Los ‘centennials’ están en todas las redes, los estafadores también

Las garras digitales de los estafadores en línea son alargadas. Pero para extraer datos personales, dinero y atención en el ciberespacio, hace falta comprender el comportamiento de los grupos a los que se pretende engañar. Un informe de xpertos en ciberseguridad repasa los procedimientos más utilizados por los criminales cibernéticos para engañar a los centennials (o generación Z, nacidos entre 1996 y 2012) mientras navegan por la web.

Jóvenes nacidos ya en un mundo plenamente digital que se desenvuelven con menores sospechas en internet. **“Si sos uno de ellos es posible que seas confiado y por eso puede que seas una persona fácil de manipular por los estafadores**”, explican desde la compañía de seguridad informática ESET.

Las cinco de las estafas más comunes dirigidas a adolescentes:

Enlaces vía chats en redes

Los centennials están en todas las redes sociales. **Desde TikTok hasta Instagram, pasando por Snapchat y WhatsApp. Y los estafadores también.** El método por excelencia de los ciberdelincuentes consiste en enviar enlaces de artículos sensacionalistas y muchas veces falsos con titulares impactantes sobre celebridades Por ejemplo: Mira lo que hizo enfadar a Rafa Nadal en el Roland Garros o Esta es la nueva operación estética de Ester Expósito. Sin embargo, cuando el usuario hace clic, es redirigido a un sitio web malicioso.

Hay más técnicas. Los estafadores también contactan a sus víctimas directamente a través de mensajes en las redes, por medio de sus diversas funciones de chats directos y los invitan a participar en concursos o sorteos. Incluso hay quienes ofrecen servicios para convertirlos en influenciadores o ayudarles a ganar seguidores y “me gusta” en sus publicaciones. Pero el enlace compartido también los redirige a un sitio web fraudulento que infecta sus dispositivos y secuestra sus datos.

Descuentos increíbles

¿Quién no busca ofertas en línea? Artículos que comúnmente cuestan mucho dinero suelen anunciarse en las redes a precios ridículamente bajos… y falsos.
Los centennials han crecido con el comercio en línea y ven como algo cotidiano adquirir productos y servicios por internet. Esto además se ha reforzado con la pandemia, que ha obligado al mundo a encerrarse en sus casas.

Los estafadores ofrecen marcas y productos que están a la moda, como zapatillas deportivas de edición limitada, ropa que suele ser demasiado cara o artículos en falsas tiendas en línea. ¿Cómo lo hacen? **“Crean un sitio web minorista falso que ofrece una amplia variedad de estos productos. Una vez que alguien compra en estos sitios, recibirá un producto de imitación o puede que no reciba nada”,** explican desde ESET. Más allá de haber pagado por algo y no recibirlo, el mayor riesgo es que si la víctima compartió los datos de su tarjeta de crédito, los ciberdelincuentes acumularán cargos y “limpiarán” la cuenta bancaria.

Expertos en ciberseguridad recomiendan **“escribir directamente la dirección en la barra de navegación o utilizar una app oficial”,** para evitar seguir enlaces que lleguen a través de mensajes o correos de dudosa procedencia. Y, sobre todo, utilizar el menos común de los sentidos: el sentido común. “Si parece demasiado bueno para ser verdad, probablemente será mentira”, concuerdan.

Becas falsas

Esta generación está comenzando o finalizando sus estudios universitarios y por ello el sector de la educación es otro escenario ideal para las estafas. El elevado coste de las matrículas lleva a muchos a buscar la forma de conseguir una beca que cubra parte de la misma. Los estafadores crean para ello programas ficticios de diversas formas. **“Por ejemplo, estos falsos programas de becas a menudo solicitarán que el interesado pague una tasa de registro. Sin embargo, la beca no existe y el estafador terminará quedándose con el dinero entregado**”, explican los expertos en ciberseguridad.

El Instituto Nacional de Ciberseguridad (INCIBE) recomienda en su sitio web este manual para reconocer fraudes en línea, al que puedes acceder aquí. **“Proporciona información útil para que los menores puedan aprender a reconocer fraudes, ya que algunas de estas estafas les afectan directamente, por ejemplo si les llegan a través del chat de un juego o un mensaje privado de redes sociales”,** explican en su portal.

Empleos demasiado buenos

Además de estudiar, muchos jóvenes de la generación centennial están buscando empleos. Los estafadores crean falsas ofertas laborales demasiado tentadoras: pocas horas de trabajo y salarios altos, trabajo desde casa y poca experiencia previa, por ejemplo. Los criminales publican sus ofertas en bolsas de empleo legítimas para obtener información personal de las víctimas y luego utilizar estos datos para abrir cuentas bancarias a nombre de los estafados o falsificar documentos con sus identidades.

“Si encuentras una oferta de trabajo que suena tentadora, pero tiene dudas al respecto, realiza una búsqueda rápida en la web de la empresa que ofrece el supuesto trabajo para ver si surge algo sospechoso. Además, recuerda brindar información personal para propósitos salariales solo después de haber sido contratado”, aconsejan .

Romances de mentira

Las plataformas para citas románticas son el escenario perfecto para las estafas. En estas redes no solo se juega con los corazones, también con los bolsillos. ¿Cómo? El estafador se hace pasar por una persona que la víctima considera atractiva para luego mantener una relación hasta lograr robarle su dinero o datos.

“Lamentablemente, en algunos casos los ciberdelincuentes utilizan tácticas aborrecibles, como manipular sus víctimas para que compartan fotos íntimas y luego extorsionarlas para que paguen dinero, amenazando con revelar estas fotos a sus seres queridos y al público en caso de no pagar”, explican desde ESET. Aunque los sitios de citas son los sitios más sencillos para realizar estas prácticas, a menudo también buscan a sus víctimas en las redes sociales y se comunican con ellos a través de mensajes privados.