TECNOLOGÍA

# Más vale cambiar las contraseñas que curar

La ciberseguridad es una constante partida de ajedrez entre hackers con intenciones funestas y usuarios que muchas veces están despistados sobre los riesgos que corren durante su presencia en el mundo digital.

FABIÁN MUSO
Domingo, 21 Octubre 2016





Foto: Max Pixel

La ciberseguridad es, en sí, una quimera, un espejismo. No existe, al menos todavía, una defensa impenetrable contra un ataque virtual. Por eso, cuando el año pasado el presidente estadounidense Donald Trump ruteó que había estado hablando con el presidente Vladimir Putin sobre crear una ciberdefensa "impenetrable", muchos expertos fruncieron el ceño. En la revista *The Atlantic*, una de sus editoras (Adrienne Lafrance) calificó la noción expuesta por Trump como una "fantasía". "Nada conectado a Internet está a resguardo de hackers. Nada. La ciberseguridad moderna es un ciclo constante de brechas a sistemas y parches para tapar esas brechas". Como si fuera una partida de ajedrez interminable, hackers y los encargados de seguridad mueven sus fichas y —como escribió Lafrance— "cada lado intenta ser más astuto que el contrincante, y uno de ellos siempre está un paso adelante en un momento dado".

## Lo que hay que saber

Esa partida de ajedrez que no deja de jugarse nunca obliga a los usuarios a actualizarse continuamente sobre aspectos de seguridad y prevención. Hace años que solo alcanzaba con saber qué era un virus. Ahora también hay que tener alguna noción sobre términos como estos:

**Adware**: Software no deseado diseñado para mostrar anuncios en su pantalla (...) Normalmente, recurre a un método subrepticio: bien se hace pasar por legítimo, o bien mediante *piggyback* en otro programa para engañarlo e instalarse en su PC, tablet o dispositivo móvil (fuente).

**Malware**: Abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento (fuente).

**Ransomware**: Los hackers utilizan esta técnica para bloquear sus dispositivos y exigir un rescate a cambio de recuperar el acceso (fuente).

**Exploits**: Programa que se aprovecha de un agujero de seguridad (vulnerabilidad) en una aplicación o sistema, de forma que un atacante podría usarla en su beneficio (fuente).

## Lo que dicen los expertos

Mateo Martínez es, además de experto en seguridad informática, director de la empresa Krav Maga Hacking, que asesora a empresas y gobiernos en este tema. Para él, que también trabaja como docente en la Universidad ORT, hay algunos conceptos sobre seguridad en el ciberespacio que conviene manejar intelectualmente:

## Conceptos

**Segundo Factor de Autenticación**: "Hoy, la mayoría de las redes sociales tienen la opción de este tipo de funcionalidades que exigen que además de usuario y contraseña se defina una clave única que se envía por SMS al teléfono celular para validar al usuario y dejarlo acceder. Esto permite que por más que un atacante robe usuario y contraseña de un usuario, no podrá acceder a sus servicios".

**VPN**: (*Red Privada Virtual, por su sigla en inglés*) "Servicios que permiten proteger la información que se transmite por Internet, más allá de que se trate de una red hostil. Crea un túnel cifrado entre nuestro dispositivo y el proveedor de la VPN, lo que protege todos los datos que transmitimos.

**Cifrado**: "Protege la información a través de algoritmos que modifican el contenido de un mensaje y no permiten acceder a la información real salvo a quienes conozcan la clave para realizar el descifrado".

Para el ingeniero Eduardo Carozo, gerente de la empresa de tecnología y comunicación ITC, hay que tener en cuenta que cada dispositivo (celular, *tablet*, PC) puede ser una "grieta" por la cual se pueden colar riesgos: "Hay que pensar en la ciberseguridad para cada dispositivo que incorporemos a nuestra vida, desde el marcapasos, pasando por el *router* WiFi y la computadora o celular, puesto que un dispositivo mal usado es una grieta por la que se cuela nuestra información sensible. Un ejemplo claro de esto son los sistemas baratos de vigilancia por cámaras de video. La mayoría de ellos son accesibles por terceras personas, pero el usuario no lo sabe. Todo nuevo dispositivo debe ser validado y revisado periódicamente, y se debe tener en cuenta que según ingresamos a la sociedad tecnológica, serán cada vez más los sistemas que interactúen con nosotros para hacer tareas que son más importantes, a menudo vitales".

