JUNIO DE 2022 | Nº 06-2022

¿CUÁLES SON LAS ESTAFAS MÁS COMUNES EN REDES SOCIALES?

BOLETÍN INFORMATIVO ARLC/FT/FPADM Y OTROS ILÍCITOS

FUENTE: ANTILAVADODEDINERO/IPROUG

Según la consultora especializada en ciberseguridad, BTR Consulting, Instagram, Tinder y LinkedIn son las plataformas más afectadas por este tipo de ataques, que se basan en la ingeniería social para preparar todo tipo de engaños que tienen asidero en la realidad.

Las estafas de phishing son una de las tácticas más utilizadas por los estafadores. Generalmente mientras se hacen pasar por marcas famosas, envían mensajes de texto y correos electrónicos falsos que contienen enlaces tratan de tentarte para que los abras con engaños variados y divertidos.

En tales esquemas, los enlaces te llevarán a páginas de inicio de sesión falsas que parecen pertenecer a marcas famosas y reconocidas. Estas páginas requieren que envíe credenciales de inicio de sesión, nombre de usuario y password para descargar una actualización de software, cambiar la configuración de la cuenta o cualquier otra acción que los estafadores le hayan pedido que complete. Las estafas de phishing son una de las tácticas más utilizadas por los estafadores

LA DIGITALIZACIÓN ACELERADA ABRIÓ UN CALDO DE CULTIVO PARA LA PROLIFERACIÓN DE NUEVAS ESTAFAS Y ATAQUES DIGITALES QUE CRECEN A TODA MARCHA Y EL PHISHING ES UNA DE LAS TÁCTICAS MÁS UTILIZADAS POR LOS ESTAFADORES PARA ACCEDER A LA INFORMACIÓN PERSONAL DE LOS USUARIOS..

Phishing en Instagram

Muchos usuarios denunciaron recibir un enlace misterioso y un mensaje incitando a abrirlo: «Creo que apareces en este video, sos vos?»

Pero el enlace te llevará a un sitio falso donde te pedirán que ingrese sus datos de inicio de sesión de Instagram.

Hacerlo es brindarles a los ciberdelincuentes las credenciales de la cuenta de Instagram y cometer robo de identidad.

Lo que es peor, pueden enviar spam a los contactos con los mismos mensajes de estafa y ampliar el universo de alcance de la
estafa.

Tinder y LinkedIn también está en la mira. Una modalidad similar pero articulada en las plataformas de citas Tinder y de profesionales LinkedIn, los estafadores difunden enlaces a sitios web fraudulentos para adultos con correos electrónicos que se hacen pasar por estas marcas que gozan de presencia en el mercado y reputación:

Los estafadores hacen todo lo posible para atraer para hacer click en el botón incrustado que dirige a un sitio web falso para adultos donde podría terminar exponiendo sus credenciales.

La ingeniería social es clave para preparar todo tipo de engaños que tienen asidero en la realidad.

Cómo protegerte del phishing

Sospechar de los obsequios y premios gratuitos. No confiar en mensajes que llegan vía WhatsApp o RRSS que ofrecen premios y/o regalos.

Nunca entregar datos personales, ni nombre de usuario y password, número de cuentas bancarias, número tarjeta de crédito, en general «datos sensibles».

Verificar en la web si existen denuncias o damnificados

Observar la URL de la página web, verificar si es un sitio oficial o un clon

Desconfiar por más que nos lleguen a través de personas que conocemos

Siempre acceder al sitio web/aplicación oficial en lugar de usar enlaces de fuentes desconocidas.

Nunca hacer click en enlaces o archivos adjuntos de fuentes desconocidas.

Activar la autenticación de dos factores