www.psicoadolescencia.com.ar

Ciberdelito:
claves para no caer en los nuevos engaños

Cómo prevenir los ataques a las redes sociales y los celulares

La frontera entre el mundo online y offline es cada vez más invisible. Hoy se trabaja, se habla con amigos, se compra y se busca entretenimiento en Internet con tal naturalidad que a veces puede olvidarse de que todo -absolutamente todo- lo que se hace allí deja una huella, y de que ese rastro puede ser una vulnerabilidad.

Conocer cuáles son los peligros a los que uno se expone es una las maneras de proteger los datos sensibles y la identidad digital. Más en momentos en que las redes sociales y las aplicaciones para celulares quedaron en el ojo de los ataques de piratas informáticos.

¿En qué consisten las principales amenazas digitales y cómo evitarlas? Es la pregunta que aparece ante los miedos de un mundo de actualizaciones permanentes. Especialistas en seguridad informática ayudan a navegar más tranquilos en la web.

"Hay una mafia que se hace de las bases de datos para mandar los mails; otra que recluta los datos de los que caen en el engaño, y otra que los usa para obtener dinero de manera no consentida", explica Daniel Monastersky, abogado especialista en ciberdelitos.

El phishing es una maniobra mediante la cual, haciéndose pasar por una empresa o institución, delincuentes informáticos consiguen que la víctima le entregue voluntariamente datos personales. Envían, por ejemplo, mails con direcciones similares a las de esa empresa - info@nombredetubanco.com-, con plantillas que también imitan su identidad gráfica, donde piden al receptor que realice una acción a través de un link, como confirmar su usuario y contraseña.

"Hemos detectado movimiento irregular en su cuenta desde un acceso remoto, vaya al link para modificar la clave y evitar inconvenientes", es el mensaje habitual que abre la puerta al engaño. Si el destinatario sigue las instrucciones, los datos que vierta en ese link van a quedar en manos y a merced de estafadores que pueden, siguiendo el ejemplo del banco, usarlos para hacer compras y transferencias.

¿Cómo se puede evitar esa estafa? Las empresas no suelen pedir por mail que se cambie contraseñas, descargue aplicaciones o se desconozca montos. Ese ya es motivo suficiente para desconfiar de ese tipo de correos que piden que realicen una acción a través de un link. "Si te metés en cualquier **home banking**, es mejor siempre tipear la dirección en tu buscador. Si tenés que modificar contraseñas o volcar cualquier tipo de información

sensible, nunca lo hagas desde un enlace que te llega por mail", recomienda Monastersky, abogado especializado en delitos informáticos.

Otra trampa puede aparecer cuando uno se conecta a una red de **wi-fi pública**, como las de aeropuertos, plazas, bares y centros comerciales. Los especialistas en ciberdelitos recomiendan preguntarse antes que nada si realmente se tiene necesidad y urgencia de hacer esa conexión. Si la respuesta es sí, el segundo consejo es tomar algunas precauciones. El riesgo es que esa red sea impostora, que no venga del aeropuerto, centro comercial o bar, sino desde la computadora de un tercero que puede ver todo lo que se realiza. Se conoce a esta maniobra como "man in the middle".

¿Qué se debería hacer cuando la conexión no es considerada segura? "No la uses para poner en internet información sensible. Si tenés que hacer una transferencia o compras con tarjeta de crédito, es más seguro usar 3G que un wi-fi público. También tenés que mirar que **las páginas que estás navegando digan "https" en la URL**. Ese es un protocolo de seguridad que significa que la información que brindes ahí va a estar cifrada. Es decir que si alguien la capta en el camino, le va a resultar inteligible", aconseja Monastersky.

Todo por un "me gusta"

El sistema de **phishing** se extendió a las redes sociales. Las técnicas para que entregues datos de manera voluntaria, pero para fines no consentidos, también suceden en esos lugares de encuentros con amigos en el cibermundo.

"Los delincuentes las aprovechan para difundir su código malicioso a través de páginas web publicadas, por ejemplo, en Facebook. Una vez que un usuario abre estos sitios -aunque los cierre enseguida-, el enlace se publica automáticamente sin su consentimiento en su muro, incluso con su propio like", explica Pamela Pérez, especialista de ***riesgo de PayPal*** Hispanoamérica.

Una **técnica para evitarlo** es pararse con el cursor sobre el link que estamos a punto de clickear y ver si la URL que aparece en la esquina inferior izquierda del navegador es de confianza. "Si ya fuiste víctima -dice Pérez-, lo primero es evitar la propagación: eliminá el posteo y avisá a tus contactos que hagan caso omiso al mismo. Después, utilizá tu antivirus para revisar que ningún malware (virus) haya quedado instalado".

