilice mensajes directos o correos electrónicos a tal efecto.
- Deshabilite las reuniones personales. Si alguien ya se conecto podría utilizar el mismo ID de la sesión para una reunión posterior.
- Aproveche la función de "sala de espera" cuando este disponible. Actívela para controlar y autorizar el ingreso de los participantes.
- Para que las reuniones se desarrollen del modo programado, configure quién puede compartir pantalla durante la sesión.
- En el mismo sentido que el punto anterior, configure previamente que el audio y/o video de los participantes se desactive de forma automática y predeterminada al ingresar a la reunión.
- Remueva a los participantes indeseados de la reunión, inclusive se puede configurar que no puedan volver a ingresar.
- Si desconfía de la procedencia de la invitación a una reunión, en lugar de hacer clic en el enlace, introduzca el ID en la plataforma para evitar ser víctima de phishing.
- No haga clic, ni descargue archivos colocados en la reunión provenientes de un desconocido.

[4]VPN son las siglas de Virtual Private Network (Red Privada Virtual).

E) Comunicación segura: Las plataformas de correo y mensajería tradicional son funcionales, pero no siempre son la alternativa que brinda mayores recaudos de seguridad. ¿Cómo distinguir si comunicamos sin que el contenido se pueda interceptar? Corroborando que el servicio o aplicación provea cifrado de extremo a extremo (end-to-end encryption) ¿Qué significa? Que el contenido de un mensaje sólo es accesible por el remitente y el destinatario.

- Proveedores de correo: Proton mail, CounterMail, Mailference, Tutanota.
- Apps de mensajería: WhatsApp, Telegram, Signal, Keeper chat (se recomiendan especialmente los últimos dos para resguardar la privacidad).
- Transferencia de archivos: OnionShare, Lufi, KeyBase, Datash, Tresorit ,SafeNote, WeTransfer.

Trabajando remotamente

Hoy en día la mayoría de las tareas se pueden realizar desde cualquier lugar, no sólo desde la oficina o el hogar. Establecimientos de café, espacios públicos, hoteles y aeropuertos son tan solo algunos ejemplos de esta modalidad. Pero hay algunos recaudos extras a considerar.
a) No utilice redes wi-fi públicas: Desde redes sin protección es muy sencillo interceptar mensajes, archivos o datos de acceso para un criminal. Utilice la VPN que provee -o autoriza- la organización.
b) No deje sus dispositivos desatendidos: A donde sea que usted va, también su dispositivo, evite que lo hurten y tengan acceso a información confidencial. Como medida extra configure una contraseña para desbloquear la pantalla y acceder al sistema con un timer de auto-bloqueo por desuso.
c) Cifre los archivos de su dispositivos: Si lo pierde o se lo roban de esta forma se evita que alguien pueda acceder al contenido.
d) Saltee las restricciones de navegación estatales: En determinadas zonas geográficas hay sitios de acceso restringido. Si utiliza una VPN podrá navegar libremente, caso contrario recomendamos descargar el navegador TOR.

¿CÓMO REACCIONAR ANTE UN ATAQUE?

Si sospecha que fue víctima de un ataque informático repórtelo ante el departamento de IT (o a quien corresponda) de inmediato. Sí tiene dudas sobre la implementación de las medidas de seguridad recomendadas, solicite asistencia para configurarlas.

[5] https://www.torproject.org