# Pishing
## SUPLANTACIÓN DE IDENTIDAD

*El phishing consiste en el empleo de mensajes de correo electrónico que aparentemente provienen de fuentes fiables para llevar a cabo prácticas delictivas.*

## ¿Qué es?

El phishing es un método que los ciber delincuentes utilizan para engañar y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso.

## Principales **ARGUMENTOS** de los mensajes suplantadores

» Problemas de carácter técnico
» Detecciones recientes de fraude y necesidad de incrementar el nivel de seguridad
» Nuevas recomendaciones de seguridad
» Cambios en la política de seguridad de la entidad
» Promoción de nuevos productos
» Premios, regalos o ingresos económicos inesperados
» Accesos o usos anómalos de tu cuenta
» Inminente desactivación del servicio
» Falsas ofertas de empleo

## Principales **DAÑOS** provocados por el phishing

» Robo de identidad y datos confidenciales de los usuarios. Esto puede conllevar pérdidas económicas para los usuarios o incluso impedirles el acceso a sus propias cuentas.
» Pérdida de productividad.
» Consumo de recursos de las redes corporativas (ancho de banda, saturación del correo, etc.).

Una de las modalidades más peligrosas del phishing es el pharming. Esta técnica consiste en modificar el sistema de resolución de nombres de dominio (DNS) para conducir al usuario a una página web falsa.

Cuando un usuario teclea una dirección en su navegador, esta debe ser convertida a una dirección IP numérica. Este proceso es lo que se llama resolución de nombres, y de ello se encargan los servidores DNS.

## Principales **SERVICIOS** utilizados para este Malware

» Bancos y cajas
» Pago online (PayPal, Mastercard, Visa, etc.)
» Redes Sociales (Facebook, Twitter, Instagram, Linkedin, etc.)
» Páginas de compra/venta y subastas (Amazon, eBay, etc.)
» Juegos online
» Soporte técnico y de ayuda (helpdesk) de empresas y servicios (Outlook, Yahoo!, Apple, Gmail, etc.)
» Servicios de almacenamiento en la nube (Google Drive, Dropbox, etc.)
»Servicios de mensajería



*Los mensajes fraudulentos generalmente se generan a través de herramientas automáticas que integran funcionalidades de traducción y diccionarios de sinónimos, por lo que* ***presentan faltas ortográficas y errores gramaticales.***

## ¿Cómo Protegerme?

» La mejor forma de no ser víctima de una estafa, es NO responder solicitudes de información personal realizadas a través de correo electrónico, llamadas telefónicas o mensaje de texto.
» Al visitar sitios web, teclea directamente la dirección URL en la barra de direcciones; nunca ingreses por enlace proporcionados por algún otro sitio. Considera que las entidades bancarias utilizan certificados de seguridad y cifrados seguros.
» Revisa periódicamente tus cuentas para detectar transferencias o transacciones irregulares.
» No olvides que las entidades bancarias no solicitan información confidencial a través de canales no seguros, como el correo electrónico.
» Utiliza un filtro anti-spam.

## GLOSARIO:

**Malware:**
El término se utiliza para hablar de todo tipo de amenazas informáticas o software hostil, y existen distintos tipos de malware en función de su origen y consecuencias.

**HelpDesk:**
Recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados a las Tecnologías de la Información y la Comunicación (TIC).

**Pharming:**
Constituye otra forma de fraude en línea, muy similar a su pariente, el phishing.

**DNS:**
Es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.

## FUENTES:

**https://www.pandasecurity.com/mexico/homeusers/security-info/cybercrime/phishing/**
**https://www.avast.com/es-es/c-phishing**
**https://www.gob.mx/policiafederal/articulos/conoces-que-es-el-phishing**
**https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen**