BOLETÍN INSTITUCIONAL
INSTITUTO NACIONAL DE SALUD

SEGURIDAD DE LA INFORMACIÓN:

¿Cómo proteger los datos personales?

Jaime Barrantes Centurión[1], Jenny Sánchez Silva[1], Sonia Gutiérrez Garcia[1]

Resumen

Reducir el riesgo de padecer un robo de identidad es posible protegiendo la información de la persona. Existen cuatro formas de hacerlo: saber con quién estamos compartiendo información; guardar y eliminar información de manera segura; hacer preguntas antes de decidir compartir información personal; y disponer de un nivel de seguridad adecuado en computadoras y aparatos electrónicos.

En la actualidad el uso de la informática, es algo indispensable con la rutina de la vida moderna, hoy en día todo trabajo tiene que ver con las aplicaciones informáticas o se utiliza el acceso a Internet para interrelacionarse entre las personas, bien de forma privada, como pública.

El número de ciberataques cada vez es mayor y más aún en periodos vacacionales. Los delincuentes aprovechan las malas prácticas que realizan los usuarios para causar el mayor daño posible.

Palabras Claves: Phishing, smishing, malware, Ingeniera Social.

Introducción

Sin ninguna duda, Internet es una herramienta muy importante porque permite obtener conocimientos instantáneos y una gran cantidad de ventajas, superiores a las que han existido en diversas épocas de la historia, pero al mismo tiempo es cierto que existen riesgos, principalmente, en privacidad que debemos tratar de controlar en el mundo digital. Existe un incremento considerable en la cantidad de hackers al acecho de personas desprevenidas, por ello es necesario cuidar nuestros datos porque los estafadores usan métodos de ingeniería social para robar las contraseñas sin que una persona se dé cuenta. Los correos electrónicos que aparentan ser legítimos (phishing), los mensajes de texto (smishing), las llamadas telefónicas falsas son las técnicas más usadas para estafar y es importante prestar atención para no caer ante estas mentiras. El robo de datos informáticos, se producen como resultado de la falta de protección de dicha información.

¿Qué es el robo de identidad?

El robo de identidad sucede cuando otra persona obtiene o utiliza información personal de forma no autorizada. Esta acción la realiza con fines fraudulentos o para cometer algún otro delito.

[1] Oficina General de Información y Sistemas, Instituto Nacional de Salud (INS). Lima, Perú

Citar como: Barrantes-Centurion J, Sánchez-Silva J, Gutiérrez-García S. Seguridad de la información: ¿Cómo proteger los datos personales? Bol Inst Nac Salud. 2020;26(3-4):45-51.

A través del robo de identidad se obtiene información personal como contraseñas, número de tarjetas de crédito, números de identificación, datos registrados con el objetivo de cometer fraudes suplantando a la víctima. Así mismo, esta información puede ser robada con intenciones ilegales, como para solicitar préstamos, hacer compras en línea o disponer de los recursos financieros.

¿Cómo se ejecuta el robo de identidad?

El robo de identidad tiene mucha relación con el phishing y otras técnicas de ingeniería social que frecuentemente se utilizan para conseguir información reservada de la víctima. Algunos de estos actos han sido reportados en algunas plataformas virtuales conocidas, como whatsApp, mensajes de texto, correos electrónicos, etc.

Algunas fuentes para adquirir la información y permitir a los criminales suplantar a sus víctimas pueden ser los perfiles públicos en redes sociales u otros servicios online.

La sobreexposición de información privada no se limita exclusivamente a las redes sociales. Sitios como Google Docs o Dropbox no son los mejores lugares para almacenar datos privados como contraseñas o documentos. En el caso de utilizar estas páginas para guardar información privada, esta debe ser almacenada en un archivo cifrado.

Tenemos algunos casos conocidos de phishing en plataformas virtuales:

Correos electrónicos

Haciendo uso de la ingeniería social, los ciberdelincuentes envían mensajes de correo para que los usuarios sean conducidos a exponer información mediante la descarga de un archivo adjunto o una página web fraudulenta. Los archivos adjuntos maliciosos pueden ser múltiples y variados, desde ejecutables que instalen malware en tu equipo hasta hojas de cálculo (Excel) que requieran de la ejecución de macros para liberar el código malicioso. Mecanismo similar al de la navegación en páginas fraudulentas.

Otro método que es frecuente, tiene relación con el envío de correos electrónicos falsos que suplantan la identidad de los bancos o conocidas empresas para captar la atención y seguridad de los usuarios, con la única intención de obtener información confidencial de la persona. El correo electrónico fraude puede consistir en una solicitud falsa de la cuenta de un cliente o también un enlace que lo direcciona a un sitio web falso que será idéntico al sitio web verdadero de dicha empresa, una vez en la página se le pedirá que coloque información personal (por ejemplo, contraseñas, datos de su tarjeta de crédito, etc.). Los correos electrónicos fraudulentos también pueden ocultarse a través de archivos que podrían contener virus.