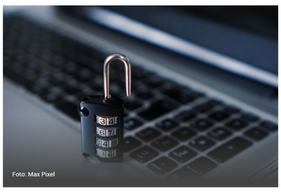

Foto: Max Pixel

También es fundamental pensar a largo plazo: "Cada vez que me vinculo con el celular, la computadora o un asistente electrónico (Alexa, por ejemplo) tengo que saber que estoy dando información relevante, como la ubicación e identificación del dispositivo. Toda esa información, más las fotos, identidades compuestas por usuario y contraseña, videos, información de uso, *likes* o visualizaciones en una página web, se va almacenando y es importante ser consciente del impacto futuro que tiene dejar esos datos que brindamos en forma constante y permanente. En este aspecto, cuanto menos información brindemos, mejor", comenta Carozo.

MATEO MARTÍNEZ, KRAV MAGA HACKING

## Tips básicos

--Navegar de forma anónima en la web, incluso en celulares y tablets.
--Usar servicios de VPN al navegar desde redes inseguras como cafeterías, shoppings, aeropuertos. Eso permite que toda la comunicación esté cifrada y que nadie pueda intervenirla. Existen múltiples servicios gratuitos.
--Usar servicios de mensajería y de voz con cifrado, como WhatsApp, Telegram o Signal.
--No publicar información sensible o personal en redes sociales.
--Aquellos documentos que sean sensibles, compartirlos en archivos comprimidos con clave.

Carozo también destaca la importancia de aprender a diferenciar un sitio legítimo, que usará los datos personales del usuario de manera adecuada, de uno que tiene como finalidad hacerse del dinero de ese usuario. Hay muchas páginas que, según él, se "cuelgan" de Internet aparentando ser sitios de tarjetas de crédito, banca electrónica o portales de pago electrónico. "El fin es robar su dinero, simulando ser usted".

## Cuando ocurre la catástrofe

Si llegara a ocurrir la catástrofe, hay que reducir daños. Primero, como recomiendan expertos como el editor de noticias de *Wired* Brian Barret, hay que intentar corroborar las barreras como las contraseñas han sido derribadas.

## Reducción de daños

Consultar el sitio haveibeenpwned.com, que puede consultarse para verificar si alguna cuenta de correo electrónico ha sido comprometida. Luego, hay que cambiar las contraseñas, y no volver a usar aquellas que ya han sido utilizadas.
Para no andar con un papelito con un montón de contraseñas anotadas, lo mejor es usar un gestor. La publicación especializada PC Mag hizo un estudio este año sobre estas herramientas, y recomendó a Last Pass como gestor gratuito y a Dashlane como servicio premium, a 40 dólares por año.

## Ciberseguridad para los más pequeños

"Debemos intentar que sea parte de la educación en la familia y en el colegio. Así como les enseñamos a no hablar con extraños, debemos enseñarles a no hablar con extraños en Internet, a cuidar su privacidad, a respetar a otros. Es importante hablar con ellos de estos temas, conocer las aplicaciones que utilizan, orientarlos y recomendarles cómo actuar frente a diversas situaciones peligrosas", dice Mateo Martínez, de Universidad ORT y agrega que "desde la organización (ISC) 2 estamos lanzando en Uruguay el programa Safe and Secure Online en la cual ofrecemos dar charlas en colegios para padres, alumnos y profesores en estos temas"

Por su parte, Eduardo Carozo, gerente de la empresa de tecnología ITC, resalta la importancia de compartir tiempo *online* con hijos e hijas. "Estar con ellos en sus interacciones en Internet es como enseñarles a cruzar la calle o pasear en la ciudad. Les tenemos que mostrar los riesgos. Dejarlos solos es igual a abrir la puerta de casa a un niño de dos años o dejarlo cinco horas solo sin supervisión, en la vereda. No lo haríamos ¿verdad? Tampoco le prohibimos salir de casa. Lo que hacemos es salir con ellos a la plaza más cercana y enseñarles a convivir con los riesgos. En el mundo cibernético es exactamente igual. Negando el acceso es cercenarles oportunidades de desarrollo y no prepararlos para la convivencia digital, cada vez más importante".