



Phishing, Vishing, Smishing...

Phishing

“¡Urgente! Su cuenta ha sido suspendida. Por favor, visite este enlace para actualizar su información y reinstalar su cuenta”. ¿Alguna vez ha recibido un correo electrónico como este, de una compañía con quién nunca ha tenido una cuenta? Si es así, usted ha sido el blanco de una estafa de phishing.

No haga clic en ningún enlace de un correo electrónico que huelga mal.

El término “phishing” fue acuñado intencionalmente como un juego de “pesca”. Pescar es exactamente lo que están haciendo los estafadores – lanzándole una carnada engañosa para ver si pica y da su información personal. Una vez que lo tengan, los estafadores pueden hacer cargos no autorizados en su cuenta bancaria o tarjeta de crédito, o incluso abrir cuentas fraudulentas en su nombre.

Los estafadores de Internet son bien conocidos por los envíos masivos de correos electrónicos (spam) o mensajes emergentes de Internet que parecen ser de un amigo o de una empresa u organización con la que usted hace tratos – tal como un banco, compañía de tarjeta de crédito, o hasta una agencia gubernamental. El mensaje puede pedirle que “actualice”, “valide” o “confirme” su cuenta. Algunos mensajes de correo electrónico de phishing amenazan con graves consecuencias si usted no responde. El mensaje le pedirá que haga clic en un enlace o llame a un número telefónico. Es muy fácil para los estafadores obtener logotipos o imágenes de Internet y recrearlos para que se vean y se sientan muy legítimos o familiares. Aunque parezcan tan reales como los sitios web, no son legítimos.

Enlaces maliciosos

No haga clic en ningún enlace de un correo electrónico que huelga mal – los estafadores pueden mostrar la dirección de un sitio web real de la compañía que fingen ser en un enlace al mismo tiempo que le envían a un sitio web falso. Abra un nuevo navegador y escriba una



dirección de web que usted sepa que es correcta, o llame a la organización que está usando el número telefónico publicado en un directorio. Como muchos consumidores han comenzado a darse cuenta de las estafas estándares, los estafadores se han vuelto más sofisticados.

Un enlace o anexo puede hacer que software malicioso, conocido como “malware”, se instale en su computadora. El malware podría permitir que un estafador acceda a sus archivos personales, registre las pulsaciones del teclado para capturar sus contraseñas y números de cuentas, e incluso tome el control de su computadora para enviar correos electrónicos de phishing a otros.

Impostores cibernéticos

Los estafadores hasta pueden usar su identidad para estafar a alguien que usted conoce. Si los estafadores son capaces de acceder a su correo electrónico o cuentas de redes sociales, ellos pueden ponerse en contacto con amigos y familiares mientras se hacen pasar por usted. Los estafadores cambiarán su contraseña inmediatamente al acceder a su cuenta, de tal modo que le impiden entrar a su cuenta y le dejan fuera cortándole de todos sus contactos.

Ellos pueden después enviar mensajes urgentes a todos sus contactos, diciéndoles que usted ha tenido

problemas, se encuentra perdido en el extranjero y necesita que le envíen dinero a la mayor brevedad posible. Para cuando puede correr la voz de que usted está bien, un amigo o familiar con buenas intenciones ya le ha enviado el dinero al extranjero. Además, muchos de los virus de computadoras se propagan a través de listas comprometidas de correos electrónicos. Un remitente familiar en un correo electrónico no es garantía de fiabilidad.

Spoofting (suplantación de identidad)

El spoofing (suplantación de identidad) ocurre comúnmente cuando los estafadores utilizan dispositivos electrónicos para disfrazar sus verdaderas identidades o para ocultar el origen de sus mensajes, mientras hacen phishing. En otras palabras, el estafador publica un nombre o número en su correo electrónico, identificador de llamadas telefónicas, mensaje de texto o dirección URL de Internet diciendo ser una persona o empresa que usted conoce y en la que confía. No se deje engañar. El estafador detrás de la identificación falsa podría estar en otro estado o país usando nombres y títulos falsos que son imposibles de rastrear.

