ESET: el phishing y smishing se han reinventado

ESET advierte que hay antiguos engaños que se han vuelto a poner en auge, como **phishing, smishing** y archivos adjuntos y los laboratorios que la empresa tienen en América Latina han analizado **dos casos de reciente circulación,** con el objetivo de repasar cómo funcionan estas viejas técnicas, combinadas con novedosos engaños para alcanzar más víctimas.

Sobre el smishing, recuerdan desde la firma que es "un tipo de técnica que se presenta cuando una víctima recibe un mensaje de texto (**SMS**) en el cual **es inducida a ingresar a un enlace malicioso** y los pretextos pueden ser una cuenta suspendida, el restablecimiento de una contraseña o un acceso indebido a una cuenta, por ejemplo".

El estafador **se hace pasar por una entidad conocida, como un banco o una empresa**. "Este tipo de técnica suele ligarse a la ingeniería social, ya que busca hacerse de contraseñas o información crítica del usuario, pero no suele propagar códigos maliciosos". Uno de los casos más recientes registraods en Latinoamérica, fue un mensaje que se progragó con el pretexto de desbloquear una cuenta del banco mexicano Banamex.

Por otro lado, **el phishing redirect con archivos adjuntos**, "es un ataque que se comete con el objetivo de adquirir fraudulentamente información personal y confidencial de la víctima donde el estafador se hace pasar por una persona o empresa de confianza, utilizando una aparente comunicación oficial como correos electrónicos, sistemas de mensajería instantánea o incluso llamadas telefónicas".

Recientemente, ESET descubrió un ataque de phishing donde el correo simulaba ser una comunicación proveniente de PayPal, aunque asegura que "si bien la dirección de origen parece ser pago@paypal.com.ar, es fácil distinguir que es en realidad un alias de otra dirección con un dominio desconocido". El pretexto del engaño es un clásico problema con la información de la cuenta, en este caso un cambio en el número de teléfono asociado. Curiosamente, el mensaje no contiene un enlace, sino un archivo adjunto. En su interior, se induce al usuario a visitar un sitio web. El mismo es malicioso y lo llevará a un sitio web que imita al original de PayPal, donde se solicitaran las credenciales de acceso.

Hay que "tener especial cuidado con mensajes que dicen provenir de entidades financieras o promociones que incluyan un enlace web, una petición urgente o que induzcan a compartir ese enlace. Mayormente son estafas, la mejor manera de comprobarlo es comunicarse con la entidad para confirmarlo", recuerdan los expertos.