Departamento de TIC

CAPSULA INFORMATIVA

¿Qué es phishing?

Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de phishing que es la más común. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita (o "suplanta su identidad") a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundirle miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia. O también puede venir en forma de una oferta de compra irresistible.

Si un usuario pica el anzuelo y hace clic en el enlace, se le envía a un sitio web que es una imitación del legítimo. A partir de aquí, se le pide que se registre con sus credenciales de nombre de usuario y contraseña. Si es lo suficientemente ingenuo y lo hace, la información de inicio de sesión llega al atacante, que la utiliza para robar identidades, saquear cuentas bancarias, y vender información personal en el mercado negro.

"El phishing es la forma más sencilla de ciberataque y, al mismo tiempo, la más peligrosa y efectiva".

A diferencia de otros tipos de amenazas de Internet, el phishing no requiere conocimientos técnicos especialmente sofisticados. De hecho, según Adam Kujawa, Director de Malwarebytes Labs, "el phishing es la forma más sencilla de ciberataque y, al mismo tiempo, la más peligrosa y efectiva. Eso se debe a que ataca el ordenador más vulnerable y potente del planeta: la mente humana". Los autores del phishing no tratan de explotar una vulnerabilidad técnica en el sistema operativo de su dispositivo, sino que utilizan "ingeniería social". Desde Windows e iPhones a Macs y Androids, ningún sistema operativo está completamente a salvo del phishing, con independencia de lo sólida que sea su seguridad. De hecho, los atacantes a menudo recurren al phishing *porque* no pueden encontrar ninguna vulnerabilidad técnica. ¿Por qué perder el tiempo tratando de burlar capas de seguridad cuando puede engañar a alguien para que le entregue la llave? En la mayoría de los casos, el eslabón más débil en un sistema de seguridad no es un fallo oculto en el código informático, sino una persona que no comprueba la procedencia de un correo electrónico.

¿Como evitarlo?:

Cuando nos llegue una notificación de cualquier índole, sea dudosa o no, debemos estar seguros de que la información que se presenta es realmente de nosotros, se dan casos en dicen que se efectuó un cargo a una tarjeta, pero no dice el número, o falta una información, que usted sabe que su banco la tiene.

Por ninguna razón utilice el enlace que viene en ese correo, simplemente vaya a la pagina principal de cualquier identidad que diga que este correo proviene y entre directamente, nunca y repito NUNCA, usen los links que están en los correos.