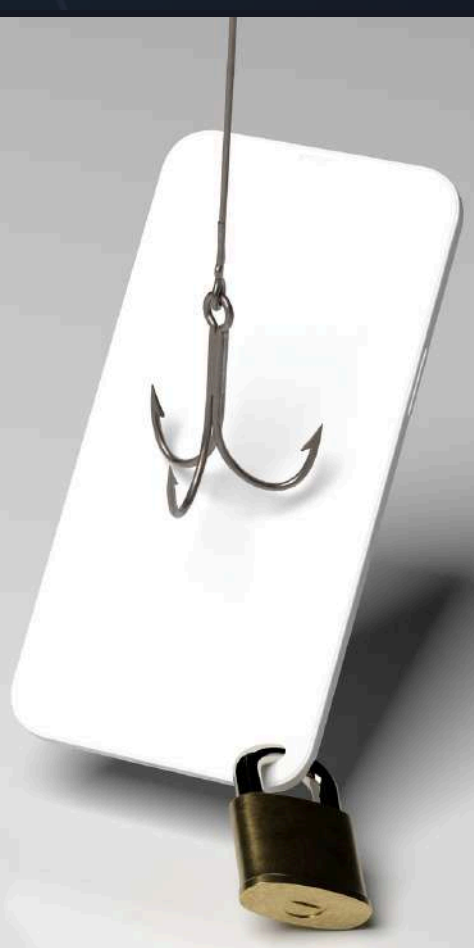
MAYO 2024

3+ Report

ANÁLISIS DE LA SEGURIDAD PRIVADA

PHISHING



Los ataques cibernéticos son accesos no autorizados a sistemas o redes informáticas por parte de terceros. Quienes incurren en estas prácticas son denominados ciberdelincuentes o “hackers”. Estos realizan dichas acciones con diversos fines, principalmente para robar información, manipular los sistemas de empresas u organizaciones específicas y pedir dinero a cambio del restablecimiento de las plataformas. Los ataques cibernéticos implican la posible vulneración, pérdida o manipulación de datos, lo que trae como consecuencia un impacto negativo para quien es víctima del delito.

En 2023 los ataques cibernéticos experimentaron un incremento del 87% a nivel global, siendo China, Rusia e Irán los países mayormente afectados y el phishing el responsable del 90% de las violaciones de datos.

El phishing es uno de los ciberataques más comunes.

¿EN QUÉ CONSISTE?

Consiste en el envío de un correo electrónico por parte de un ciberdelincuente simulando ser una entidad legítima (red social, banco, institución pública, etc.)

Con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo a un usuario.

Para ello, el criminal adjunta archivos infectados o enlaces a páginas fraudulentas en el correo electrónico.

Actualmente a diario se registran 3.400 millones de correos spam, como resultado del phishing.

En Colombia se ha reportado un promedio de cuatro intentos de phishing por minuto, y se encuentra entre los cinco delitos cibernéticos con mayor materialización

De acuerdo con “Kaspersky”, empresa global de ciberseguridad y privacidad digital

RECOMENDACIONES

- Al recibir un correo electrónico, cerciórese de que conoce al remitente. Si no le parece conocido, desconfíe del mensaje. En caso contrario, revise que el correo utilizado esté escrito correctamente y que sea el mismo del que normalmente recibe los mails.
- No diligencie o entregue datos personales o información financiera a través de formularios o encuestas enviadas por correo. Las entidades bancarias o empresas no solicitan contraseñas, usuarios o información sensible de sus productos por ningún canal de comunicación.
- Evite ingresar a portales bancarios a través de hipervínculos. Por el contrario, ignore, elimine y reporte a su entidad bancaria u organización cualquier mensaje sospechoso.
  Revise si el correo contiene fallas gramaticales. Este tipo de ataques por lo general contienen errores ortográficos y vocabulario poco usual.
- No confié en nombres genéricos de asuntos del mensaje (factura, recibo, entre otros).
  Revise que los archivos adjuntos no contengan extensiones “.js”, ya que estas últimas pueden saltarse las protecciones del antivirus.
- Habilite la opción del sistema operativo que permite ver las extensiones de los archivos. De este modo, podrá comprobar si se trata de un ejecutable, un documento de texto, javascript, etc.
- Deshabilite las macros de Microsoft Office y tenga cuidado con aquellos archivos que le pidan habilitarlas.
- Si sospecha de algún enlace que venga incluido en el correo, analice el link minuciosamente.
- Recuerde mantener su sistema operativo con antivirus y aplicaciones siempre actualizadas a su última versión.
- Manténganse permanente informado respecto a las nuevas tendencias de captación de datos, suplantación u otras modalidades delictivas que se derivan del phishing, para así tener concientización de cómo actuar.
- Si considera que ha sido víctima de phishing repórtelo ante las entidades financieras, organizaciones y grupos de interés, para evitar la masificación de otros delitos como estafa, tercerización de información, suplantación de identidad, etc.