Cuentas protegidas. Ciberseguridad en tiempos de aislamiento/5

Cuentas protegidas.
La ciberseguridad en tiempos de cuarentena

VIGILANCIA
Guía de recomendaciones

El aislamiento aumenta las horas frente a la computadora y multiplica las posibilidades de ser víctimas de ataques online

Mónica Fernández
PARA LA NACIÓN

Computadoras, tablets y celulares trabajan a destajo por estos días. Casi sin respiro, cumplen con el *home office*, son el vehículo para pagar cuentas y hacer transferencias, al rato tienen a un niño sentado frente a su clase de matemáticas y antes de terminar el día se convierten en pantalla de cine. Son una puerta abierta al exterior. Y también una puerta abierta a ciberataques.

"Los cibercriminales siempre están esperando este tipo de oportunidades y usan la ingeniería social para explotar la debilidad humana, como cualquier otra vulnerabilidad. La ingeniería social es esencialmente una forma de manipulación de las personas y una forma fácil para los criminales de obtener ingresos con resultados altamente efectivos", describe Fabián Bogado, gerente de Consultoría en Sistemas de Grant Thornton Argentina.

"Los ataques se multiplicaron porque pasamos más tiempo online y eso nos hace durante más tiempo vulnerables, estamos muy preocupados por temas que nada tienen que ver con la seguridad informática y eso nos hace cometer errores. Además dependemos de una infraestructura digital casera que no siempre es segura", advierte Martín Elizalde, al frente de Foresenics, e inmediatamente subraya: "Siempre hay que estar atentos, con o sin pandemia".

Roberto Heker, director de NextVision, una firma dedicada a la ciberseguridad, lo explica en términos sencillos: "El tipo de engaño más frecuente es el *phishing*: viene del término en inglés 'pescar' y es una técnica que busca engañar a los usuarios para robar sus datos personales, bancarios o de las tarjetas".

"La gente está pasando más horas conectada a internet: para relacionarse, hacer pagos, hacer actividades de ocio y trabajar. Incluso compartimos el mismo equipo distintos miembros de la familia, y el control de lo que se hace sobre el dispositivo es aún más difícil", detalla Heker y advierte que según los últimos informes, la Argentina se posiciona entre los primeros países de Latinoamérica en recibir ataques cibernéticos.

Los cibercriminales están siempre al acecho de oportunidades de estafa SHUTTERSTOCK

El "engaño", el *phishing* como lo llaman los especialistas en sistemas, vienen en mails, enlaces o documentos disfrazados de indicaciones sobre cómo prevenir el coronavirus o falsas guías o comunicados que parecen provenientes de la mismísima Organización Mundial de la Salud (OMS).

Todos lo sufrimos varias veces al día con dominios "covid", "corona" o "virus", entre otros. Muchos logramos identificarlos, y evitarlos. Pero son tantos, que en algún momento "pescan" a alguien con las defensas bajas. Es igual que el cuento del tío o los secuestros virtuales: los delincuentes hacen miles y miles de intentos que fallan, hasta que dan con su víctima. "Tenemos que ponernos en la cabeza de un ciberdelincuente. Hoy se encuentra ante un escenario ideal para engañar en el mundo digital. Por ejemplo en la última semana, la policía española detectó 12.000 sitios nuevos falsos ofreciendo curas al virus, promociones de productos o servicios de diferente índole aprovechando la cuarentena. Estas promociones nos llegan por muchos sitios, entre ellos el teléfono, el sitio donde somos más vulnerables a dar doble clic", plantea Heker.

¿Cómo protegernos? Los especialistas despliegan una larga lista de medidas preventivas. "Probablemente nueve de cada diez inicios de sesión sean maliciosos. Pero también es cierto que en un 95% de los casos, los incidentes pueden evitarse con prevención", dice Elizalde y pone sobre la mesa sus primeras recomendaciones:

- Mantener actualizados sistemas y software. Aceptar las actualizaciones, aunque "detengan" por un rato la PC o el celular.
- Asegurar su punto de acceso wifi (no utilizar redes públicas, sin contraseñas)
- Usar una red privada virtual (VPN).

