EL PHISHING

El *phishing* es un tipo de ingeniería social en la cual un ciberdelincuente se hace pasar por un colega de confianza, un conocido o una organización con el fin de manipular a su víctima a compartir información confidencial o acceso a una red privada. La carnada para este tipo de ataque puede venir en forma de un mensaje de correo electrónico, un mensaje de texto o hasta una llamada. Cuando el ciberataque se da exitosamente, el ciberdelincuente puede ganar acceso a redes privadas y afectar no solo a su víctima, sino también a terceros relacionados a esta. El resultado puede ser exfiltración de datos, pérdida de datos o servicios, fraude de identidad, infección de *malware* o *ransomware*.

La susceptibilidad al *phishing* se refiere a la probabilidad de un individuo a convertirse en víctima del *phishing*. La alta susceptibilidad aumenta la probabilidad de que un ciberdelincuente pueda aprovecharse de su blanco.

¡No seas víctima! Puedes prevenir el éxito de un ataque de *phishing* y mitigar los efectos negativos. Así funciona la técnica adversaria:

PAUSA
PIENSA
PROTEGE
TUS DATOS

El análisis y los hallazgos presentados en este documento son derivados de datos relacionados al *phishing* que fueron recolectados durante evaluaciones de CISA.

1 Seleccionan la carnada

Los ciberdelincuentes se hacen pasar por un colega de confianza, un conocido o una organización reputable para solicitar información personal o convencer a las víctimas a descargar y ejecutar *malware*. Su carnada suele ser mensajes de correo electrónico que tientan a la víctima a abrirlo. Ejemplo: mensajes con líneas de asunto que contienen alertas, una acción, o solicitan información:

- Alertas y actualizaciones sobre seguridad financiera
- Anuncios y avisos de una organización
- Alertas específicas al usuario, como avisos de entrenamientos

2 Colocan el anzuelo en su lugar

Un solo mordisco puede resultar en una explotación exitosa para el ciberdelincuente. Estos colocan numerosos anzuelos y esperan que una víctima vaya por la carnada.

8 de 10 organizaciones tienen al menos 1 individuo que fue víctima de un ataque de *phishing* orquestado por los evaluadores de CISA.

1 de 10 de los correos electrónicos con ataques de *phishing* que los evaluadores de CISA enviaron, fue abierto por usuarios que interactuaron con un enlace o archivo malicioso.

3 Agarran su pesca

El ciberdelincuente agarra a su pesca cuando un correo electrónico no es detenido por alguna herramienta de seguridad. Este alcanza a una víctima que responde con información valiosa o ejecuta un enlace o archivo malicioso. El ciberdelincuente entonces puede beneficiarse de información sensible, credenciales o accesos que puedan comprometer el dispositivo.

70% de los archivos adjuntos y enlaces con *malware* no son bloqueados por controles de seguridad en las redes, como *firewalls* y configuración de *routers*.

15% de los archivos adjuntos y enlaces maliciosos no son bloqueados por protecciones en dispositivos (ej. antivirus), los cuales existen para reducir la cantidad de actividad no deseada o maliciosa.

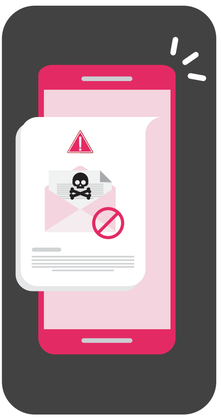
84% de empleados caen por la carnada en los primeros 10 minutos de recibir un mensaje de correo electrónico; estos respondieron con información sensible o interactuaron con un archivo adjunto o enlace malicioso.

13% de los empleados que recibieron mensajes reportaron el atentado de *phishing*. El no reportar estos ataques limita la habilidad de una organización para responder a la amenaza y advertir a otros.

