



Apropiación de cuentas: depredadores emocionales

Tomada por sorpresa: la historia de Emma

Emma estaba navegando por Facebook cuando vio una publicación emotiva de su prima, Sara. La publicación compartía noticias devastadoras: el anciano padre de Sara se había mudado a un centro de atención para jubilados y estaba vendiendo sus pertenencias para ayudar a cubrir los gastos médicos. Se incluyeron fotografías de artículos como su auto, joyas y muebles antiguos a precios increíblemente bajos.

Queriendo ayudar y conseguir una gran oferta, Emma se comunicó rápidamente con Sara a través de Facebook Messenger por primera vez en años. Sara se alegró de recibir noticias de su prima y le informó a Emma sobre el estado de su padre. Ella se apresuró a pasar a los detalles del pago e instó a Emma a actuar rápido, ya que muchos artículos ya estaban reservados. Emma envió rápidamente el dinero, solo para descubrir más tarde que toda la publicación era una estafa.

De hecho, Emma nunca había hablado con su prima. La cuenta de Facebook de Sara había sido hackeada y tomada por un estafador. Después de obtener acceso total, el estafador publicó noticias falsas sobre el padre de Sara y luego explotó la red de confianza de amigos y familiares de Sara fingiendo vender sus artículos. Cuando la gente pensaba que estaban comprando artículos de Sara (y apoyando a su padre), en realidad estaban pagando a un estafador que simplemente se fue con su dinero.

¿Qué está sucediendo?

Los estafadores secuestran cuentas de redes sociales en plataformas como Facebook o Instagram, a menudo averiguando nombres de usuario y contraseñas. Una vez dentro, se hacen pasar por el propietario de la cuenta para compartir publicaciones falsas que suelen incluir detalles emocionales para crear una sensación de urgencia e impulsar a las personas a la acción. Estas estafas a menudo incluyen historias como haber sido asaltado en una ciudad y necesitar ayuda, o haber tenido un accidente automovilístico y necesitar dinero, o que un ser querido falleció y sus pertenencias se están vendiendo.

Las víctimas se sienten atraídas, creyendo que la publicación es de alguien que conocen y en quien confían. Envían dinero, a menudo a través de métodos de pago imposibles de rastrear, como aplicaciones peer to peer o transferencias bancarias, solo para descubrir más tarde que en realidad no estaban tratando con su familia o amigos, y su dinero desaparece.

¿Qué hace que estafas como estas sean tan peligrosas?

- **Confianza robada:** los estafadores aprovechan la red de confianza de las cuentas de redes sociales que controlan. Las publicaciones parecen provenir de un amigo o familiar de confianza, lo que las hace más creíbles.

- **Manipulación emocional:** los estafadores usan temas personales y emocionales que a menudo crean una fuerte sensación de urgencia u oportunidad, presionando a las personas para que, en última instancia, cometan un error.
- **Propagación rápida:** una vez que la cuenta de la víctima se ve comprometida, el estafador puede llegar rápidamente a cientos o miles de personas. Además, muchas personas usan la misma contraseña para varias cuentas de redes sociales, por lo que una vez que una cuenta es comprometida, esa misma contraseña puede usarse para apropiarse de las otras cuentas de redes sociales de la víctima.

Cómo protegerte y proteger a los demás

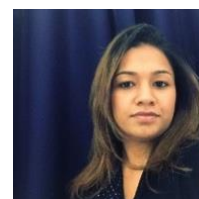
- **Sé escéptico con las publicaciones emotivas que involucran dinero:** si una publicación parece inusualmente emotiva o urgente e involucra enviarle dinero a alguien, detente y verifica, podría ser una estafa.
- **Verifica con la persona directamente:** comunícate con la persona a través de un canal separado para confirmar la historia. Por ejemplo, llámala por teléfono o habla con ella en persona. Muy a menudo, la víctima ni siquiera sabe que su cuenta ha sido comprometida o sobre las publicaciones del estafador en su cuenta.
- **Busca alertas rojas:** los estafadores suelen solicitar el pago a través de métodos imposibles de rastrear, como tarjetas de regalo o criptomonedas. Otra alerta roja es si te piden que utilices una plataforma diferente para continuar la conversación (como pasar de Facebook Messenger a WhatsApp).
- **Protege tu cuenta:** si hackean tu cuenta y se apoderan de ella, lo primero que suelen hacer los cibercriminales es cambiar tu contraseña, lo que te impedirá acceder a ella. Una vez que esto suceda será muy difícil recuperarla. Comienza por proteger cada una de tus cuentas con una contraseña larga y única. Luego habilita la autenticación multifactor para cada cuenta. Estos dos sencillos pasos hacen que tus cuentas sean mucho más seguras, ¡y los estafadores te odiarán por ello!

Mantente un paso adelante

Cuando se trata de estafas de robo de cuentas, la mejor defensa eres tú. Si sospechas que te enfrentas a esta estafa, denuncia la cuenta y notifica a tu plataforma de redes sociales de inmediato.

Editor invitado

Amie Dsouza es una profesional de la ciberseguridad y trabaja para una importante aerolínea de los EE.UU. Ella trabaja en seis países y se desempeña como miembro de la junta directiva de Women in Cybersecurity (WiCys). Amie aboga activamente por educar a todos sobre cómo mantener seguros los datos personales en línea.



Recursos

Detonantes emocionales - cómo te engañan los estafadores: <https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/>

Cómo los cibercriminales te roban tus contraseñas: <https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords>

El poder de las frases de contraseña: <https://www.sans.org/newsletters/ouch/power-passphrase/>

Fui hackeado, ¿ahora qué?: <https://www.sans.org/newsletters/ouch/im-hacked-now-what/>

Traducido a la comunidad por: Célica Martínez Aponte (SSAP) e Iván Galindo.

OUCH! OUCH! es publicado por SANS Security Awareness y distribuido bajo la [licencia Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Eres libre de compartir o distribuir este boletín siempre y cuando no lo vendas o modifiques. Comité editorial: Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.