Cómo empezar a cuidar tu seguridad digital

Guía rápida de buenas prácticas

Análisis de gestión de riesgos

La seguridad digital debe planificarse desde la gestión de riesgos. Pretender proteger toda tu información de cualquier persona, todo el tiempo, es poco práctico y un dispendio de recursos innecesario.

Un buen modo de comenzar a ocuparse de la protección de nuestros activos digitales es pensar en soluciones que se adapten a nuestras necesidades. ¿De qué forma? A través de una serie de preguntas podemos realizar una evaluación sobre el estado de situación, para luego analizar qué medidas concretas tomar.

La gestión de la seguridad digital es un proceso integral, que debe desencadenar un cambio de cultura para pensar los riesgos y las prácticas que llevamos adelante para mitigarlos.

Es importante considerar que las decisiones que tomes sobre las medidas de seguridad implican, a su vez, aceptar una menor simplicidad y posible incomodidad. Por eso es que no hay respuestas o soluciones universales.

Recordá que la seguridad digital es un proceso que debe revisarse periódicamente, por lo que las medidas que apliques no van a ser infalibles. Se trata de mitigar y reducir riesgos.

Preguntas para iniciar la evaluación:

- **¿Qué información tengo? ¿Dónde se encuentra almacenada? ¿Quién tiene acceso a la misma? ¿Qué detiene o impide que terceras personas puedan acceder a esa información?**

Por ejemplo: e-mails, contactos, mensajes, documentos y ubicación geográfica presentan diversos niveles de riesgos.

- **¿De quién o de qué la quiero proteger? ¿Quiénes son mis adversarios?**

Se pueden presentar diversos escenarios, por ejemplo: empleado con malas intenciones, robo/hurto/pérdida de dispositivo, intento de ingreso ilegítimo a cuentas/servicios online.

- **¿Qué puede ocurrir si no la protejo? ¿Cuáles son las consecuencias? Este paso ayuda a clasificar la información en base a su riesgo.**

- **¿Qué medidas estoy dispuesto a tomar para proteger esa información?**

Buenas prácticas iniciales

Administración de contraseñas

Las contraseñas son la puerta de entrada a nuestras cuentas.

- Antes que pensar en contraseñas como un conjunto de caracteres con letras, números y símbolos mezclados, podemos usar ***passphrases***, es decir, frases largas que combinan varias palabras.

- Las ***passphrases***, o frases de contraseña, nos permiten cumplir con un criterio más importante que la mezcla de caracteres: la **longitud**. Una frase aleatoria, de al menos, **16 caracteres**, incrementa el tiempo que demandaría "romper" esa clave.

- Una vez que creemos **las frases de contraseña, es importante hacerlo de forma aleatoria. Además, cada servicio o cuenta debe tener su propia clave única.**

- **¿Por qué es importante que las claves sean únicas?** Más allá de que nosotros podamos ser cuidadosos con nuestras contraseñas, asegurarnos de protegerlas y no caer en ninguna trampa, hay otra capa que está fuera de nuestro control y es la seguridad de los servicios que usamos. Si sufren una falla de seguridad, y se filtra información de sus servidores, se puede exponer la información de nuestras cuentas (como el correo electrónico y su contraseña), por lo que una clave única ayuda a evitar que luego puedan ser comprometidas otras cuentas que usaban esa misma contraseña.

¿Cómo gestiono mis claves?

Lo ideal es usar un administrador de contraseñas. Entre los más populares se encuentran:

Los gestores de contraseñas permiten almacenar –mediante el uso de cifrado– todas las claves de una manera segura en tus dispositivos. Estos tres cuentan con distintas funciones en particular, por lo que es conveniente informarte sobre sus características y elegir el que más se adecúe a tu análisis de riesgo.

Además de contar con claves robustas como vimos antes, es necesario activar la **verificación de 2 factores** en todas las cuentas que lo permitan.

Conocido como *"2FA"*, esta es una configuración que nos ayuda a colocar una **segunda barrera de protección al ingreso a nuestras cuentas.** De esta manera, incluso si alguien obtiene la información de usuario y la clave, no podría acceder a la cuenta a menos que tenga la segunda pieza de información.

Este segundo factor puede tener diversos formatos:

a. Algo que sé: como el caso de las respuestas a "preguntas secretas".

b. Algo que tengo: como puede ser una clave numérica brindada por una aplicación, como un *token*.

c. Algo que soy: como el caso de la verificación con datos biométricos, utilizando la huella dactilar o el reconocimiento facial.