PAUSA
PIENSA
PROTEGE
TUS DATOS

ACCIONES PARA EVITAR SER LA PESCA DEL DÍA

1 Bloquea la carnada

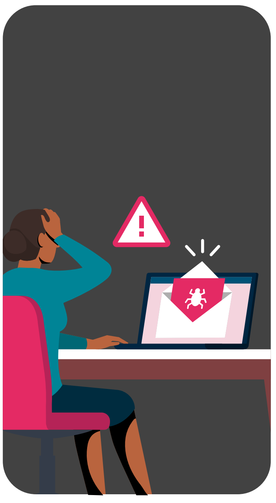


- Coordina con PRITS la implementación de EDR, Defender for Office 365, AZURE Conditional Access Policy y MFA para tu agencia. Estos controles ayudan a prevenir ataques de phishing, o a reducir su impacto, en caso de ser exitoso.
- Configura los servicios de correo electrónico a utilizar protocolos diseñados para verificar la legitimidad del origen de las comunicaciones de correo electrónico. Por ejemplo: implementación de autenticación SPF, DKIM y DMARC.
- Incorpora listas de bloqueo (*derylists*) o fuentes de inteligencia de amenazas cibernéticas a tus reglas de *firewall* para bloquear los dominios de web, URLs y direcciones IP que sean conocidamente maliciosas. Si necesitas asistencia, accede al *Service Desk* de PRITS o comunícate con nuestro equipo de ciberseguridad.

2 Rechaza la carnada

- Es importante enseñarle a los empleados a reconocer indicadores comunes del *phishing*, como un correo electrónico de un emisor sospechoso, saludos genéricos, *hyperlinks* ilegítimos, errores gramaticales o estructurales, y archivos adjuntos sospechosos.
- Educa a los empleados a que mantengan la guardia en todas sus plataformas de comunicación, incluyendo las redes sociales. Que ellos reporten toda actividad sospechosa para que esta pueda ser evaluada por un equipo de seguridad.

3 Reporta el anzuelo



- Educa a los empleados sobre qué hacer cuando reciben un mensaje de correo electrónico con *phishing*, independientemente de si ya cayeron en la trampa:
  - Reportar el mensaje de correo electrónico al equipo de seguridad apropiado.
  - No redirigir el correo electrónico malicioso a otros en la organización.
- Cuando los empleados reportan comunicaciones maliciosas, el equipo de respuesta de incidentes analiza la amenaza con intención de prevenir que el ciberdelincuente amplíe el ataque o intrusión:
  - El equipo de respuesta de incidentes puede determinar si el ataque fue un evento aislado o a nivel organizacional.
  - El equipo de respuesta de incidentes puede implementar medidas para evitar que el ataque impacte a toda la organización.

4 Protege las aguas

Luego de obtener acceso inicial por medio de un ataque de *phishing* exitoso, los ciberdelincuentes a menudo intentan tomar control de las cuentas o equipos de sus víctimas. Pueden intentar moverse lateralmente dentro de las redes de la organización. Protege la red:

- Suscríbete a los servicios gratuitos de CISA y el MS-ISAC para evaluar tus mecanismos de defensa y reducir el riesgo.
- Examina y reduce la cantidad de cuentas con acceso a datos y equipos importantes.
- Utiliza autenticación multifactorial a prueba de *phishing* para salvaguardar recursos y protegerte de ataques laterales.
- Limita quién tiene acceso a contraseñas administrativas y elimina privilegios no esenciales a usuarios para reducir la vulnerabilidad a un ciberataque.

Como última línea de defensa, siempre protege los dispositivos:

- Automatiza actualizaciones de seguridad mandatorias en los navegadores, aplicativos y antivirus de todos los equipos y dispositivos con acceso a internet.
- Implementa restricciones de *software* para solo permitir actividades laborales en los equipos y dispositivos de la organización.
- Coordina con PRITS la implementación de EDRs para proteger todos los dispositivos de tu agencia (computadoras y servidores).

PAUSA PIENSA PROTEGE TUS DATOS