Phishing

¿Qué es y cómo podemos evitarlo?

En esta entrada, queremos hablarte sobre el Phishing, una técnica muy dañina llevada a cabo de forma digital y utilizada para robar información a través de engaños.

En los últimos tiempos se viene hablando mucho de esta práctica, debido a las grandes pérdidas económicas que ya causó y al aumento del número de víctimas . Por eso, te vamos a explicar en qué consiste exactamente el phishing y dejarte algunos consejos que podés aplicar para evitar caer en este tipo de engaño.

¿Qué es el Phishing?

Phishing es el delito de engañar a las personas en el mundo digital para que compartan información confidencial, como por ejemplo contraseñas de correos personales o aplicaciones, cuentas bancarias, número de tarjetas de crédito, etc. Normalmente se lleva a cabo a través del envío de correos electrónicos, dentro de los cuales hay enlaces maliciosos que llevan a las personas a revelar datos.

El origen del término “phishing” se encuentra en la palabra en inglés “fishing” que significa “pescar”. Se usa esta palabra porque la finalidad de este tipo de engaños es justamente “pescar” a personas a través de internet para que revelen información confidencial; es decir, se intenta que “agarren el anzuelo”. Empieza con las letras “ph” para denotar que la estafa se lleva a cabo en el entorno digital, ya que los primeros hackers eran conocidos como phreaks.

¿Cómo funciona?

El phishing es una técnica relativamente simple, pero muy efectiva. En palabras de Adam Kujawa, experto en ciberseguridad, “el phishing es la forma más sencilla de ciberataque y, al mismo tiempo, la más peligrosa y efectiva. Eso se debe a que ataca la computadora más vulnerable y potente del planeta: la mente humana”.

En general, las víctimas reciben un correo electrónico de una persona u organización aparentemente de confianza, como un banco, ONG, entidad pública o alguna otra organización, pero que en realidad provienen de una persona o grupo con intenciones de robar información. Después, cuando la víctima abre el correo electrónico encuentra un mensaje especialmente construido para que pueda, impulsado por sus emociones y la urgencia del mensaje, hacer clic en un botón de acción, imagen o enlace incluidos dentro del correo.

Si la persona pica el anzuelo y hace clic en el enlace, es llevado hasta una página web muy similar a la de la organización que se está imitando, al punto de parecer legítima, en donde se le intentará sacar información sensible. En esta web se le pide que se siga unos pasos, como por ejemplo que se ingresen datos personales, credenciales de nombre de usuario y contraseña o alguna otra información sensible de sus cuentas. Si el usuario cumple con los pasos, la información que ingresó llega al atacante y él lo utiliza para robar identidades, vaciar cuentas bancarias, vender información personal, etc.

Algunos ejemplos de mensajes en correos de phishing

- Anuncios de que se resultó **ganador de un sorteo** y que se tiene que ingresar en el enlace para reclamar el premio.
- Correos de **entidades financieras solicitando datos** sensibles poder seguir usando la cuenta
- Mensajes **solicitando que se pague una deuda** para evitar que se cancele cierto servicio
- **Mensajes de soporte técnico** para informar supuestas irregularidades

¿Cómo identificar correos de phishing?

Una forma bastante efectiva de evitar caer en este tipo de estafas es identificando los correos maliciosos. Podemos hacer esto analizando el formato de los correos que nos llegan y viendo si cumplen alguna de estas características

- **Contiene faltas ortográficas:** los correos de phishing por lo general están mal escritos y contienen varias faltas ortográficas.
- **Incluye urgencias o amenazas:** en este tipo de correos se pide a la persona que realice cierta acción de forma inmediata, ya sea para evitar un inconveniente o para obtener algo exclusivo.
- **Tienen un aspecto visualmente sospechoso:** el correo en general se ve poco profesional, los logos están pixelados o desproporcionados.
- **Incluye enlaces mal escritos y no tienen certificado de seguridad:** los enlaces tienen faltas ortográficas y no empiezan con “https”, que indica que la conexión en una página es segura.
- **Remitente desconocido y dirección de correo inapropiado:** el remitente usa una dirección de correo particular (@gmail, @hotmail.), y no una corporativa que incluya el nombre de la organización desde la cual supuestamente se comunican. Así también envían el correo de forma masiva y usan copia oculta.
- **Se solicitan datos personales sensibles:** en este tipo de correos se solicitan datos personales sensibles, como contraseñas, nombres de usuarios, números de cuenta o tarjetas, etc.

¿Qué podemos hacer para evitar caer en el phishing?

Estos son algunos consejos que podés seguir para evitar caer en este tipo de engaños:

Revisá semanalmente tus cuentas bancarias para identificar algún movimiento que no realizaste

Cada cierto tiempo cambiá tus contraseñas y hacelas seguras

No cargues datos sensibles en páginas que no sean 100% confiables y seguras.

Instalá un antivirus y mantenelo actualizado

Analizá siempre las características de los correos que te llegan, para ver si son confiables

Y si ya caí en un engaño por phishing, ¿qué puedo hacer?

Muchas veces caer en engaños es inevitable. Si fuiste víctima de phishing es importante que mantengas la calma y actúes lo más rápido posible.

- Algunas medidas que podés llevar a cabo en situaciones así son:
- Identificá qué información es la que expusiste, de modo a conocer la gravedad de la situación y saber cómo actuar.
- Inmediatamente cambiá la contraseña del servicio afectado, cancelá la suscripción si hay alguna relacionada o bloquea tu tarjeta en caso de que corresponda.
- Ponete en contacto con la empresa u organización que está siendo suplantada para informarles de la situación.
- Si el caso amerita, denunciá la situación a las autoridades. En Paraguay podés acudir a la Unidad Especializada de Delitos Informáticos del Ministerio Público.
- Hacé uso de las redes sociales para comentar sobre el caso de phishing y así evitar que otras personas sean víctimas.

La prevención es la clave

Siempre tenemos que cuestionar el origen de todos los mensajes o correos sospechosos que nos llegan. Por ejemplo, si el correo es de un banco debemos hablar con nuestro oficial de cuentas para corroborar que sea un pedido real de la entidad.

Somos parte de un mundo cada vez más digital. La tecnología nos facilita la vida en muchísimos aspectos y nos permite hacer cosas rápidamente y desde donde estemos. El peligro siempre va a estar presente y de nosotros depende ser precavidos y responsables para evitar ser víctimas de situaciones desagradables.

Desde Vaquita estamos comprometidos a brindarte siempre servicios financieros sencillos, modernos y, sobre todo, seguros. Te invitamos a suscribirte al blog y a compartir la información con tus amigos para seguir aprendiendo juntos sobre este y otros temas.