El Boletín Mensual de Concientización en Seguridad para ti

Estafas por desastres o caridad

Los ciberdelincuentes saben que una de las mejores maneras de apresurar a las personas para que cometan un error es creando un mayor sentido de urgencia, y una de las formas más fáciles de crear un sentido de urgencia es aprovechar una crisis. Es por eso que a los ciberdelincuentes les encanta cada vez que hay un evento traumático con impacto global. Lo que la mayoría de nosotros consideramos una tragedia, los ciberdelincuentes lo ven como una oportunidad, como el comienzo de una guerra, un gran desastre natural como una explosión volcánica y, por supuesto, brotes de enfermedades infecciosas como la COVID-19. Cuando hay una inmensa cobertura en redes sociales y noticias sobre un determinado evento, los ciberdelincuentes saben que es el momento de atacar.

Aprovechan esta oportunidad para crear correos electrónicos de phishing o estafas sobre el evento, y luego envían dichos correos o lanzan la estafa a millones de personas en todo el mundo. Por ejemplo, durante un desastre natural, pueden pretender ser una organización benéfica pidiendo donaciones para salvar a niños necesitados. Los ciberdelincuentes pueden actuar a las pocas horas de una crisis o desastre, ya que tienen toda la infraestructura técnica preparada y lista con anticipación. ¿Cómo podemos protegernos la próxima vez que haya una gran crisis o desastre y los ciberdelincuentes intenten explotarlo?

Cómo detectar y defenderse contra estas estafas

La clave para evitar estas estafas es sospechar de cualquiera que trate de acercarse a ti. Por ejemplo, no confíes en un correo electrónico urgente que dice ser de una organización benéfica que necesita donaciones desesperadamente, incluso si el correo electrónico parece ser de una marca que conoces y en la que confías. No confíes en una llamada telefónica que dicen ser de un banco de alimentos local que te presionan para que dones. Cuanto mayor sea el sentido de urgencia, es más probable que la solicitud sea un ataque. Estas son algunas de las pistas más comunes de que es un ataque de caridad:

- Sospecha mucho de cualquier organización benéfica que requiera que dones a través de criptomonedas, Western Union, transferencias de dinero o tarjetas de regalo.
- Los ciberdelincuentes pueden cambiar el número de teléfono del identificador de llamadas para que parezca que su llamada proviene de tu código de área local o de un nombre de confianza. No se puede confiar en el identificador de llamadas en estos días.
- Algunos ciberdelincuentes usarán nombres y logotipos que suenan o se ven como una organización benéfica real. Esta es una de las razones por las que vale la pena investigar un poco antes de donar.
- Los ciberdelincuentes frecuentemente harán muchas afirmaciones poco claras y sentimentales sobre lo que harán con tu dinero, pero no darán detalles sobre cómo se utilizará la donación.

- No asumas que las peticiones de ayuda en sitios de financiación colectiva como GoFundMe o de redes sociales como TikTok son legítimas, especialmente después de una crisis o tragedia.
- Algunos ciberdelincuentes pueden tratar de engañarte para que les hagas una donación agradeciéndote por otra que hiciste en el pasado cuando, en realidad, nunca donaste en primer lugar.
- No proporciones información personal o financiera en respuesta a una petición no solicitada.

Cómo hacer una diferencia de manera segura

Para donar en momentos de necesidad o para ayudar a las personas afectadas por un desastre, dona solo a organizaciones reconocidas y confiables. Inicia tú las conexiones y decide a quién contactar, qué sitios web visitar o qué organizaciones llamar. Cuando consideres donar a una organización benéfica, busca su nombre y palabras como "queja", "opinión", "calificación" o "estafa". ¿No estás seguro en qué organizaciones benéficas confiar? Comienza investigando en sitios web del gobierno en los que confíes, o quizás en los enlaces proporcionados por una organización de noticias reconocida y de gran confianza. Donar en momentos de necesidad es una forma fantástica de hacer la diferencia, solo asegúrate de donar a organizaciones legítimas.

Editor invitado

La Dra. Jessica Barker es una líder galardonada en el lado humano de la seguridad. Es co-CEO de Cygenta y autora exitosa. Jessica está en el consejo consultivo de la Conferencia SANS Security Awareness.

Recursos

Cómo evitar estafas de caridad (CFT): https://consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams
Ingeniería social: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Top tres de estafas: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Smishing- Ataques a través de mensajería instantánea: https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
Ataques a través de llamadas telefónicas: https://www.sans.org/newsletters/ouch/vishing/
Buscador de organizaciones benéficas: https://www.charitynavigator.org/

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