Atención: estas son las estafas más comunes en Instagram

18/09/2021

Con el paso de los años Instagram se ha convertido en una de las redes sociales más importantes del mundo, siguiendo los pasos de su “app madre”, Facebook, y de la plataforma de videos más famosa del mundo, YouTube.

De acuerdo con el informe Digital 2021, elaborado por We Are Social y Hootsuite, Instagram se posiciona como la cuarta red social con mayor número de usuarios registrados en su plataforma, con más de 1.220 millones, por detrás de Facebook con 2740 millones, YouTube (2291 millones), WhatsApp (2 mil millones) y Facebook Messenger (1300 millones).

Sin embargo, entre más popularidad adquiere una plataforma de este estilo, más sensible se convierte en cuanto a ataques a

la seguridad de sus usuarios se refiere. Por supuesto, el número de personas conectadas con las que cuenta Instagram actualmente, es una situación atractiva para **los ciberdelincuentes que ven como una opción potencial efectuar sus ataques.**

Por esto, Infobae da a conocer algunas de las estrategias de estafa más comunes dentro de Instagram, para que pueda prevenir cualquiera de estas en caso de que se presenten durante su navegación en esta red social. REUTERS/Steve Marcus/File Photo

Phishing

El **phishing** es un tipo de ciberataque que consiste en suplantar la identidad de una persona o compañía, en este caso Instagram, por medio de un e-mail que llega a su correo electrónico, en el que se le alerta de un supuesto problema relacionado con su cuenta dentro de la plataforma. Así, por medio de un enlace adjunto al mensaje principal, **los ciberdelincuentes hacen que la persona acceda a una página muy similar a la de Instagram, ofreciendo, sin que el usuario lo sepa, los datos de acceso como usuario y contraseña, a los estafadores.**

También, se puede presentar por medio de los DM de la aplicación, a los que llegará un mensaje de un presunto agente de soporte que también necesita que inicie sesión en una página. De forma automática, este sitio recopilará sus datos personales y pondrá a completa disposición de los delincuentes su perfil de Instagram.

“Para evitar ser víctima del phishing se aconseja prestar atención a determinados elementos que muchas veces dan una pista de que puede tratarse de un mensaje falso, como son los **errores gramaticales o el uso de saludos genéricos en lugar de personalizados**”, explicó Camilo Gutiérrez Amaya, jefe

del Laboratorio de Investigación de ESET Latinoamérica, por medio de un comunicado oficial. Se buscará limitar el envío de mensajes directos en Instagram entre jóvenes y adultos desconocidos

Cuentas clonadas

Otro de los ataques más comunes a la seguridad en Instagram es la clonación de cuentas, una problemática que afecta a todas las redes sociales por igual. En este caso, el modus operandi consiste en robar la identidad de una persona y crear una cuenta alterna a la oficial para así hacerse pasar por dicho usuario. De esta forma, **el delincuente (que tiene el poder de la cuenta clonada), podría hacer pensar a su víctima que la cuenta legítima de su familiar o amigo ha sido robada y que durante este falso acto ilegal los ladrones limpiaron las cuentas bancarias de la persona**, haciendo que la víctima crea en la historia y acceda a dar un poco de dinero para contrarrestar "la pérdida".

Asimismo, los delincuentes pueden simplemente hacer uso de ingeniería social (trabajo mental), para convencer a las víctimas de ofrecer su ayuda en medio de una presunta situación económica lamentable.

Lo recomendable en estos casos es contactar a la persona citada y verificar si es cierto o no su infortunio. Las cuentas falsas utilizan fotos e información privada de las cuentas originales.

¿Cuenta verificada?

Los ciberdelincuentes también suelen aprovechar la "sed" de las personas por obtener la verificación de sus cuentas en Instagram: un símbolo azul que aparece al lado de sus nombres y que demuestra que el usuario es una persona real además, de influyente e importante dentro de la red social.

En este caso, lo único que tienen que hacer los ciberdelincuentes es escribir a un determinado usuario por medio de un mensaje directo y venderle la falsa idea de que puede ayudarle a verificar su cuenta, todo por una módica suma de dinero. **“Sin embargo, si paga, lo único que se verificará es el hecho de que se convirtió en víctima de una estafa”**, indicó ESET.

Cuidado con el amor

Este punto es claro: existe una persona que, en busca de dinero, contacta a un usuario de Instagram y primero, por medio de comentarios a sus publicaciones, y después por mensajes directos, logra ganarse su confianza. Tras alcanzar este nivel, el delincuente pone en marcha su plan empezando, según el informe de ESET, **“a pedir dinero utilizando como excusa una emergencia médica o la necesidad de una ayuda económica para financiar un vuelo que les permita verse en persona”.**

De acuerdo con la Comisión Federal de Comercio de Estados Unidos, en 2020 este tipo de estafa arrebató más de 304 millones de dólares a usuarios que, infortunadamente, fueron víctimas de falsas promesas de amor. 13-09-2021 Estafadores en las apps de citas POLITICA INVESTIGACIÓN Y TECNOLOGÍA KASPERSKY

¿Vendedores o delincuentes?

Por último, solo queda hablar de las estafas presentes en los acuerdos comerciales dentro de Instagram. Muchas veces se crean cuentas empresariales en esta plataforma con las que se pretende robar a las personas, por medio de promesas de productos excelentes a precios muy bajos. No obstante, **cuando se transfiere el dinero, este se esfuma, pues simplemente nunca llegará el producto deseado.** El trabajo de los delincuentes está hecho y la persona se convirtió en una

víctima más.

“El mejor consejo es el que se ha repetido incontables veces: **no confíe ciegamente y verifique siempre. Tenga cuidado con los correos electrónicos no solicitados, si algo parece fuera de lugar, investigue, y si algo parece demasiado bueno para ser verdad, lo más probable es que sea una estafa**”, concluyó la empresa en su comunicado.

Fuente: Infobae