Consejos para la protección del robo de identidad en Internet

El phishing es una técnica fraudulenta que se utiliza para obtener información confidencial y financiera de las personas, como nombres de usuario, contraseñas y números de tarjetas de crédito. Los delincuentes que practican el phishing envían correos electrónicos o mensajes de texto aparentemente legítimos que representan ser de una empresa de confianza, como un banco o un sitio web de comercio electrónico. Estos correos electrónicos pueden incluir enlaces a sitios web falsos que parecen ser legítimos y que piden a la persona que ingrese información personal y financiera.

El phishing es una amenaza muy seria para la seguridad de la información y el dinero de las personas. Cada año, millones de personas son víctimas de este tipo de fraude y pierden grandes cantidades de dinero. Por esta razón, es importante que todos estemos informados sobre el phishing y sepamos cómo

protegernos de él.

El phishing es una forma sofisticada de engaño que puede ser difícil de detectar. Los delincuentes que practican el phishing utilizan técnicas muy avanzadas para hacer que sus correos electrónicos y mensajes de texto parezcan legítimos. Esto incluye el uso de logotipos y marcas registradas de empresas reales, así como la creación de sitios web falsos que parecen ser legítimos.

Para protegerse del phishing, es importante que las personas sean conscientes de los peligros y aprendan a reconocer los correos electrónicos y mensajes de texto fraudulentos. Es importante no hacer clic en enlaces desconocidos o sospechosos y no proporcionar información personal y financiera a sitios web no confiables. También es una buena idea utilizar software de seguridad en línea y tener contraseñas seguras y únicas para cada cuenta en línea.

Además, es importante estar atento a los mensajes de alerta y avisos de seguridad de los bancos y otras instituciones financieras. Estos mensajes pueden proporcionar información valiosa sobre las últimas técnicas de phishing y cómo protegerse de ellas.

En resumen, el phishing es una amenaza muy real para la seguridad de la información y el dinero de las personas. Para protegernos del phishing, es importante estar informados sobre este fraude, reconocer los correos electrónicos y mensajes de texto fraudulentos y tomar medidas para proteger nuestra información.

Por lo tanto, es importante estar informado y alerta sobre las técnicas de phishing que se utilizan y tomar medidas para protegerse contra ellas. Mantener contraseñas seguras, verificar la autenticidad de los correos electrónicos y no proporcionar información personal o financiera a nadie que la pida sin verificar antes su identidad son algunas de las

medidas que puedes tomar para prevenir ser víctima de phishing. Además, es importante mantener actualizados los programas de seguridad en tu computadora y dispositivos móviles para proteger tus datos. Con estos cuidados, podrás disfrutar de una experiencia en línea más segura y protegida contra el phishing.

Consejos para no ser víctima del robo de información en Internet

Es cualquier época del año comenzamos a recibir correos electrónicos que quieren robar nuestros datos y contraseñas de acceso a redes sociales o peor aún, de nuestras cuentas bancarias. Ya los debes conocer, aquellos emails con los famosos asuntos como: «Su cuenta está a punto de ser cerrada», «Hay un bloqueo en su cuenta», «¿Podría ayudarme a reclamar mis fondos?» o mi favorito de todos los tiempos «Felicidades, has ganado la lotería del Reino Unido».

En las épocas de comprar regalos para la familia, clientes o empleados y lo último que necesitamos es que nuestra cuenta de banco o tarjeta de crédito se vea obstaculizada. Eso es exactamente lo que están esperando estos «estafadores cibernéticos», y desafortunadamente, algunos de nosotros estamos tentados a seguir las instrucciones enviadas para investigar.

En primer lugar, **¡NO SIGAS LAS INSTRUCCIONES EN EL CORREO ELECTRÓNICO!** Si crees que puede haber un problema, accede a la cuenta en cuestión como lo haces normalmente en tu PC y no con el enlace proporcionado en el correo falso.

He recibido algunos correos electrónicos que parecen muy auténticos supuestamente de bancos, que incluso copiaron los colores del logo del banco y el estilo de papelería. Pero, no caigas en la estafa. De hecho, ni siquiera abras el correo electrónico, ya que muchos están diseñados para liberar un

programa de virus en tu computadora solo con ser abiertos. Simplemente, reenvía el correo electrónico sospechoso a la dirección de «correo electrónico engañoso» proporcionada por tu banco o compañía de tarjetas de crédito.

