# LOS CIBERPELIGROS DEL 2017: NUEVOS… O PEOR, ¡REFORZADOS!

Claves para que “no dé papaya” frente a los sofisticados métodos de los ladrones en línea.

Ejecutivos, empleados, estudiantes, amas de casa… Nadie está exento de las amenazas que hay hoy en la red. ¿Sabía, por ejemplo, que tres de cada cuatro páginas web lo ponen en situación de riesgo?

Los datos del más reciente reporte de amenazas de Symantec (año 2016) son elocuentes. En el 2015 hubo un millón de ataques por día, el ‘phishing’ o captura de datos personales a través de webs y correos falsos creció un 55 por ciento, el secuestro de datos aumentó un 35 por ciento (y ya se extendió a los celulares) y casi 500 millones de identidades fueron robadas y expuestas públicamente.

Probablemente usted ya habrá escuchado que no debe creer en correos que le advierten que su cuenta bancaria será cerrada de inmediato, si no se conecta al banco a través de un enlace que viene en el mismo correo y que lo llevará directo a los ciberatracadores; o que no debe abrir correos de desconocidos, por provocativo o preocupante que resulte el asunto del mensaje (el anzuelo), ya que dentro del mismo seguramente habrá alguna sorpresa desagradable: desde un programa que ‘esclavizará’ su computador, hasta uno que le secuestre todos sus datos (encriptándolos), y frente a lo cual solo tendrá dos opciones, pagar o resignarse a perderlos.

La verdad es que son trampas muy viejas, aunque mucha gente siga cayendo en ellas por ingenuidad, ignorancia o, sencillamente, indolencia. Según cifras del Banco Interamericano de Desarrollo, el cibercrimen le cuesta al mundo cerca 575.000 millones de dólares al año, lo que representa 0,5 por ciento del Producto Interno Bruto (PIB) global. Solo en América Latina y el Caribe los delitos digitales cuestan alrededor de 90.000 millones de dólares al año, recursos con los cuales se podría cuadruplicar el número de investigadores científicos de la región.

El tema es que el cibercrimen se sofistica minuto a minuto y sus tentáculos son cada vez más poderosos. Cinco formas nuevas o repotencializadas de este problema y cómo evitarlas, para que usted no sea la próxima víctima.

1. Aplicaciones ‘trampa’: ¿Busca una ‘app’ y bajo el mismo nombre aparecen cinco? Si descarga la equivocada es posible que esta llegue incluso a secuestrar de manera virtual su celular y/o hacer operaciones con las cuentas que allí tiene. Obtener la ‘app’ desde PlayStore o AppStore ayuda a aminorar el riesgo, así como elegir la que tenga un mayor número de descargas, un programador con referencias en internet y múltiples reseñas positivas. Sin embargo, aun así es posible que el engaño pase inadvertido, y es ahí en donde es recomendable no compartir datos personales ni financieros a través de aplicaciones. Si requiere hacer una transacción, recurra a plataformas de pago seguras, como PayPal.

2. El ‘phishing’ viene recargado: Es posible que ya sepa reconocer algunos correos que en realidad no son de su banco ni de su tienda favorita, y que le solicitan ingresar datos confidenciales. Aun así, ¡cuidado! Los defraudadores son cada vez más sofisticados y específicos. Una tendencia en crecimiento es el ‘spear phishing’, es decir, el envío de correos falsos que parecen relacionados al trabajo, a clientes o al área legal, de finanzas o de recursos humanos de su empresa, para el robo de identidad o corporativo.

La única forma de prevenir cualquier tipo de ‘phishing’, además de navegar en redes seguras y privadas, es estar en alerta permanente. Si le solicitan información sensible: usuario, contraseñas, nombre, número de seguridad social o tarjetas bancarias, contacte directamente a la organización respectiva para confirmar que la solicitud sea real. No haga clic en los enlaces (‘links’) del correo ni marque a los teléfonos que ahí le proporcionan. Busque la página web que inicie con https directamente, contacte al ‘call center’ oficial… pregunte, investigue, desconfíe.

3. Centros de servicio falsos: Una de las más ingeniosas y maliciosas caras de los ciberataques son los centros de ayuda, soporte y asistencia falsos. El usuario recibe mensajes –y hasta llamadas– de supuestos centros de atención al cliente que le piden comunicarse con un número para corregir ciertos problemas de su equipo o mejorar su 'software' o servicio. Esta es la puerta de entrada a ladrones de datos. Cuando tenga que acudir a un servicio, busque la página oficial y el teléfono oficial de su proveedor, cualquiera que sea el servicio. Un dato: en el 2015, Symantec bloqueó 100 millones de estos ataques.

4. El secuestro del 'Like': En el 2015, eMarketer estimó que el 93 por ciento de los usuarios de redes sociales en América Latina están conectados a Facebook. Los ciberdelincuentes aprovechan este factor para difundir códigos maliciosos a través de páginas web publicadas en dicha red social, con contenido llamativo o morboso. Una vez que un usuario abre estos sitios –y aunque luego los cierre–, el enlace se publica automáticamente sin su consentimiento en su historial, incluso con su propio 'Like'.

Si ha sido víctima, lo primero que debe hacer es evitar la propagación: elimine el post y avise a sus amigos que hagan caso omiso del mismo. Luego, use un programa antivirus para revisar que ningún 'malware' (virus) haya quedado instalado. Y en el futuro, considere que si las publicaciones son demasiado sensacionalistas, pueden representar un riesgo de 'hackeo'.

5. ¿Wifi gratis? Desconfíe: Ciertamente no es totalmente falso, pues en efecto usted se puede conectar y navegar por internet a través de él. Usualmente está disponible en lugares públicos y parece una inocente red inalámbrica de cafeterías o centros comerciales. En realidad las redes de wifi fueron colocadas por algún cibercriminal para ver todo lo que realicen quienes se conecten en ese momento, robarles información e incluso insertarles un bot (programa malicioso), para posteriormente manejar sus equipos a distancia.

La mejor solución es no conectarse a redes públicas, a menos que tenga la plena certeza de que pertenecen a un proveedor legítimo. Si decide tomar el riesgo, lo mejor es usar una red privada VPN. Funciona como si usted se colocara un traje protector para bucear en internet. Otras medidas incluyen instalar un buen 'firewall' en su computador o evitar ingresar contraseñas y datos bancarios durante la navegación.

6. El internet de las cosas, en la mira: En el 2016 había por lo menos 6.400 millones de objetos conectados a internet. Relojes, electrodomésticos, cámaras, televisores e incluso hogares en sí mismos. Esa cifra va a crecer exponencialmente, y se sabe que los ataques hacia este tipo de dispositivos se dispararán.

Se los llama 'jackware', una forma especializada de secuestro digital. ¿Cómo opera? Un código malicioso bloquea su automóvil, la alarma de su casa o la calefacción de todo un edificio en pleno invierno, y el ciberdelincuente exige un pago a cambio de liberarlos.

## ACTIVIDAD PARA RESPONDER

1. Identifique al menos 7 palabras desconocidas y consulte el significado

2. ¿Cuál considera que es el mayor riesgo que puede tener una persona que ha sido víctima del robo de información? Explique

3. ¿Cuál considera que es la mejor manera de evitar ser víctima del robo de información personal? Explique.

4. resumen, lo más importante de la lectura mínimo 7 renglones.