Para evitar estos robos se debe tener en cuenta:

- La información del remitente (¿Conoces al remitente?; en caso de ser así, ¿su dirección de correo es la que utiliza normalmente? y ¿está correctamente escrito su nombre?),
- El cuerpo del mensaje (faltas de ortografía, vocabulario poco corriente, etc.),
- Los archivos adjuntos (¿reconoces el nombre del archivo adjunto?, ¿se trata de un archivo ejecutable?), y los enlaces.

El phishing es otra manera de fraude más frecuente de realizar a través de Internet. Por tanto, es importante estar atento a las cuentas habilitadas, así como a las contraseñas, y tener precaución ante una contraseña que genere algún error sospechoso. Los hackers suelen predecir sus acciones, pero… ¡más vale prevenir, que curar!

Redes Sociales

Realizar publicaciones en redes sociales, mucho más allá de lo necesario, no tener el cuidado respectivo a la hora de conectarse a una red o descuidar la confidencialidad de los datos a la hora de hacer una transacción puede ser la oportunidad de ataque de los ciberdelincuentes.

El uso de medios virtuales se ha convertido en la principal herramienta tanto para comunicación, como para la obtención de información. El empleo de estos medios puede llegar a ser perjudicial para el usuario por la posibilidad del robo de datos o de información introducida en algunas páginas web.

Por ello:

- Mantener los perfiles de redes sociales privados.
- No compartir la información personal mediante teléfono, dirección o lugar de trabajo.
- Aceptar solicitudes de amistad de personas que se conoce.

- Revisar que los contactos no sean perfiles falsos.
- Cambiar inmediatamente la clave de seguridad ante la sospecha del ingreso a su perfil o cuenta.
- Personalizar las opciones de seguridad del perfil, a fin de valorar quien y a que información acceder.
- Organizar los contactos para la configuración de la privacidad por grupos.

Al seguir estas recomendaciones de seguridad los datos se encontrarán protegidos contra ataques cibernautas y se tendrá pleno control de los activos digitales.

WhatsApp

Dentro de la plataforma de whatsapp, se ha evidenciado phishing mediante mensajes que resaltan un código y un enlace, por los que al ingresar a estos el usuario aprueba la usurpación de identidad. Según informa la Organización de Consumidores y Usuarios (OCU) de España, el mensaje que se recibe cuando una persona usurpa la identidad es un código de verificación que llega "cada vez que se configura la aplicación en un terminal nuevo para vincular la aplicación a tu número de teléfono", lo que significa que alguien comunica a WhatsApp que "cambias de número" y que se solicita trasladar los datos a un nuevo smartphone.

Así mismo se han reportado otras modalidades de phishing, como el uso de campañas virtuales de marcas conocidas, que para acceder a las promociones y descuentos es necesario realizar una encuesta que incluye datos personales.

Mensajes de texto

Los mensajes de texto fraudulentos o smishing (de SMiShing; a su vez, de SMS y fishing); son una nueva modalidad de robo electrónico a base de técnicas de ingeniería social con SMS dirigidos a los usuarios de telefonía móvil. Estas estafas se materializan cuando el usuario recibe un mensaje de texto del ciberdelincuente, quien suplanta la identidad del banco, con el fin que el usuario haga clic o acceda al enlace enviado mediante el cual le sugiere compartir sus datos personales y financieros en una página web falsa.

Otro tipo de estafa por medio de mensajes SMS, es cuando se solicitan datos o se pide llamar a un número o entrar a una web. El sistema emisor de estos mensajes de texto, intentará suplantar la identidad de alguna persona conocida del grupo de contactos, o incluso a una empresa de confianza.

¿Cómo protegerte del robo de identidad?

a. Para los usuarios

- De preferencia usar internet del hogar, empresa o datos móviles.
- Proteger la laptop, equipo móvil o Tablet del software malicioso usando un antivirus de paga (no gratuita ya que tienen limitaciones).
- Mantenerse alejado de sitios Web y mensajes sospechosos.
- Crear contraseñas fuertes que sean largas, complicadas y no predecibles. Evitando el uso de contraseñas simples y conocidas, como las que se mencionan a continuación: 12345, 123456, 123456789, etc.
- Monitorizar las cuentas bancarias y de crédito
- Si se desea destruir documentos que contienen información personal sensible o privada, debe realizarlo de manera segura (destruyéndolos hasta que se vuelvan irrecuperables).
- No compartir información confidencial que podría ser utilizada de manera indebida para la suplantación.