Casi 10 millones de personas en el mundo se convirtieron en víctimas del robo de identidad el año pasado, costando a las empresas y a las personas miles de millones de dólares. Aquí hay algunos otros consejos para ayudarte:

1. Entender los peligros de las tarjetas de débito: mayor responsabilidad que las tarjetas de crédito. Cuando se trata de fraude, las tarjetas de débito tienen una responsabilidad personal mucho mayor que las tarjetas de crédito, dependiendo de cuánto tiempo informes la pérdida de la tarjeta. Si no informas el uso no autorizado dentro de los 60 días de recibir tus estados de cuenta bancarios, podrías perder todo el dinero.
2. Comprende los peligros de las tarjetas de débito: mayor responsabilidad que las tarjetas de crédito. En cuanto a fraude, las tarjetas de débito conllevan una responsabilidad personal mucho mayor que las tarjetas de crédito, dependiendo de cuán rápido informe la pérdida de la tarjeta. Si no informa el uso no autorizado dentro de los 60 días después de recibir sus estados de cuenta bancarios, podría perder todo el dinero en la cuenta y ser responsable de la cantidad de dinero que se haya retirado de su línea de crédito.
3. Reevaluar el escribir cheques: Ese pequeño trozo de papel contiene demasiada información. Algunos expertos aconsejan contra el escribir cheques porque brindan tu dirección, número de cuenta bancaria, firma y número de licencia a extraños completos. Además, no hay legislación federal para limitar tu responsabilidad por cheques falsificados (cada estado tiene su propio conjunto de reglas). Los expertos aconsejan que investigues la automatización de tus pagos de facturas.

4. Protege tu correo: Tu buzón es una mina de oro de información. Entre los estados de cuenta bancarios, las facturas y todas esas ofertas de tarjetas de crédito pre-aprobadas, tu buzón está lleno de datos personales que los ladrones de identidad pueden utilizar para solicitar fácilmente una tarjeta de crédito en tu nombre. A menos que verifiques cuidadosamente tu informe de crédito, es posible que nunca lo sepas. Una forma de evitar esto es tener tu buzón bajo llave, pero la mayoría de nosotros en Santa Clarita tenemos nuestros buzones en la acera frente a nuestra casa y el cartero no aprueba cargar docenas y docenas de llaves. La otra solución es tener un buzón de correo alquilado o desalentar a los ladrones que buscan en los basureros comprando una trituradora y destruyendo los documentos antes de desecharlos.
5. Sé lo más virtual posible: Para comprar en línea, existen números de tarjeta «virtuales». Estos son números de tarjeta de crédito generados aleatoriamente que son desechables y que los compradores en línea utilizan una vez y luego descartan. Está directamente vinculado a tu cuenta real de tarjeta de crédito, por lo que las compras aparecen en tu factura mensual. El servicio es fácil de usar y ¡es GRATIS! Todo lo que necesitas hacer es registrarte con las compañías que ofrecen la tarjeta virtual, como MBNA, Discover y Citigroup.
6. Crea un kit de emergencia de identidad: ¿Sabrías cómo contactar a tu compañía de tarjeta de crédito en una emergencia? Crea un kit de emergencia que contenga: el número de cuenta, la fecha de vencimiento, el nombre de la compañía emisora y el número de contacto de emergencia para cada tarjeta que poseas. Mientras lo haces, haz copias de tu licencia de conducir, tarjeta de seguridad social, certificado de nacimiento y pasaporte y guárdalos en una caja con candado o un archivador, o en una caja de seguridad. Me gusta la caja de seguridad

mejor, porque esto te brinda protección en caso de una catástrofe como incendios, terremotos, etc.

Todo esto puede parecer mucho trabajo y sobre todo innecesario, pero si eres víctima de robo de identidad, incluso solo una vez, te darás cuenta de que vale la pena el esfuerzo.

Además, es importante recordar que si no fuera por lo que llevamos en nuestras billeteras o carteras, todos seríamos John y Jane Doe (personajes genéricos) si no podemos hablar debido a una lesión o si no estamos acompañados por alguien que nos conozca. ¿Cuánto menos estresante sería saber que en una caja de seguridad bancaria, sin importar dónde estés, hay elementos que pueden verificar tu identidad? ¡Más vale prevenir que lamentar!