Falsas Apps

Las aplicaciones falsas para celulares son otra nueva forma de trampas en la red. Para asegurarse de que las aplicaciones descargadas en el teléfono sean seguras, el recaudo fundamental es bajarlas desde plataformas oficiales -como Google Play y App Store-. "Estas tiendas de aplicaciones se encargan de que las que están publicadas ahí sean medianamente seguras. También hay que ser cuidadosos con los videojuegos. Algunos te

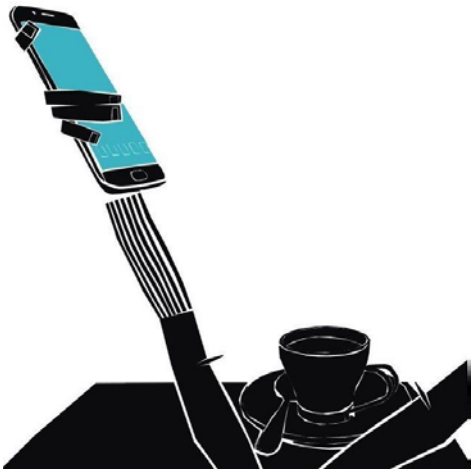
dan la opción de jugar en línea o bajar el archivo, y si accedés a decargarlo lo estás haciendo desde un vector no oficial, que puede contener algún tipo de malware", advierte Gustavo Linares, Director General de Seguridad Informática del Gobierno de la Ciudad de Buenos Aires.

La seguridad en las compras es otro momento a tomar en cuenta. Según la ***Cámara Argentina de Comercio Electrónico***, durante 2016 se facturaron 102 mil millones de pesos por ese medio. Los beneficios de comprar a través de internet están a la vista, pero hay que tomar recaudos para que los datos bancarios queden protegidos. Según Horacio Azzolin, Fiscal en la Unidad Fiscal Especializada en Ciberdelincuencia, es ***recomendable usar las plataformas de pago conocidas, como MercadoPago y PayPal***, que cifran los paquetes de datos, y nunca tildar la opción de dejar guardados los datos de la tarjeta de crédito, para que no queden en servidores más tiempo que el necesario.

También es importante chequear que el sitio -una agencia de viajes o un centro de estética, por ejemplo- tenga el protocolo "***https***". Azzolin agregó: "Otro consejo es usar sistemas operativos actualizados, que ya hayan reparado los agujeros de seguridad que puedan tener las versiones anteriores, y tener antivirus con web security, que te avisan si estás entrando a un sitio reportado como peligroso".

Detrás de la huella digital

¿Qué pasa cuando alguien cae en una de esas estafas? Generalmente, cuando se realizan operaciones no consentidas, los bancos, aerolíneas o tarjetas de crédito tienen la política de asumir los costos. Por este motivo, los usuarios no suelen llegar a la instancia de llevar la denuncia a la justicia. Y no hay estadísticas oficiales recientes sobre la incidencia de esta práctica en la Argentina, según explicó Azzolin.



De todas maneras, en muchos casos se activan las investigaciones judiciales: "Lo que hacemos es rastrear la operación. Por más recursos que haya para que la actividad en

Internet sea anónima, la compra de bienes y servicios siempre deja alguna marca y nosotros tratamos de encontrarla", señaló el fiscal encargado de delitos informáticos.

Los trucos más utilizados por los estafadores

Las actualizaciones tecnológicas dan oportunidades a los piratas del ciberespacio

Alguien te observa

La conexión a redes inalámbricas abiertas puede tener sus riesgos. Los especialistas en seguridad informática aconsejan evitar el uso de Wi-Fi públicos en bares o aeropuertos a menos que sea urgente la necesidad de navegar en la red. Es que un pirata online podría facilitar ese acceso para capturar datos, en el sistema conocido como "hombre en el medio"

Compras seguras

El comercio electrónico crece día a día, pero presenta desafíos a la seguridad digital que obligan a tomar algunas precauciones. Para los expertos en ciberdelitos es de vital importancia chequear que el sitio en el que se realiza la adquisición online tenga el protocolo https, ya que esa particularidad confirma que se trata de una operación con datos encriptados

Pesca de incautos

Aunque fuese una de las primeras trampas conocidas en la red, mantiene su vigencia el sistema de solicitar por mail que la propia víctima complete formularios con sus datos sensibles. Para conseguirlo, los piratas informáticos logran simular incluso las páginas oficiales de bancos, por ejemplo. Esa técnica de captura de información se extendió a las redes sociales

Celular en riesgo

Una de las nuevas modalidades empleadas por los estafadores en la red apunta a las aplicaciones que se bajan en el celular. Es una trampa informática que está en ascenso. Y los expertos en ciberdelitos estiman que la mejor manera de evitar esa nueva amenaza es descargar las apps directamente desde plataformas oficiales, como Google Play y Apps Store

Lucila Pinto
LA NACION 18 DE MARZO DE 2017
http://www.lanacion.com.ar/1995020-ciberdelito-claves-para-no-caer-en-los-nuevos-enganos