El Boletín Mensual de Concientización en Seguridad para ti

Top tres de estafas en redes sociales

Resumen

Si bien las redes sociales son una forma fantástica de comunicarse, compartir y divertirse con los demás, también son una forma económica para que los ciberdelincuentes engañen y se aprovechen de millones de personas. No seas víctima de las tres estafas más comunes en redes sociales.

Estafas de inversión

¿Alguna vez has visto una publicación sobre una oportunidad de inversión que promete un gran retorno en poco tiempo con un riesgo supuestamente mínimo o nulo? La realidad es que estas promesas son en realidad estafas de inversión. Los estafadores simplemente robarán tu dinero después de que les pagues. Estas estafas usualmente incluyen anuncios o historias de éxito de clientes anteriores para promover dichas inversiones, pero son solo testimonios falsos para aumentar tu confianza. A menudo, estas estafas de inversión tienen que ver con invertir en criptomonedas o bienes raíces, y el pago se suele realizar en este u otros métodos de pago no estándares. Si una inversión parece demasiado buena para ser verdad, lo más probable es que no lo sea. Recuerda, no existen las inversiones garantizadas de alto rendimiento. Solo invierte tu dinero instrumentos financieros conocidos y regulados, no en extraños que conozcas en línea que impulsan un plan para hacerse rico rápidamente.

Estafas amorosas

Cuando los delincuentes establecen una relación en línea con alguien que han identificado como solitario o vulnerable para engañarlos y sacarles dinero, esto se conoce como una estafa amorosa. Los delincuentes utilizarán todas las tácticas que puedan para generar confianza, incluido el envío de fotos falsas u obsequios, y luego compartirán una historia trágica sobre la necesidad de dinero para pagar gastos como las facturas del hospital o los costos de viaje para visitar a la víctima en persona. Para evitar reunirse en persona, estos delincuentes pueden decir que trabajan en una industria que les impide hacerlo, como la construcción, la medicina internacional o el ejército. Frecuentemente solicitan dinero mediante transferencias bancarias o tarjetas de regalo para obtener efectivo rápidamente y permanecer anónimos. Estos tipos de estafas no solo son comunes en las redes sociales, sino también en las apps de citas en línea. Ten cuidado con las personas que conoces en línea, toma las cosas con calma y nunca envíes dinero a alguien con quien solo te has comunicado por ese medio.

Además, si crees que alguien que conoces puede ser vulnerable a un ataque de este tipo o tiene una relación en línea que genera estas alertas, ofrece tu ayuda. A veces puede ser muy difícil para alguien con una conexión emocional darse cuenta de lo peligrosa que se ha vuelto la situación.

Estafas de compras en línea

Las estafas de compras en línea ocurren cuando compras artículos en línea a precios extremadamente bajos o increíbles, pero nunca los recibes. Los anuncios tentadores en las redes sociales promoverán precios increíbles y tendrán enlaces que te llevarán a sitios que parecen legítimos y venden marcas conocidas, pero estos sitios suelen ser falsos. Ten cuidado con los sitios web que no tienen información de contacto, que tienen formularios de contacto rotos o usan direcciones de correo electrónico personales. Escribe el nombre de la tienda en línea o su dirección web en un motor de búsqueda para ver lo que otros han dicho al respecto. Busca términos como "fraude", "estafa", "nunca más" y "falsificación". Ten mucho cuidado con las promociones u ofertas en línea que parecen demasiado buenas para ser verdad. Es mucho más seguro comprar artículos que pueden costar un poco más, pero de sitios confiables que tú o tus amigos hayan usado antes.

La buena noticia es que la mejor defensa eres tú. Tú tienes el control. Solo mantente alerta ante estafas como estas y podrás aprovechar al máximo las redes sociales de manera segura.

Editor invitado

Chris Elgee (@chriselgee) es pentester y diseñador de desafíos para @CounterHackSec, comandante de batallón cibernético en la Guardia Nacional de EE.UU. e instructor certificado de SANS. Disfruta aprender aspectos técnicos a fondo, para implementarlos en la organización y compartirlos con estudiantes y clientes.

Recursos

Rastreador de estafas del Better Business Bureau: https://www.bbb.org/ScamTracker
Ingeniería social: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Compras en línea de forma segura: https://www.sans.org/newsletters/ouch/shopping-online-securely-nov-21/
Ataques y estafas a través de llamadas telefónicas: https://www.sans.org/newsletters/ouch/vishing

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