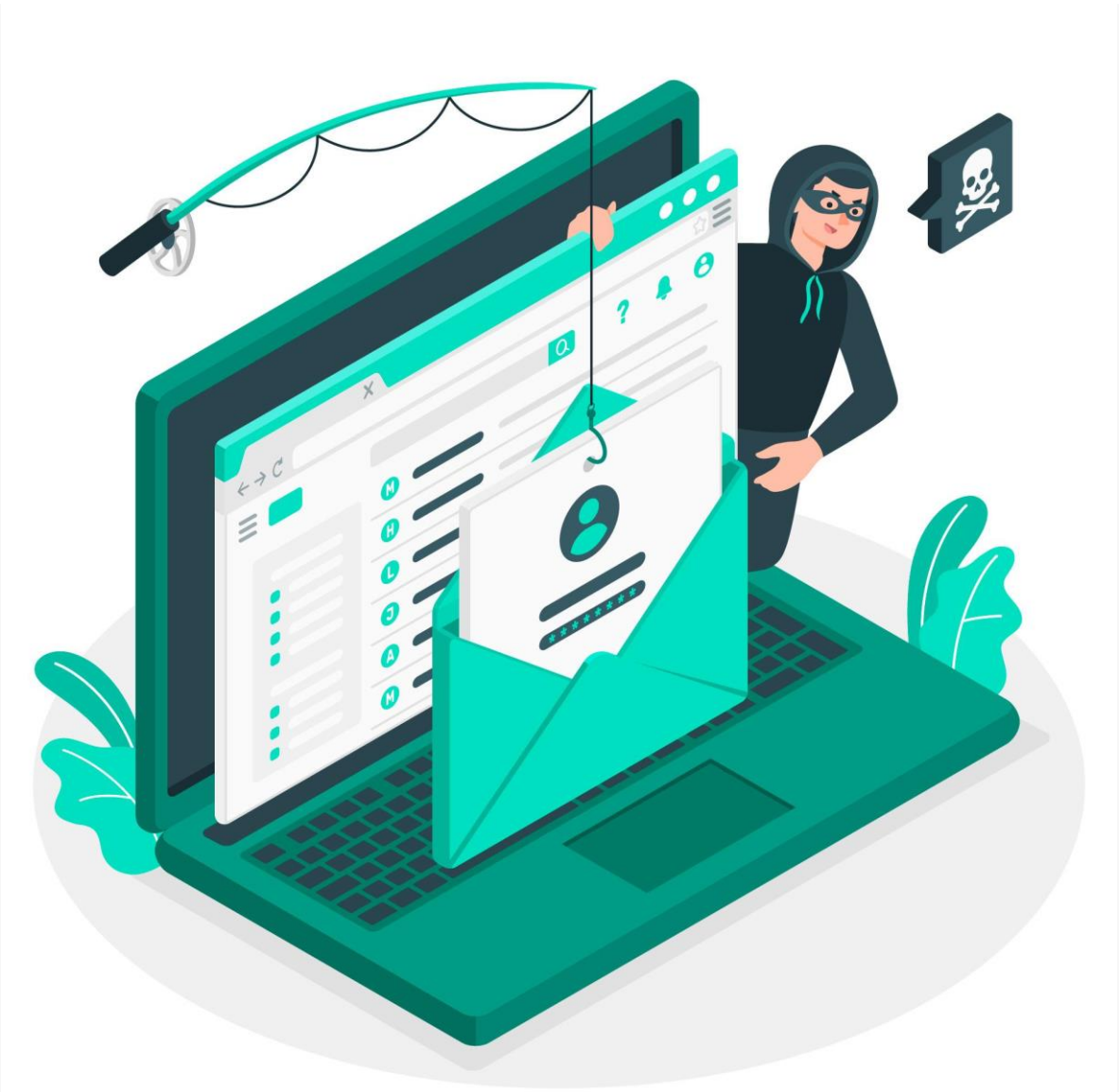
-HABLEMOS DE PHISHING-



¿Qué es phishing?

Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de phishing que es la más común. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita (o “suplanta su identidad”) a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con

la intención de debilitar su buen juicio al infundirle miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia.

Si un usuario pica el anzuelo y hace clic en el enlace, se le envía a un sitio web que es una imitación del legítimo. A partir de aquí, se le pide que se registre con sus credenciales de nombre de usuario y contraseña. Si es lo suficientemente ingenuo y lo hace, la información de inicio de sesión llega al atacante, que la utiliza para robar identidades, saquear cuentas bancarias, y vender información personal en el mercado negro.

El phishing es la forma más sencilla de ciberataque y, al mismo tiempo, la más peligrosa y efectiva.

Historia del phishing

El origen del nombre “phishing” es fácil de rastrear. El proceso de llevar a cabo una estafa de phishing es muy similar al de la pesca (“fishing” en inglés). Se prepara el anzuelo pensando en engañar a una víctima, y luego se lanza y se espera a que pique. En cuanto al dígrafo “ph” en sustitución de “f,” podría ser el resultado de la combinación de las palabras inglesas “fishing” y “phony,” pero algunas fuentes apuntan a otro posible origen.

En los años 70, se formó una subcultura en torno a los ataques de baja tecnología para explotar el sistema telefónico. Estos primeros hackers se llamaban “phreaks”, una combinación de las palabras inglesas “phone” (teléfono) y “freak” (raro, friqui). En una época en la que no había demasiados ordenadores en red que hackear, el phreaking era una forma común de hacer llamadas gratuitas de larga distancia o llegar a números que no salían en los listines.

Incluso antes de que arraigara el término “phishing”, se describió en detalle una técnica de phishing en una presentación del Grupo Internacional de Usuarios HP, Interex, en 1987.