Las recomendaciones de Grant Thornton van de lo general a lo particular:

- Es preferible entrar a sitios web tecleando la dirección antes que entrar cliqueando enlaces sospechosos. Siempre conviene asegurarse de haber escrito bien la dirección del sitio web, ya que muchas se aprovechan de una letra fuera de lugar.
- Es recomendable no responder a una solicitud de información personal a través de correo electrónico o mensaje de texto (SMS). Las entidades y organismos jamás solicitan contraseñas o tarjetas de crédito.
- Es aconsejable comprobar que la página web a la que se accede tiene un protocolo de seguridad. En la barra del navegador debe comenzar con https:// y tener un pequeño candado, por lo general de color verde.
- Conviene analizar archivos adjuntos incluso cuando se esté esperando recibirlos y/o provengan de personas conocidas. Algunos servicios de correo lo hacen de forma automática, pero si no lo hiciera puede recurrirse a un antivirus.
- Contar con un filtro de spam en la casilla de correo.

Finalmente la lista la completa Heker de NextVision con recomendaciones para grandes y chicos:

- No descargar programas ni películas, música en sitios gratuitos. Suelen ser creados por los ciberdelincuentes para añadir virus.
- Verificar que en las reuniones a distancia (Zoom, Skype, *meetings*, etc.) no haya presencia de desconocidos. En lo posible, que accedan con contraseña provista por el organizador.
- Tapar la webcam cuando no se está utilizando. Una cinta adhesiva opaca es suficiente.
- Hacer *backup* de los datos en un disco externo o en la nube (hay muchos sitios como Dropbox, Box, Drive, etc.). Esto nos facilitará la recuperación de los datos en caso de una situación donde la información se extravíe. En el caso de los discos externos, solo mantenerlos conectados al equipo cuando se hace el *backup*, dado que si un *ransomware* se activa, cifra todas las unidades conectadas en ese momento.

Plataformas seguras

¿Qué pasa con las cuentas bancarias y otros sitios de pago online?. "El movimiento bancario se hace a través de plataformas seguras. La banca online es segura siempre que se navegue en el sitio oficial. Lo mismo con las aplicaciones (para el teléfono) que se descargan del sitio oficial", tranquiliza Elizalde.

"Debemos contar con contraseñas seguras. Son las llaves de nuestro mundo digital. Como no damos las llaves de nuestra casa a nadie, jamás deberíamos dar nuestras contraseñas a quien nos las solicite. Si sucede, es una clara pista de que estamos ante una estafa", postula Heker, y recomienda "no utilizar las mismas contraseñas para los servicios, ni aplicaciones ni redes sociales. Deben contener números, letras mayúsculas y minúsculas y en lo posible caracteres como -,*./ u otros".

El especialista desaconseja también tener anotadas las contraseñas. Si no se pueden memorizar, la opción es la opción es utilizar aplicaciones para guardarlas. Son como llaveros digitales, que las conservan en forma segura.

"Más allá del *phishing*, los cibercriminales pueden realizar ataques mediante el uso de distintas técnicas, ya sea a través de links maliciosos o páginas falsas o mediante *malware* del tipo *ransomware*; por ejemplo", advierte Eduardo Diego, gerente de sistemas de Grant Thornton. "En las últimas semanas, por ejemplo, se ha detectado el uso de NetWalker, un *ransomware* empleado por los criminales para atacar hospitales de EE.UU. y España, y que afectan a los equipos de alta tecnología de los centros de salud", agrega.

Queda claro que no es un problema solo hogareño. Los ciberdelincuentes están por todos lados y en tiempos de coronavirus y aislamiento más que nunca se impone estar muy atentos. "Siempre aconsejamos como medida preventiva, utilizar el sentido común y desconfiar. Es muy común que este tipo de engaños interpelen nuestras emociones, nos entusiasmen por conseguir algo gratis o nos apuren a tomar alguna acción. Si en el mundo real nadie nos regala nada, ¿por qué Netflix, por ejemplo, querría regalarnos un año de servicio gratis?", advierte para finalizar Heker.●

EN LA MIRA

29%
ATAQUES
Es el porcentaje de las empresas argentinas que fueron víctimas de ciberataques, según un relevamiento de la consultora Ipsos

51%
VULNERABLES
Es el porcentaje de las firmas locales que declararon sentirse vulnerables ante la acción de los cibercriminales. La industria de los servicios es la más afectada.

