Ciberseguridad: 5 estafas comunes dirigidas a los adolescentes

08/06/2021

Si bien los adolescentes no son tan impresionables como los niños pequeños, aún pueden estar sujetos a diversas influencias externas. **En este sentido es posible que sean más confiados y por esta razón puedan convertirse en un objetivo para estafadores que buscan engañarlos y quedarse con su dinero o sus datos personales.**

ESET, una compañía en detección proactiva de amenazas, analizó algunas de las estafas más comunes dirigidas a adolescentes y explica a qué prestar atención para evitar caer en la trampa ayudándolos así a mantenerse seguros en Internet.

Las 5 estafas más comunes dirigidas a los adolescentes y consejos sobre cómo mantenerse protegidos:

1- Estafas en las redes sociales

Dado que las redes sociales ocupan mucho espacio en la vida de la mayoría de los adolescentes, es natural que los estafadores traten de apuntar a ellos en el lugar en el que pasan la mayor parte de su tiempo. Algunos de los métodos más comunes que utilizan los delincuentes consiste en enviar enlaces de artículos sensacionalistas con titulares impactantes sobre celebridades.

Sin embargo, cuando el usuario hace clic en dicho enlace es redirigido a un sitio web malicioso. Alternativamente, los estafadores pueden intentar contactar a sus víctimas directamente a través de mensajes en los que se invita a participar en concursos o sorteos, pero nuevamente, el enlace compartido muy probablemente redirigirá al adolescente a un sitio web fraudulento que infectará sus dispositivos con malware o tratará de sustraer información confidencial.

2- Grandes descuentos en artículos y productos que suelen ser costosos

Para hacer que sus ofertas sean atractivas para los adolescentes, los estafadores intentan ofrecer marcas y productos que les resulten atractivos, como zapatillas deportivas de edición limitada, ropa de marcas que suelen ser demasiado caras para un salario medio o un trabajo a tiempo parcial, o falsas tiendas en línea de Ray-Ban, por nombrar un ejemplo.

El engaño consiste en crear un sitio web minorista falso que ofrece una amplia variedad de estos productos. Una vez que alguien realiza una compra en estos sitios, recibirá un producto de imitación o directamente puede que no reciba nada. Y en el peor de los casos, si la víctima compartió los datos de su tarjeta de crédito, los ciberdelincuentes acumularán cargos y limpiarán la cuenta bancaria.

3- Estafas de becas

Los estafadores intentan aprovecharse de los estudiantes que buscan este tipo de ayuda financiera creando falsas becas, las cuales pueden adoptar 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. Alternativamente, la estafa puede consistir en una beca que la persona ganó a través de un sorteo. En este caso también se solicitará al estudiante que pague una “tasa de procesamiento” o una “tasa de desembolso” justificando este pago debido a los costos impositivos, pero en última instancia, el resultado es el mismo.

4- Estafas laborales

Ser un adolescente con múltiples intereses, como ir a conciertos, viajar o hasta ser fashionista, no es fácil, especialmente porque muchas veces no se cuenta con el dinero suficiente para poder realizar estas actividades. Para dirigirse a los jóvenes que buscan empleo, los ciberdelincuentes crean falsas ofertas laborales que suelen parecer demasiado buenas para ser verdad.

Los estafadores publicarán estas ofertas de trabajo en bolsas de empleo legítimas y, por lo general, ofrecerán puestos que le permitirán trabajar desde casa y ganar un sueldo considerable. Sin embargo, el objetivo final es obtener información personal de las víctimas para luego utilizar estos datos en diversas actividades ilícitas, como abrir cuentas bancarias a nombre de sus víctimas o usar sus identidades para falsificar documentos.

5- Estafas románticas

Las apps y plataformas de citas online se han convertido en terrenos de caza para delincuentes que llevan adelante las denominadas estafas románticas. Sin embargo, estos estafadores no solo se limitan a los sitios de citas, a menudo buscan a sus víctimas en las redes sociales y se comunican con ellos a través de mensajes privados. El engaño se basa en hacerse pasar por una persona que la víctima considere atractiva. Luego, el o la estafadora construirá un vínculo de confianza con su víctima hasta lograr su objetivo final: robarle su dinero.

Lamentablemente, en algunos casos los ciberdelincuentes utilizan tácticas de manipulación como solicitar fotos intimas y luego extorsionar a las víctimas para que paguen dinero, amenazando con revelar estas fotos a sus seres queridos y al público en caso de no pagar.

Si bien las estafas dirigidas a los adolescentes ocurren a gran escala, desde ESET comparten formas en las que protegerse contra ellas:

- Si se encuentra una oferta de trabajo que suena tentadora, pero se tiene dudas al respecto, realizar una búsqueda rápida en la web de la empresa que ofrece el supuesto trabajo para ver si surge algo sospechoso. Además, recordar brindar información personal para propósitos salariales solo después de haber sido contratado.
- Un consejo similar se aplica en el caso de las becas: si se está buscando una, asegurarse de verificar si la organización que ofrece la beca es legítima realizando una búsqueda en la web o comunicándose directamente con sus oficinas. Y nunca realizar ningún tipo de tasa de "procesamiento" o "adelanto" sin hablar antes con el establecimiento.
- Una de las reglas de oro en Internet es: "si parece demasiado bueno para ser verdad, probablemente lo sea". Entonces, al toparse con un producto de edición limitada a un precio sorprendentemente bajo, seguramente se trate de una estafa. Si todavía se estáintrigado, consultar directamente al fabricante e investigar para chequear su autenticidad.

- Si se recibe un mensaje no solicitado de alguien que no se conoce, tener cuidado, especialmente si hace referencia a una oferta dudosa o contiene un enlace. En cualquier caso, la mejor opción es ignorar el mensaje y recordar: nunca se debe hacer clic en un enlace de un desconocido.
- En caso de que un extraño esté tratando de iniciar contacto y luego de unos pocos mensajes comience a profesar su amor, se debería prestar atención. Una búsqueda rápida de las imágenes en reversa de esta persona debería ser suficiente para descubrir si se

están haciendo pasar por alguien o no.

“Independientemente de la edad, como usuarios es importante estar atento a los mensajes que recibimos, no ingresar nuestros datos en sitios desconocidos, ni acceder a links sospechosos. Tomarse unos minutos para analizar el proceso, pensar las cosas y revisar los sitios y la información solicitada es indispensable. Conocer los riesgos a los que se está expuesto, actualizar las aplicaciones, contar con una solución de seguridad en los distintos dispositivos y aplicar el sentido común a la hora de interactuar en línea permitirá evitar caer en cualquier tipo de engañou oferta que resulte demasiado buena para ser verdad.”, aconseja Cecilia Pastorino, Investigadora del Laboratorio de ESET Latinoamérica.

Fuente: Ámbito