SEA CIBERNÉTICAMENTE INTELIGENTE
#CyberMonth

MES DE CONCIENTIZACIÓN SOBRE SEGURIDAD CIBERNÉTICA DE 2021: PONGA DE SU PARTE. #BECYBERSMART

PHISHING Y SPOOFING

Los ataques de phishing utilizan el correo electrónico o páginas web maliciosas para infectar su máquina con programas maliciosos y virus para recolectar su información personal y financiera. Los delincuentes cibernéticos tratan de engañar a los usuarios para que hagan clic en un enlace o abran un archivo adjunto que infecte sus computadoras y crea vulnerabilidades que los delincuentes pueden usar para atacar. Los correos electrónicos podrían parecer provenir de una institución financiera legítima, sitio de comercio electrónico, agencia gubernamental o cualquier otro servicio, negocio o persona. El correo electrónico también podría solicitar su información personal, por ejemplo, los números de sus cuentas, sus contraseñas o sus números de Seguro Social. Cuando los usuarios responden con la información o hacen clic en el enlace, los atacantes aprovechan para acceder a las cuentas de los usuarios.

Los ataques de spoofing usan direcciones de correo electrónico, nombres de remitentes, números de teléfono o direcciones de páginas web que se disfrazan de manera que parecen ser una fuente de confianza. Los delincuentes cibernéticos tratan de engañar a los usuarios al cambiar una letra, un símbolo o un número en el nombre. Esta táctica se utiliza para convencer a los usuarios de que estén comunicándose con una fuente conocida. Los delincuentes cibernéticos quieren que usted crea que estas comunicaciones "spoofed" son verdaderas para que descargue softwares maliciosos, envíe dinero o divulgue su información personal, financiera u otros datos confidenciales.

CÓMO LOS DELINCUENTES LO ENGAÑAN

Los siguientes mensajes de OnGuardOnline de la Comisión Federal de Comercio son ejemplos de lo que los atacantes podrían enviar por correo electrónico o mensaje de texto cuando realizan el phishing para información confidencial:

- "Sospechamos que se ha intentado realizar una transacción no autorizada en su cuenta. Para asegurar que su cuenta no esté comprometida, haga clic en el enlace a continuación y confirme su identidad."
- "Durante nuestra verificación regular de las cuentas, no pudimos verificar su información. Haga clic aquí para actualizar y verificar su información."
- "Nuestros registros indican que se ha sobrecargado a su cuenta. Debe llamarnos dentro de 7 días para recibir su reembolso."

Para ver ejemplos de correos electrónicos de phishing reales, y los pasos que debe seguir si cree que ha recibido un correo electrónico de phishing, visite StopRansomware.gov.

CONSEJOS SENCILLOS

- **Juegue a hacerse el difícil con extraños.** Los enlaces en correos electrónicos y publicaciones en Internet frecuente son la manera en que los delincuentes cibernéticos comprometen su computadora. Si no está seguro quién le ha enviado un correo electrónico—incluso si los detalles parecen correctos—no responda y no haga clic en los enlaces o los adjuntos en el correo electrónico. Tenga cuidado con saludos genéricos, tales como "Hola

cliente del banco", ya que frecuentemente son signos de intentos de phishing. Si está preocupado sobre la legitimidad de un correo electrónico, llame a la compañía directamente.

- **Piense antes de actuar.** No confíe en las comunicaciones que le exhortan a que actúe de inmediato. Muchos correos electrónicos de phishing intentan generar un sentido de urgencia para que el receptor tema que su cuenta o su información esté en peligro. Si recibe un correo electrónico sospechoso que parece ser de alguien que conoce, comuníquese directamente con esa persona en una plataforma segura distinta. Si el correo electrónico es de una organización, pero se ve como un intento de "phishing", comuníquese con la organización a través de su servicio al cliente para verificar la comunicación.
- **Proteja su información personal.** Si las personas que contactan a usted tienen detalles claves sobre su vida—el título de su trabajo, varias direcciones de correo electrónico, su nombre completo, y más información que usted podría haber publicado en Internet en algún momento—pueden tratar de dirigir un ataque de "spear phishing" en su contra. Los delincuentes cibernéticos también pueden usar la ingeniería social con esos detalles para tratar de manipular a usted para que omita los protocolos de seguridad normales.
- **Tenga cuidado con los enlaces.** Evite hacer clic en los enlaces que aparecen en los correos electrónicos y deje que su cursor flote sobre los enlaces para verificar su autenticidad. También asegure que las direcciones URL empiezan con "https". La "s" indica que el cifrado está habilitado para proteger la información del usuario.
- **Duplique la protección de sus credenciales.** Habilite la autenticación por múltiples factores (MFA, por sus siglas en inglés) para asegurar que la única persona con acceso a sus cuentas sea usted mismo. Úsela para su correo electrónico, su banco, sus redes sociales y todo otro servicio que requiere que inicie sesión. Si MFA es una opción, habilítela con un dispositivo móvil fiable, tal como su teléfono inteligente, una aplicación de autenticación o un token seguro—un dispositivo físico pequeño que puede llevar en su llavero. Para más información, lea la Guía a la Autenticación por Múltiples Factores (MFA, por sus siglas en inglés).
- **Altere su protocolo para sus contraseñas.** Según la guía del Instituto Nacional de Estándares y Tecnología, usted debe pensar en usar la contraseña o frase de contraseña más larga que se permite. Sea creativo y adapte su contraseña estándar para páginas diferentes, ya que esto puede evitar que los delincuentes cibernéticos obtengan acceso a estas cuentas y proteger a usted en caso de una filtración de datos. Use administradores de contraseñas para generar y recordar distintas contraseñas complejas para cada una de sus cuentas. Para más información, lea la Hoja de consejos sobre cómo crear una contraseña.
- **Instale y actualice software antivirus.** Asegúrese de instalar y actualizar con regularidad el software antivirus, cortafuegos, filtros de correo electrónico y programas contra el spyware en todas sus computadoras, dispositivos del Internet de las cosas, teléfonos y tabletas.

CÓMO HACER UNA DENUNCIA

Para denunciar intentos de phishing, spoofing o para informar que ha sido víctima de éstos, visite www.ic3.gov para hacer la denuncia. Para más información sobre las maneras en que puede proteger su información, visite la página de StopRansomware.gov.

COMUNÍQUESE CON EL EQUIPO DEL MES DE CONCIENTIZACIÓN SOBRE SEGURIDAD CIBERNÉTICA DE CISA

Muchas gracias por su apoyo y compromiso continuos con el Mes de Concientización sobre Seguridad Cibernética y por ayudar a todos los estadounidenses a mantenerse seguros en Internet. Para aprender más, envíe un mensaje por correo electrónico a nuestro equipo en CyberAwareness@cisa.dhs.gov, o visite www.cisa.gov/cybersecurity-awareness-month o staysafeonline.org/cybersecurity-awareness-month/.