La creación del término se atribuyó a un conocido spammer y hacker de mediados de los años 90, Khan C Smith. Asimismo, según los registros de Internet, la primera vez que se utilizó públicamente la palabra phishing y quedó registrado fue el 2 de enero de 1996. La mención ocurrió en un grupo de noticias Usenet denominado AOHell. En ese momento, America Online (AOL) era el proveedor número uno de acceso a Internet, con millones de conexiones diarias.

Naturalmente, la popularidad de AOL la convirtió en blanco de los estafadores. Los hackers y piratas informáticos la utilizaron para comunicarse entre sí, así como para realizar ataques de phishing contra usuarios legítimos. Cuando AOL adoptó medidas para cerrar AOHell, los atacantes recurrieron a otras técnicas. Enviaban mensajes a los usuarios de AOL afirmando ser empleados de esta compañía y les pedían que verificaran sus cuentas y facilitaran la información de facturación. Con el tiempo, el problema creció tanto que AOL añadió advertencias en todos los programas cliente de correo electrónico y mensajería instantánea indicando que “nadie que trabaje en AOL le pedirá su contraseña o información de facturación”.

Tipos de ataques de phishing

A pesar de sus muchas variedades, el denominador común de todos los ataques de phishing es el uso de un pretexto fraudulento para adquirir datos valiosos. Algunas categorías principales incluyen:

Spear phishing

Mientras la mayoría de las campañas de phishing envían correos electrónicos masivos al mayor número posible de personas, el spear phishing es un ataque dirigido. Spear phishing ataca a una persona u organización específica, a menudo con contenido personalizado para la víctima o víctimas. Requiere un reconocimiento previo al ataque para descubrir nombres, cargos, direcciones de correo electrónico y similares. Los hackers buscan en Internet para relacionar esta información con lo que han averiguado sobre los colegas profesionales del objetivo, junto con los nombres y las relaciones profesionales de los empleados clave en sus organizaciones. Con esto, el autor del phishing crea un correo electrónico creíble.

Por ejemplo, un estafador podría crear un ataque de spear phishing a un empleado cuyas responsabilidades incluyen la capacidad de autorizar pagos. El correo electrónico aparenta proceder de un ejecutivo en la organización, que exige al empleado que envíe un pago sustancial al ejecutivo o a un proveedor de la empresa (cuando en realidad el enlace del pago malicioso lo envía al atacante).

Phishing de clonación

En este ataque, los delincuentes hacen una copia, o clonan, correos electrónicos legítimos enviados anteriormente que contienen un enlace o un archivo adjunto. Luego, el autor del phishing sustituye los enlaces o archivos adjuntos con contenido malicioso disfrazado para hacerse pasar por el auténtico. Los usuarios desprevenidos hacen clic en el enlace o abren el adjunto, lo que a menudo permite tomar el control de sus sistemas. Luego el autor del phishing puede falsificar la identidad de la víctima para hacerse pasar por un remitente de confianza ante otras víctimas de la misma organización.

Phishing telefónico

Con los intentos de phishing a través del teléfono, a veces llamados phishing de voz o “vishing,” el phisher llama afirmando representar a su banco local, la policía o incluso la Agencia Tributaria. A continuación, le asustan con algún tipo de problema e insisten en que lo solucione inmediatamente facilitando su información de cuenta o pagando una multa. Normalmente le piden que pague con una transferencia bancaria o con tarjetas prepago, porque son imposibles de rastrear.

Phishing vía SMS, o “smishing,” es el gemelo malvado del vishing, que realiza el mismo tipo de estafa (algunas veces con un enlace malicioso incorporado en el que hacer clic) por medio de un mensaje de texto SMS.

¿Cómo protegerse del phishing?

Como se ha indicado previamente, el phishing es una amenaza que ofrece “igualdad de oportunidades”, capaz de aparecer en ordenadores de escritorio, portátiles, tabletas y teléfonos inteligentes. La mayoría de los navegadores de Internet disponen de formas de comprobar si un enlace es seguro, pero la primera línea de defensa contra el phishing es su buen criterio. Aprenda a reconocer los signos del phishing e intente practicar informática segura siempre que compruebe su correo electrónico, lea posts de Facebook, o juegue a su juego online favorito.

Una vez más, nuestro Adam Kujawa propone algunas de las prácticas más importantes para mantenerse a salvo:

- No abra correos electrónicos de remitentes que no le sean familiares.

- No haga clic en un enlace dentro de un correo electrónico a menos que sepa exactamente a dónde le lleva.

- Para aplicar esa capa de protección, si recibe un correo electrónico de una fuente de que la que no está seguro, navegue manualmente hasta el enlace proporcionado escribiendo la dirección legítima del sitio web en su navegador.

- Busque el certificado digital del sitio web.

- Si se le pide que proporcione información confidencial, compruebe que la URL de la página comienza con “HTTPS” en lugar de simplemente “HTTP”. La “S” significa “seguro”. No es una garantía de que un sitio sea legítimo, pero la mayoría de los sitios legítimos utilizan HTTPS porque es más seguro. Los sitios HTTP, incluso los legítimos, son vulnerables para los hackers.

- Si sospecha que un correo electrónico no es legítimo, seleccione un nombre o parte del texto del mensaje y llévelo a un motor de búsqueda para ver si existe algún ataque de phishing conocido que utiliza los mismos métodos.

- Pase el cursor del ratón por encima del enlace para ver si es legítimo.

- Como siempre, recomendamos utilizar algún tipo de software de seguridad antimalware. La mayoría de las herramientas de seguridad informática tienen la capacidad de detectar cuando un enlace o un archivo adjunto no es lo que parece, por lo que incluso si llega a caer en un intento inteligente de phishing, no terminará compartiendo su información con las personas erróneas.