En caso de correos electrónicos

- Habilitar la opción del sistema operativo que permita ver las extensiones de los archivos. De esta manera, se podrá comprobar si se trata de un ejecutable, un documento de texto, javascript, etc.
- Deshabilitar las macros de Microsoft Office y tener cuidado con aquellos archivos que pidan su habilitación.
- Si se sospecha de algún enlace que venga incluido en el correo, analizar el link.
- Recordar mantener el sistema operativo con antivirus y aplicaciones actualizadas a su última versión. Instalar y configurar algún tipo de filtro antispam y desactivar la vista de correos en HTML de las cuentas que se consideren críticas.

b. Para las plataformas virtuales

- Así mismo, las plataformas o sistemas de información pueden implementar el uso del doble factor de autenticación por cada uno de ellos y por cada cuenta de usuario. Esta estrategia ha sido considerada efectiva para evitar la usurpación de identidad digital, según lo mencionado por Google.

Conclusiones

Teniendo en cuenta lo detallado en el presente artículo se aprecia que existe diversidad de formas y maneras de ataques a través de internet que, en muchos casos, buscan robar información personal en beneficio del delincuente.

Es necesario proteger y salvaguardar la información personal con la finalidad de evitar que un atacante pueda suplantar su identidad. Los daños y perjuicios causados, debido al robo de identidad no se centra únicamente a temas financieros, éste puede tener un gran impacto tanto en el aspecto personal y sentimental de la víctima.

Es necesario supervisar a los niños cuando estén usando la computadora y el acceso a internet, teniendo en cuenta que en la actualidad se han visto obligados a utilizar salas virtuales y servicios de internet para poder continuar con sus clases.

Referencias

1. ¡Cuidado! Estafa en WhatsApp podría robar tu cuenta y acceder a todos tus datos [Internet]. El Comercio. 2019 [actualizado el 12 de diciembre de 2019; citado 17 abril 2020]. Disponible en: https://elcomercio.pe/tecnologia/whatsapp-estafa-podria-robar-tu-cuenta-y-tener-acceso-a-todos-tus-datos-personales-phishing-noticia/?ref=ecr
2. Robo de identidad [Internet]. ESET. 2019 [citado 17 abril 2020]. Disponible en: https://www.eset.com/es/caracteristicas/robo-de-identidad/
3. Lubeck L. Circula engaño por WhatsApp anunciando que Adidas está regalando zapatos y camisetas [Internet]. We Live Security. 2019 [citado 17 abril 2020]. Disponible en: https://www.welivesecurity.com/la-es/2019/12/18/circula-engano-por-whatsapp-anunciando-que-adidas-esta-regalando-zapatos-y-camisetas/
4. Cómo evitar incidentes relacionados a los archivos adjuntos al correo [Internet]. Instituto Nacional de Ciberseguridad. 2020 [citado 17 abril 2019]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/evitar-incidentes-relacionados-los-archivos-adjuntos-al-correo

5. Amenazas por correo electrónico, ¿qué hacer? [Internet]. Beyond. 2019 [citado 17 abril 2020]. Disponible en: http://www.beyondservicios.com.ar/amenazas-por-correo-electronico/
6. Tomáš F. Las peores contraseñas del 2019: ¿utilizas alguna de la lista? [Internet]. We Live Security. 2019 [citado 17 abril 2020]. Disponible en: https://www.welivesecurity.com/la-es/2019/12/17/peores-contrasenas-2019/
7. Juan Manuel H. Doble factor de autenticación: la solución más efectiva para prevenir el secuestro de cuentas [Internet]. We Live Security. 2019 [citado 17 abril 2020]. Disponible en: https://www.welivesecurity.com/la-es/2019/05/21/doble-factor-autenticacion-solucion-seguridad-mas-efectiva/
8. ¡Cuidado! Estafa en WhatsApp podría robar tu cuenta y acceder a todos tus datos personales [Internet]. El Comercio. 2020 [actualizado el 12 de diciembre de 2019; citado 12 diciembre 2019]. Disponible en: https://elcomercio.pe/tecnologia/whatsapp-estafa-podria-robar-tu-cuenta-y-tener-acceso-a-todos-tus-datos-personales-phishing-noticia/
9. Robo de datos informáticos y protección criptográfica [Internet]. Tu abogado defensor. 2020 [citado 28 mayo 2020]. Disponible en: https://www.tuabogadodefensor.com/proteccion-criptografica-datos/
10. Ignacio C. Cómo evitar el robo de información privada a través de Internet [Internet]. El Economista. 2019 [citado 28 mayo 2020]. Disponible en: https://www.eleconomista.es/gestion-empresarial/noticias/10040712/08/19/Como-evitar-el-robo-de-informacion-privada-a-traves-de-Internet.html
11. Gabriela C. Claves para detectar mensajes de texto falsos [Internet]. BBVA. 2019 [citado 28 mayo 2020]. Disponible en: https://www.bbva.com/es/claves-para-detectar-mensajes-de-texto-falsos/