El Boletín Mensual de Concientización en Seguridad para ti

Reconoce y evita ataques por mensaje de texto

¿Qué son los ataques por mensajería instantánea?

Smishing (una palabra que combina los términos en inglés SMS y phishing) son ataques que ocurren cuando los ciberdelincuentes utilizan mensajes de texto (SMS) o aplicaciones de mensajería para engañarte y hacer que tomes una acción que no deberías tomar. Quizás te engañen para que proporciones los datos de tu tarjeta de crédito, te hagan llamar a un número telefónico para obtener tu información bancaria o convencerte para que llenes una encuesta en línea para obtener tu información personal. Al igual que en los ataques tradicionales de phishing por correo electrónico, los ciberdelincuentes suelen jugar con tus emociones para conseguir que actúes con sentido de urgencia o curiosidad, por ejemplo. Sin embargo, lo que hace al smishing tan peligroso es que hay menos información y pocas pistas en un mensaje de texto que en un correo electrónico, lo que hace que sea mucho más difícil detectar que algo anda mal.

Una estafa común es un mensaje que te dice que ganaste un iPhone y solo necesitas hacer clic en un enlace y completar una encuesta para reclamarlo. En realidad, no hay teléfono y la encuesta está diseñada para recopilar tu información personal. Otro ejemplo sería un mensaje que indica que no se pudo entregar un paquete, con un enlace a un sitio web, donde te piden que proporciones la información necesaria para completar la entrega, incluyendo los detalles de tu tarjeta de crédito para cubrir los famosos "cargos por servicio". En algunos casos, estos sitios pueden incluso pedirte que instales una aplicación móvil no autorizada que infecte y tome el control de tu dispositivo.

A veces, los ciberdelincuentes incluso combinan ataques telefónicos y de mensajería. Por ejemplo, podrías recibir un mensaje de texto urgente de tu banco preguntándote si autorizas un pago sospechoso. El mensaje te pide que respondas “SÍ” o “NO” para confirmar el pago. Si respondes, los ciberdelincuentes ahora saben que estás dispuesto a interactuar y te llamarán pretendiendo ser el departamento de fraude del banco. Luego intentarán convencerte para que proporciones tu información financiera y de tu tarjeta de crédito, incluso el nombre de usuario y la contraseña de tu cuenta bancaria.

Reconociendo y evitando el smishing

Aquí hay algunas preguntas que debes hacerte para detectar las pistas más comunes de un ataque de mensajería de texto:

- ¿El mensaje crea una gran sensación de urgencia al intentar apresurarte o presionarte en tomar una acción?

- ¿El mensaje te lleva a sitios web que solicitan tu información personal, tarjeta de crédito, contraseñas u otra información sensible a la que no deberían tener acceso?
- ¿El mensaje suena demasiado bueno para ser verdad? No, realmente no te van a regalar un nuevo iPhone.
- ¿El sitio web o el servicio te obliga a pagar utilizando métodos no usuales como Bitcoin, tarjetas de regalo o transferencias no rastreables?
- ¿El mensaje te pide el código de autenticación multifactor que se envió a tu teléfono o que generó tu aplicación bancaria?
- ¿El mensaje parece el equivalente a un "número equivocado" de llamadas? Si es así, no respondas ni intentes comunicarte con el remitente; simplemente elimínalo

Si recibes un mensaje de una organización oficial que te alerta, verifica con ellos directamente. No uses el número de teléfono incluido en el mensaje, usa un número confiable en su lugar. Por ejemplo, si recibes un mensaje de texto de tu banco que dice que hay un problema con tu cuenta o tarjeta de crédito, identifica un número de teléfono confiable en el sitio web del banco, en un estado de cuenta o en el reverso de tu tarjeta. También recuerda que la mayoría de las agencias gubernamentales, como las agencias tributarias o de aplicación de la ley, nunca se comunicarán contigo por mensaje de texto, solo se comunicarán por correo tradicional.

Cuando se trata de ataques de mensajería, la mejor defensa eres tú.

Editor invitado

Jeff Lomas es detective del Grupo de Investigación Cibernética del Departamento de Policía Metropolitana de Las Vegas e imparte el curso SANS SEC487 de recopilación y análisis de información de fuentes abiertas (OSINT). Jeff investiga delitos financieros de alta complejidad tecnológica, incluidos incidentes de correo electrónico empresarial, smishing, ransomware y casos complejos de robo de criptomonedas y lavado de dinero.

Recursos

Evita el phishing: https://www.sans.org/newsletters/ouch/stop-that-phish/
Ingeniería social: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Vishing: Ataques a través de llamadas telefónicas: https://www.sans.org/newsletters/ouch/vishing/

Traducido para la comunidad por: Célica Martínez Aponte and Iván Galindo, UNAM-CERT