Cuentas protegidas. Ciberseguridad en tiempos de aislamiento/5 Cuentas protegidas. La ciberseguridad en tiempos de cuarentena

vigilancia Guía de recomendaciones El aislamiento aumenta las horas frente a la computadora y multiplica las posibilidades de ser víctimas de ataques online

Mónica Fernández

pARA LA NACIóN Computadoras, tablets y celulares trabajan a destajo por estos días. Casi sin respiro, cumplen con el home office, son el vehículo para pagar cuentas y hacer transferencias, al rato tienen a un niño sentado frente a su clase de matemáticas y antes de terminar el día se convierten en pantalla de cine. Son una puerta abierta al exterior. Y también una puerta abierta a ciberataques.

`Los cibercriminales siempre están esperando este tipo de oportunidades y usan la ingeniería social para explotar la debilidad humana, como cualquier otra vulnerabilidad. La ingeniería social es esencialmente una forma de manipulación de las personas y una forma fácil para los criminales de obtener ingresos con resultados altamente efectivos`, describe Fabián Bogado, gerente de Consultoría en Sistemas de Grant Thornton Argentina.

`Los ataques se multiplicaron porque pasamos más tiempo online y eso nos hace durante más tiempo vulnerables, estamos muy preocupados por temas que nada tienen que ver con la seguridad informática y eso nos hace cometer errores. Además dependemos de una infraestructura digital casera que no siempre es segura`, advierte Martín Elizalde, al frente de Foresenics, e inmediatamente subraya: `Siempre hay que estar atentos, con o sin pandemia`. Roberto Heker, director de Next- Vision, una firma dedicada a la ciberseguridad, lo explica en términos sencillos: `El tipo de engaño más frecuente es el phishing: viene del término en inglés ´pescar´ y es una técnica que busca engañar a los usuarios para robar sus datos personales, bancarios o de las tarjetas`.

`La gente está pasando más horas conectada a internet: para relacionarse, hacer pagos, hacer actividades de ocio y trabajar. Incluso compartimos el mismo equipo distintos miembros de la familia, y el control de lo que se hace sobre el dispositivo es aún más difícil`, detalla Heker y advierte que según los últimos informes, la Argentina se posiciona entre los primeros países de Latinoamérica en recibir ataques cibernéticos. El `engaño`, el phishing como lo llaman los especialistas en sistemas, vienen en mails, enlaces o documentos disfrazados de indicaciones sobre cómo prevenir el coronavirus o falsas guías o comunicados que parecen provenientes de la mismísima Organización Mundial de la Salud (OMS). Todos lo sufrimos varias veces al día con dominios `covid`, `corona` o `virus`, entre otros. Muchos logramos identificarlos, y evitarlos. pero son tantos, que en algún momento `pescan` a alguien con las defensas bajas. Es igual que el cuento del tío o los secuestros virtuales: los delincuentes hacen miles y miles de intentos que fallan, hasta que dan con su víctima. `Tenemos que ponernos en la cabeza de un ciberdelincuente. Hoy se encuentra ante un escenario ideal para engañar en el mundo digital. por ejemplo en la última semana, la policía española detectó 12.000 sitios nuevos falsos ofreciendo curas al virus, promociones de productos o servicios de diferente índole aprovechando la cuarentena. Estas promociones nos llegan por muchos sitios, entre ellos el teléfono, el sitio donde somos más vulnerables a dar doble clic`, plantea Heker. ¿Cómo protegernos? Los especialistas despliegan una larga lista de medidas preventivas. `probablemente nueve de cada diez inicios de sesión sean maliciosos. pero también es cierto que en un 95% de los casos, los incidentes pueden evitarse con prevención`, dice Elizalde y pone sobre la mesa sus primeras recomendaciones: b Mantener actualizados sistemas y software. Aceptar las actualizaciones, aunque `detengan` por un rato la pC o el celular. b Asegurar su punto de acceso wifi (no utilizar redes públicas, sin contraseñas) b Usar una red privada virtual (VpN). Las recomendaciones de Grant Thornton van de lo general a lo particular: b Es preferible entrar a sitios web tecleando la dirección antes que entrar cliqueando enlaces sospechosos. Siempre conviene asegurarse de haber escrito bien la dirección del sitio web, ya que muchas se aprovechan de una letra fuera de lugar. b Es recomendable no responder a una solicitud de información personal a través de correo electrónico o mensaje de texto (SMS). Las entidades y organismos jamás solicitan contraseñas o tarjetas de crédito. b Es aconsejable comprobar que la página web a la que se accede tiene un protocolo de seguridad. En la barra del navegador debe comenzar con https:// y tener un pequeño candado, por lo general de color verde.