Vishing & Smishing

Después de que los consumidores comenzaron a darse cuenta de las estafas a través de correos electrónicos, los estafadores encontraron un nuevo método de atraer víctimas por teléfono: vishing. El **vishing** es muy similar al phishing, pero los estafadores utilizan las llamadas telefónicas (ya sea en vivo o “robocalls” pregrabadas) en lugar de correos electrónicos para tratar de atraer a la gente a que den su información personal. Los vishers (estafadores) a menudo se hacen pasar por un banco local, cooperativa de crédito o cualquier otro negocio legítimo en el que usted podría estar inclinado a confiar o patrocinar.

Ya que los estafadores pueden suplantar cualquier nombre o número telefónico que deseen, el estafador puede fácilmente mostrar en su identificador de llamadas el nombre de una empresa familiar o de confianza. Por ejemplo, un mensaje grabado afirma que la cuenta bancaria de un consumidor se ha visto comprometida. Cuando el consumidor regresa la llamada, habla con una persona en vivo haciéndose pasar como empleado del banco, quien convence al consumidor que la única manera de proteger la información preciosa de la cuenta bancaria de los

criminales es dando al “empleado del banco” sus datos personales.

Si alguna vez recibe una llamada de vishing de alguien que dice ser un empleado de un banco, una compañía de tarjeta de crédito, o cualquier otra empresa – cuelgue. Llame inmediatamente a la empresa real para reportar el incidente. Asegúrese de llamar utilizando solamente un número telefónico fiable obtenido de su guía telefónica local o de sus documentos con esa empresa.

Cuando en la estafa se usan mensajes de texto en lugar de llamadas telefónicas o correo electrónico, la técnica de la estafa se conoce como **smishing**. Por lo general, los mensajes de textos smishing provienen de un número “50000” en lugar de mostrar un número telefónico normal. Esto indica que el mensaje fue enviado de una dirección de correo electrónico, y no de un teléfono existente.

Al igual que con las estafas de phishing y vishing, **usted no debe responder** a un mensaje de texto smishing. Si parece ser un mensaje de su banco u otra empresa con la cual usted está familiarizado, contáctese usando un número telefónico fiable de su guía de teléfono local o de sus documentos con esa empresa.

Si usted recibe un correo electrónico de phishing, pregúntese:

1. **¿Alguna vez he hecho negocios con esta compañía?** Si la respuesta es sí, siga siendo cauteloso antes de hacer clic en algún enlace. Si no, no haga clic en ningún enlace y borre el correo electrónico.
2. **¿Existe algún anexo con el correo electrónico?** Si la respuesta es sí, no haga clic en ellos. Si usted cree que el correo electrónico y el anexo son legítimos, contacte al remitente primero para verificar el contenido y la seguridad del anexo.
3. **¿Pide el correo electrónico alguna información personal (como número de Seguridad Social, número de tarjeta de Medicare, fecha de nacimiento, números de tarjetas de crédito, números de cuentas bancarias, o contraseñas)?** Si es así, no responda. Borre el correo electrónico.
4. **¿Contiene el correo electrónico errores gramaticales y enunciados torpes?** Si es así, no

responda. Muchas veces los estafadores son de países extranjeros. Los errores gramaticales son una bandera roja que indican que el correo electrónico no es de una empresa profesional, acreditada y, lo más importante, legítima.

5. **¿Aún no está seguro de la legitimidad del correo electrónico?** Si usted todavía piensa que el correo electrónico puede ser de una compañía legítima con la cual usted ha hecho negocios (tal como su banco o una agencia gubernamental), busque el número telefónico de esa empresa o agencia. Use una guía de teléfono local fiable o use sus documentos con esa empresa (como un estado de cuenta bancaria o del dorso de una tarjeta de crédito o débito). Llame a la empresa o agencia directamente y pregúnteles si ellos le enviaron el correo electrónico.

Qué hacer si es víctima

Si usted cree que ha caído en un intento de una estafa de phishing, vishing o smishing, no se asuste. Hay medidas simples que usted puede tomar para proteger su información personal.

1. **Revise su informe de crédito anual gratuito con regularidad.** Obtenga su informe de crédito **GRATIS** cada año de cada una de las tres (3) agencias principales de informes de crédito. Verificar su informe regularmente es una de las mejores maneras de protegerse del robo de identidad. Le recomendamos que verifique un informe una vez cada cuatro (4) meses. Usted puede obtener su informe de crédito gratis de cualquiera de las tres (3) agencias – Equifax, Experian y TransUnion – llamando al 1-877-322-8228, o en línea en www.annualcreditreport.com. Revise su informe en busca de errores o posible fraude. Si encuentra algún error o posible fraude, contacte a la agencia de informes de crédito y discuta su reclamo. Nuestra oficina también puede ayudarle con este proceso.
2. **Coloque una alerta de fraude en su informe de crédito.** Una alerta de fraude es un servicio gratis que puede pedir a cada una de las tres agencias principales de informes de crédito. La alerta le deja saber a los acreedores potenciales que usted ha sido víctima de robo de identidad. Una alerta de fraude puede dificultar que alguien consiga crédito

en su nombre porque les dice a los acreedores que sigan ciertos procedimientos con el fin de protegerlo. Se mantiene en su informe por 90 días y puede ser renovado. Puede solicitar el alerta de fraude llamando a una de las tres agencias principales de informes de crédito, que notificará a las otras dos agencias principales de informes de crédito.

Equifax

1-800-685-1111

www.equifax.com

Experian

1-888-397-3742

www.experian.com

TransUnion

1-888-909-8872

www.transunion.com

3. **Coloque un congelamiento en sus informes de crédito.** Un congelamiento de seguridad prohibirá la divulgación de la información contenida en el informe de crédito sin expresa autorización. Los congelamientos están diseñados para prevenir extensiones de crédito aprobadas sin consentimiento, lo que impide que los ladrones de identidad abran nuevas cuentas a su nombre. Solicite el congelamiento de créditos gratuitamente contactándose con las agencias de informes de créditos antes mencionadas.
4. **Cierre todas las cuentas financieras que pudieran haber sido comprometidas.** Si usted ha dado un número de tarjeta de crédito o de cuenta de cheques, llame a su institución financiera y pida que le cierren sus cuentas y se las vuelvan a abrir bajo un número de cuenta nuevo. Pregúntele a su banco si puede colocar una contraseña en sus cuentas. Algunas instituciones pueden ofrecer supervisar su cuenta, pero le recomendamos sumamente que cierre la cuenta comprometida.

Si usted proporcionó el número de su licencia de conducir, contacte the Division of Motor Vehicles. Llámelos al (608) 264-7447 o búsquelos en línea:

www.dot.state.wi.us.

5. **Para ayudar a reducir las llamadas de telemarketing, inscribese en la Lista de No Llame**

de Wisconsin. Registre su número telefónico de casa o celular sin costo alguno al visitar www.donotcall.gov o llamando al 1-888-382-1222. Tiene que llamar desde el número de teléfono que quiere registrar. Los tele vendedores tienen hasta 31 días desde la fecha en que se registra para que paren de llamarle.

- 6. Si usted es víctima de robo de identidad, contáctese con nuestro Departamento de Protección al Consumidor.** Usted puede llamar al 1-800-422-7128 o mandarnos un correo electrónico a:

DATCPWisconsinPrivacy@wi.gov

Para más información, visite el sitio web:

www.datcp.wi.gov

Para más información o para presentar una queja visite nuestro sitio web o contáctese con:

Wisconsin Department of Agriculture, Trade and Consumer Protection

Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53708-8911

Correo electrónico: DATCPHotline@wi.gov

Sitio web: datcp.wi.gov

(800) 422-7128 TTY: (608) 224-5058