PHISHING

La estrategia en la que los atacantes envían correos electrónicos malintencionados diseñados para estafar a sus víctimas. Los ataques de phishing son correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos diseñados para manipular personas para que descarguen (malware) y que es: es un término que abarca cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo).

El término phishing (que en inglés suena igual que ´´fishing´´ que literalmente significa: pescar) se acuñó a mediados de la década de 1990, cuando los hackers comenzaron a utilizar correos electrónicos fraudulentos para pescar información de usuarios.

La idea suele ser que los usuarios revelen información financiera, números de la seguridad social, tarjetas de crédito, números de cuentas bancarias, (credenciales inicio de sesión) de cuentas personales o realicen otras acciones que los exponga a mismos internautas de la web.

Los atacantes se sirven del miedo y del sentido de la urgencia. Es común que los atacantes les digan a los usuarios que sus cuentas están restringidas o que se suspenderán si el usuario no responde al correo electrónico. El miedo logra que los usuarios víctimas ignoren las señales de advertencia más comunes un claro ejemplo de ingeniería social: una colección de técnicas que los estafadores emplean para manipular la psicología humana. Las técnicas de ingeniería social incluyen la falsificación, las mentiras y las falsas instrucciones.

Otras técnicas del phishing:

El **phishing por SMS o smishing**: es un tipo de phishing que utiliza mensajes de texto de móvil o smartphone. Los esquemas de smishing más efectivos son contextuales, es decir, relacionados con las aplicaciones o la gestión de cuentas de un smartphone. Por ejemplo, los destinatarios pueden recibir un mensaje de texto que les ofrece un regalo de 'agradecimiento' por pagar una factura de teléfono, o pedirles que actualicen la información de su tarjeta de crédito para poder continuar utilizando un servicio de streaming.

El **phishing de voz o vishing**: es un tipo de phishing que utiliza llamadas telefónicas. Gracias a la tecnología de voz sobre los estafadores pueden realizar millones de llamadas de automatizadas al día; a menudo, utilizan la suplantación de llamada entrante para que parezca que sus llamadas se realizan desde organizaciones o números locales legítimos. Las personas que responden terminan dando datos confidenciales a personas que trabajan para los estafadores; algunos

incluso llegan a darles el control remoto de sus ordenadores a los estafadores al otro lado de la llamada.

El **phishing en redes sociales**: utiliza las distintas prestaciones de una plataforma de redes sociales para obtener información confidencial de sus miembros. Los estafadores utilizan los propios servicios de mensajería de las plataformas (por ejemplo, Facebook Messenger, la mensajería de LinkedIn o Gmail, Twitter) de forma muy parecida a como utilizan los mensajes de texto o correo electrónico normales una 'mala práctica' demasiado común.

COMO EVITARLO

se anima a las organizaciones a enseñar a los usuarios cómo reconocer las estafas de phishing y a desarrollar mejores prácticas sobre cómo tratar un mensaje de texto o correo electrónico sospechoso. Por ejemplo, se puede enseñar a los usuarios a reconocer estas características a continuación:

- Solicitudes de información personal actualización de un perfil o información de pago.
- Solicitudes de envió de dinero.
- Archivos adjuntos que el destinatario no ha solicitado ni esperaba.
- Mala ortografía o gramática
- Dirección del remitente incoherente o falsificada
- Imágenes de texto utilizadas en lugar de texto (en mensajes o en páginas web vinculadas en los mensajes).
- Cargos fraudulentos en tarjetas de crédito.
- Declaraciones de impuestos realizadas a nombre de una persona
- Publicaciones falsas en redes sociales hechas en las cuentas de una persona.

Sectores más propensos a sufrir ataques tiendas en línea.

- Redes sociales.
- Bancos y otras instituciones financieras.
- Sistemas de pago (procesadoras de tarjetas).
- Compañías de telecomunicaciones.
- Compañías de envíos.

Marcas Mas Suplantadas atacadas en Google

- Microsoft, Amazon, Chase, Apple, LinkedIn, FedEx, DHL.

Esta es solo una lista parcial; desafortunadamente, los hackers siempre están ideando nuevas técnicas de phishing para evitar mejor la detección.

RECOMENDACIONES PARA NO CAER EN PHISHING

El phishing es una amenaza que afecta a todos los dispositivos por igual, ya sea una tableta, un ordenador o un móvil, y sea cual sea el sistema operativo. El sentido común es la mejor herramienta que tienes para evitar picar el anzuelo, pero también puedes protegerte.

Una buena manera de protegerse es utilizar un buen navegador web, que puede bloquear muchas de las amenazas. En un reciente análisis intentamos acceder a 600 páginas de phishing con los navegadores web más comunes entre los usuarios, pudimos comprobar que, de nuevo, los mejores navegadore en Windows son Mozilla Firefox y Microsoft Edge, que fueron capaces de bloquear más del 70% de las amenazas. Sin embargo, Google Chrome, que es el navegador más usado por los españoles, sigue siendo el que menos protección ofrece

Recurre a un antivirus, además, disponer de un buen antivirus en el ordenador también te protege. La protección que ofrece el antivirus se sumaría a la protección que ya ofrece de base el navegador web, consiguiendo un bloqueo mayor de páginas de phishing.

Proteja su teléfono celular configurando la actualización automática del programa. Estas actualizaciones podrían ofrecerle una protección crucial contra las amenazas de seguridad

Proteja sus cuentas usando un sistema de autenticación de múltiples factores. Hay algunas cuentas que ofrecen un mayor nivel de seguridad porque para iniciar la sesión en su cuenta usted tiene que ingresar dos o más credenciales. Esto se llama autenticación de múltiples factores. Las credenciales adicionales que necesita para iniciar la sesión en su cuenta se dividen en tres categorías:

Algún dato que usted conoce, como un código de acceso, un PIN o la respuesta a una pregunta de seguridad.

Algún dato que usted tiene, como un código de acceso por única vez que recibe a través de un mensaje de texto, email, aplicación de autenticación o una llave de seguridad.

Algún dato de reconocimiento personal, como un escaneo de su huella digital, retina o rostro.

Con el sistema de autenticación de múltiples factores a los estafadores que tienen su nombre de usuario y contraseña les resulta más difícil acceder a sus cuentas

Proteja sus datos haciendo copias de seguridad. Haga copias de los datos de su computadora en un disco o dispositivo externo o en la nube. También haga copias de seguridad de los datos de su teléfono.

Bibliografías:

Pagina web: https://consumidor.ftc.gov/articulos/como-reconocer-y-evitar-las-estafas-de-phishing(2023)

Pagina web: https://www.proofpoint.com/es/threat-reference/phishing(2022)