**Tipos de phishing**

El phishing, o suplantación de identidad, es uno de los tipos más comunes de **ingeniería social**, que son técnicas de manipulación que explotan el error humano para obtener información privada, acceso u objetos de valor. Como ya aprendiste, el **phishing** es el uso de comunicaciones digitales para engañar a las personas de manera que revelen datos confidenciales o instalen software malicioso en sus equipos.

A veces, los ataques de phishing parecen provenir de una persona o empresa de confianza. Esto puede llevar a destinatarios desprevenidos a actuar en contra de su buen juicio y romper los procedimientos de seguridad. En esta lectura, aprenderás sobre las tácticas comunes de phishing que utilizan los atacantes en la actualidad.



**Los orígenes del phishing**

El phishing existe desde los primeros tiempos de Internet. Se remonta a la década de 1990, momento en que personas de todo el mundo se conectaban por primera vez. A medida que Internet se hizo más accesible, comenzó a atraer la atención de agentes de amenaza, quienes se dieron cuenta de que Internet les daba un nivel de anonimato suficiente para cometer crímenes.

**Primeras tácticas de persuasión**

Uno de los primeros casos de phishing fue dirigido a un popular servicio de chat llamado AOL Instant Messenger (AIM). Los usuarios del servicio comenzaron a recibir correos electrónicos en los que se les pedía que verificaran sus cuentas o proporcionaran información de facturación personal, y no sabían que estos mensajes eran enviados por agentes de amenaza que simulaban ser proveedores de servicios.

Este fue uno de los primeros ejemplos de phishing masivo y es una muestra de los ataques que consisten en el envío de correos electrónicos maliciosos a un gran número de personas. Este hecho aumenta la probabilidad de que alguien caiga en la trampa.

Al llevar adelante los ataques a AIM, los agentes de amenaza elaboraron cuidadosamente correos electrónicos que parecían provenir directamente de AOL. Los mensajes usaban logos, colores y fuentes oficiales para engañar a usuarios desprevenidos y lograr que compartieran su información y detalles de cuenta.

Una vez obtenida la información, los atacantes la utilizaron para crear cuentas de AOL fraudulentas que podían utilizar para llevar a cabo otros delitos de forma anónima. Debido al ataque, AOL se vio obligada a adaptar sus políticas de seguridad para hacer frente a estas amenazas. Por ejemplo, el servicio de chat comenzó a incluir mensajes en sus plataformas que advertían a los usuarios sobre los ataques de phishing.

**Cómo evolucionó el phishing**

El phishing continuó evolucionando a principios de siglo, a medida que las empresas y las nuevas tecnologías fueron ingresando al mundo digital. A principios de la década de 2000, el comercio electrónico y los sistemas de pago en línea comenzaron a convertirse en alternativas cada vez más masivas. La incorporación de las transacciones en línea presentó nuevas oportunidades para que los atacantes cometieran delitos.

Fue durante este período que comenzaron a aparecer varias técnicas, muchas de las cuales se siguen usando en la actualidad. Entre ellas, hay cinco tipos comunes de phishing que todo analista de seguridad debe conocer.

* El **phishing por correo electrónico** es un tipo de ataque en el que los agentes de amenaza envían correos electrónicos en los que se hacen pasar por una persona o entidad de confianza.
* El **smishing** es un tipo de phishing que utiliza el servicio de mensajes cortos (SMS) y demás servicios de mensajería de texto como los iMessages de Apple, WhatsApp y otros medios de chat en teléfonos móviles.
* El **vishing** consiste en el uso de llamadas de voz o mensajes de voz para engañar a los objetivos de modo que proporcionen información personal.
* El **phishing localizado**, ospear phishing, es una subcategoría del phishing por correo electrónico que hace foco en personas específicas, como los contadores de una pequeña empresa.
* El **ataque de caza de ballenas**, o whaling, es una categoría de phishing localizado dirigido a ejecutivos de alta jerarquía en una organización.

Desde los comienzos del phishing, los ataques por correo electrónico siempre han sido los más comunes. Si bien en un principio se usaban para engañar a las personas, a fin de que compartieran credenciales de acceso e información de tarjetas de crédito, luego el phishing por correo electrónico se convirtió en un método popular para infectar sistemas informáticos y redes con software malicioso.

A finales de 2003, atacantes de todo el mundo crearon sitios web fraudulentos que se parecían a los de empresas como eBay y PayPal™. También se lanzaron campañas masivas de phishing dirigidas a sitios bancarios y de comercio electrónico, mediante las cuales se distribuían programas maliciosos.



**Tendencias recientes**

A partir de la década de 2010, los atacantes comenzaron a abandonar el phishing masivo, que consistía en atraer a personas desprevenidas a una trampa, y empezaron a implementar lo que se conoce como“intentos de phishing dirigidos”, apoyándose en las nuevas tecnologías. El phishing dirigido tiene como particularidad que los ataques se envían a objetivos específicos mediante métodos altamente personalizados, para crear una intensa sensación de familiaridad.

Un tipo de phishing dirigido que evolucionó en la década de 2010 es el **angler phishing**, una técnica en la que los atacantes se hacen pasar por representantes de servicio al cliente en redes sociales. Esta táctica evolucionó a partir de la tendencia de las personas a dejar sus quejas a las empresas, en línea. Aprovechando esto, los agentes de amenaza interceptan quejas de lugares como tableros de mensajes o secciones de comentarios y contactan, a través de redes sociales, a la persona enojada. Al igual que en el caso de los ataques de AIM de la década de 1990, usan cuentas fraudulentas que parecen similares a las de empresas reales. Luego, engañan a los clientes enojados hasta convencerlos de que compartan información confidencial, con la promesa de resolver su problema.

**Conclusiones clave**

Las tácticas de phishing fueron volviéndose cada vez más sofisticadas a lo largo de los años. Lamentablemente, no existe una solución perfecta que evite que estos ataques ocurran. Hoy, algunas tácticas como el phishing por correo electrónico, que comenzó en el siglo pasado, siguen siendo un método efectivo y rentable de ataque para los delincuentes en línea.

Si bien no hay una solución tecnológica que pueda prevenir el phishing por completo, existen muchas maneras de reducir el daño cuando estos ocurren. Una es concientizar e informar. Como profesional de la seguridad, es posible que una de tus responsabilidades sea ayudar a otras personas a identificar formas de ingeniería social como el phishing. Por ejemplo, puedes crear programas de capacitación que informen a los empleados sobre este tema. Compartir tu conocimiento con otras personas es una responsabilidad importante que ayuda a construir una cultura de la seguridad.

**Recursos para obtener información adicional**

Mantenerte al corriente sobre las amenazas de phishing es una de las mejores medidas que puedes tomar para capacitarte y ayudar a tu organización a tomar decisiones de seguridad más inteligentes.

* El [test de phishing de Google](https://phishingquiz.withgoogle.com/) es una herramienta que puedes usar o compartir y que ilustra lo difícil que puede ser identificar estos ataques.
* [Phishing.org](https://www.phishing.org/) informa sobre las últimas tendencias de phishing y comparte recursos gratuitos que pueden ayudar a reducir los ataques de phishing.
* El [Anti-Phishing Working Group (APWG)](https://apwg.org/) es un grupo sin fines de lucro de expertos en seguridad de distintas disciplinas, que publica un informe trimestral sobre las tendencias de phishing.