Actualmente, la mayoría de los servicios digitales online permiten configurar la verificación de 2 factores a través de un número telefónico o de una app, como medios para conseguir el código de acceso.

Siguiendo estos vínculos vas a poder consultar cómo activar 2FA en: Twitter, Facebook, Instagram, Google (Gmail, Youtube, Drive), Microsoft (Outlook, OneDrive, Skype), Yahoo Mail, iCloud, Dropbox, Slack, WhatsApp, Signal, Telegram y Zoom. En caso de duda, podés consultar en la web Two Factor Auth y buscar si el servicio online que utilizás permite activar 2FA.

En el caso de consignar el número de teléfono, cada vez que inicies sesión en tu cuenta vas a recibir un mensaje de texto (SMS) con un código que te permitirá ingresar. Sin embargo,

este método puede traer otros problemas. Por un lado, le estás brindando más información personal a la empresa, y en base a tu análisis de riesgo tal vez esto lo quieras evitar. Por otra parte, existe el riesgo de que alguien se haga pasar por vos frente a tu compañía de telefonía para obtener una copia de tu tarjeta SIM y de esta forma acceder a los SMS para poder ingresar. Este fraude se conoce como *"SIM swap"*.

Para evitar estos problemas, lo mejor es utilizar una aplicación que genere automáticamente los códigos para ingresar a tu cuenta. Una de las apps más usadas para gestionar la verificación de 2 factores es Authy, aunque existen varias alternativas, incluyendo opciones de código abierto (es decir, que se puede verificar cómo está programada), como andOTP o Aegis.

¿Es cierto que debo cambiar mi contraseña frecuentemente?

Si seguís los pasos y recaudos para generar una frase de contraseña larga, única y que no pueda ser deducida en base a tu información personal (tu equipo deportivo favorito, el colegio donde estudiaste, tu año de nacimiento, el nombre de tu mascota, etcétera) o fácilmente adivinable con un diccionario, no es necesario actualizarla en cortos períodos de tiempo.

Sin embargo, debés considerar otros factores. Por ejemplo, si esa contraseña la compartiste con varias personas que ya no trabajan con vos o que ya no deseás que tengan acceso a tu cuenta. Pero por sobre todo, hay que prestar atención a posibles filtraciones de datos de los servicios que utilizás. Para ello, podés consultar have i been pwned? e informarte si alguna de tus direcciones de e-mail fueron afectadas por filtraciones.

¿Qué se supone que haga con las "preguntas de seguridad"?

En principio, es recomendable que las respuestas no sean reales. Es decir, si la pregunta de seguridad es "¿cómo se llama tu mascota?", no brindar el nombre real de ella sino uno inventado. Podemos generar palabras o caracteres aleatorios con el gestor de contraseñas y utilizarlas para las respuestas, o inventar algunas alternativas totalmente ficticias.

¿De qué hay que tener cuidado? Debe evitarse brindar indicios o datos que luego puedan utilizarse como ventaja para comprometer nuestras cuentas. En particular, cuando se trata de información de familiares, mascotas, o aspectos personales que son de difusión pública. Esto es en especial relevante en el caso de personas con una alta exposición pública y que tengan una fuerte presencia online por su profesión.

Detectar *phishing, malware,* sitios falsos y otros engaños

Cuando trabajamos con herramientas digitales, podemos encontrarnos con sitios web o emails que parecen reales, pero que en realidad presentan un peligro inminente para nuestra seguridad, al tratar de hacernos caer en la trampa de ingresar nuestra clave y perder control de la cuenta. Esta práctica, conocida como *phishing*, puede darse en diversos ámbitos, contextos y formatos. El *phishing* puede ser general o estar dirigido a un destinatario específico (conocido como *spearphishing*).

Por eso es importante familiarizarse con algunos indicios que permiten agudizar la vista para tratar de detectar los casos de *phishing*, ya sea que lleguen vía e-mail, mensaje o sitios web en general.

La principal recomendación es verificar la fuente de las URL. Esta es la dirección web a la cual está dirigiendo un *link*, un botón, una imagen, etcétera. ¡Es importante revisar los *links* completos!

Por ejemplo, los siguientes URL están pensados para simular ser servicios de Google y Paypal:

https://drive--google.com
https://drive.google.com.download-photo.sytez.net/AONh1e0hVP
googloclassroom\.com
googieclassroom\.com
https://www.paypaI.com/ (con mayúscula "i" en lugar de una minúscula "L")

Estos claros ejemplos de phishing utilizan leves cambios de gramática para que a simple vista se lean rápidamente como los sitios originales, pero en realidad conducen a sitios maliciosos que tratarán de recolectar tus claves de acceso cuando intentes iniciar sesión.

Algunos tips para detectar casos de *phishing:*

- ¿El nombre está bien escrito?
- ¿A qué URL dirige un *link* en un e-mail?
- ¿Coincide con el *link* oficial que conozco?
- ¿El lenguaje que utiliza es igual a la manera oficial en la que se dirige la empresa/servicio?
- No te confíes solo porque una web utilice cifrado con HTTPS.

Podés poner a prueba tus habilidades con dos juegos: https://phishingquiz.withgoogle.com y https://safe.page/quiz

Es importante, también, estar atento sobre la posibilidad de recibir malware en los canales de comunicación, ya sea un mensaje de texto, WhatsApp, e-mail, un documento en PDF o planilla de cálculo, etcétera.

El *malware* es un programa malicioso que está diseñado para comprometer la seguridad de un dispositivo, por lo general con el fin de tomar control del mismo para poder acceder a su contenido.

Servicios como VirusTotal permiten remitirles documentos o URLs para corroborar que no se trate de ningún archivo amenazante que contiene *malware*.

(re)Tomar control sobre tus dispositivos y comunicación

Al igual que los servicios online que utilices, tus dispositivos también necesitan atención. A continuación repasamos algunos aspectos elementales que no podés olvidar:

a. Mantener el sistema operativo y el software/apps actualizados

b. Asignar claves a los dispositivos y activar el cifrado completo del mismo (conocido como *full disk encryption*):

- Smartphones: en el caso de iOS, una vez que configurás la clave, el dispositivo ya activa el cifrado. Para smartphones con Android, desde la versión 6.0 en adelante debería estar cifrado por defecto cuando utilizas un PIN. Si no es el caso, podés seguir estos simples pasos.

- Computadoras de escritorio y notebooks: si utilizás Windows podés consultar esta guía de Microsoft para verificar que tu versión pueda activar el cifrado. En el caso de macOS, una vez que configurás una clave la computadora ya activa el cifrado.

Si usás alguna distribución de Linux, debés activar la opción de cifrado al momento de instalar el sistema operativo.

c. Revisar las configuraciones de privacidad en las aplicaciones

- Qué *apps* de terceros pueden acceder a nuestras cuentas (por ejemplo, para realizar publicaciones en redes sociales de manera automática).

- Qué información es recolectada sobre nosotros y nuestros dispositivos (geolocalización, por ejemplo).

d. Utilizar canales de comunicación seguros

- Servicios como Signal, Wire, WhatsApp o iMessage, ofrecen cifrado de punto a punto para todos los mensajes que envíes (e incluso para las llamadas). Esto impide que algún intermediario en la red –como tu proveedor de servicio de internet– pueda ver esos mensajes.

- Es importante que consideres, en base a tu análisis de riesgo, qué información vas a compartir a través de qué canal. Por ejemplo, tal vez puede ser útil pensar en el correo electrónico como igual que una tarjeta postal: el intermediario en esa comunicación (el servicio de email o un tercero que intercepte la comunicación), puede ver a quién le escribiste y qué enviaste.

Seguridad desde el mundo físico

Finalmente, junto con el ámbito virtual también hay que considerar qué ocurre en el espacio físico, para evaluar de qué necesitás protegerte. Te compartimos dos escenarios puntuales que pueden inspirarte para considerar tu contexto particular:

1. Te encontrás en un lugar rodeado de muchas personas, tal vez en el espacio de trabajo o en un espacio público, y te llega un mensaje. ¿Leerías el mensaje inmediatamente? Antes de hacerlo, ¿consideraste la posibilidad de que alguien a tu alrededor pueda husmear lo que ocurre en la pantalla de tu dispositivo? Podés considerar, también, utilizar un protector de pantalla de privacidad, que oscurece la misma cuando se ve desde un ángulo.

2. En medio de una reunión, debés atender un llamado y dejaste tu tablet o computadora sobre la mesa de la sala. ¿Bloqueaste los dispositivos para que nadie pueda ingresar sin la clave o ver lo que tenías en pantalla?

Es considerado una buena práctica mantener dispositivos separados para el uso personal y profesional. De esta manera, reducis la posibilidad de que algún problema en tus cuentas personales desencadene otros inconvenientes en tus activos digitales de trabajo. En base a tu análisis de riesgo, considerá la posibilidad de incorporar múltiples dispositivos con distintos propósitos específicos.

* * *