b Conviene analizar archivos adjuntos incluso cuando se esté esperando recibirlos y/o provengan de personas conocidas. Algunos servicios de correo lo hacen de forma automática, pero si no lo hiciera puede recurrirse a un antivirus.

b Contar con un filtro de spam en la casilla de correo. Finalmente la lista la completa Heker de NextVision con recomendaciones para grandes y chicos:

b No descargar programas ni películas, música en sitios gratuitos. Suelen ser creados por los ciberdelincuentes para añadir virus. bVerificar que en las reuniones a distancia (Zoom, Skype, meetings, etc.) no haya presencia de desconocidos. En lo posible, que accedan con contraseña provista por el organizador.

bTapar la webcam cuando no se está utilizando. Una cinta adhesiva opaca es suficiente.

bHacer backup de los datos en un disco externo o en la nube (hay muchos sitios como Dropbox, Box, Drive, etc.). Esto nos facilitará la recuperación de los datos en caso de una situación donde la información se extravíe. En el caso de los discos externos, solo mantenerlos conectados al equipo cuando se hace el backup, dado que si un ransomware se activa, cifra todas las unidades conectadas en ese momento. Plataformas seguras ¿Qué pasa con las cuentas bancarias y otros sitios de pago online?. `El movimiento bancario se hace a través de plataformas seguras. La banca online es segura siempre que se navegue en el sitio oficial. Lo mismo con las aplicaciones (para el teléfono) que se descargan del sitio oficial`, tranquiliza Elizalde.

`Debemos contar con contraseñas seguras. Son las llaves de nuestro mundo digital. Como no damos las llaves de nuestra a casa a nadie, jamás deberíamos dar nuestras contraseñas a quien nos las solicite. Si sucede, es una clara pista de que estamos ante una estafa`, postula Heker, y recomienda `no utilizar las mismas contraseñas para los servicios, ni aplicaciones ni redes sociales. Deben contener números, letras mayúsculas y minúsculas y en lo posible caracteres como -,,/ u otros`. El especialista desaconseja también tener anotadas las contraseñas.

Si no se pueden memorizar, la opción es la opción es utilizar aplicaciones para guardarlas. Son como llaveros digitales, que las conservan en forma segura.

`Más allá del phishing, los cibercriminales pueden realizar ataques mediante el uso de distintas técnicas, ya sea a través de links maliciosos o páginas falsas o mediante malware del tipo ransomware; por ejemplo`, advierte Eduardo Diego, gerente de sistemas de Grant Thornton. `En las últimas semanas, por ejemplo, se ha detectado el uso de NetWalker, un ransomware empleado por los criminales para atacar hospitales de EE.UU. y España, y que afectan a los equipos de alta tecnología de los centros de salud`, agrega. Queda claro que no es un problema solo hogareño. Los ciberdelincuentes están por todos lados y en tiempos de coronavirus y aislamiento más que nunca se impone estar muy atentos. `Siempre aconsejamos como medida preventiva, utilizar el sentido común y desconfiar. Es muy común que este tipo de engaños interpelen nuestras emociones, nos entusiasmen por conseguir algo gratis o nos apuren a tomar alguna acción. Si en el mundo real nadie nos regala nada, ¿por qué Netflix, por ejemplo, querría regalarnos un año de servicio gratis?`, advierte para finalizar Heker.ß shutterstock Los cibercriminales están siempre al acecho de oportunidades de estafa

en la Mira 29% ataques Es el porcentaje de las empresas argentinas que fueron víctimas de ciberataques, según un relevamiento de la consultora Ipsos 51% vuLnerabLes Es el porcentaje de las firmas locales que declararon sentirse vulnerables ante la acción de los cibercriminales. La industria de los servicios es la más afectada.

finanzas personaLes