Qué es el phishing y cómo protegerse

Seguro que alguna vez en los últimos meses has recibido en tu buzón de correo electrónico algún mensaje enviado por alguna empresa conocida (sobre todo de entidades bancarias) que realmente no es lo que dicen ser. Este tipo de envíos con la intención de engañar al usuario es lo que se conoce popularmente con el nombre de phishing o suplantación de identidad, un tipo de ataque que puede causar muchos problemas si no se toman las medidas de seguridad adecuadas.

Qué es el phishing

El phishing es una de las modalidades de estafa más utilizadas en la actualidad por los atacantes para intentar conseguir datos de gran importancia del usuario como su número de tarjeta de crédito, o cualquier información que después pueda ser utilizada de forma fraudulenta.

El estafador, conocido habitualmente con el nombre de phisher, hace uso de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de total confianza y contactando mediante algún formato electrónico, generalmente un email idéntico al que suelen enviar esos contactos de confianza. Si la persona que recibe estos correos no tiene ciertos conocimientos, no será capaz de detectar que se trata de un fraude.

En estos mensajes se suele informar al usuario que tiene que entrar en una url para indicar de nuevo sus datos o algo similar, pero realmente, donde estamos entrando es a una dirección web totalmente falsa, en la que lo único que conseguiremos será proporcionar nuestra información al atacante.

Tradicionalmente el phishing está asociado al mundo del correo electrónico, pero además de esta vía, también se puede dar por otros medios como las redes sociales, llamadas telefónicas, el envío de SMS/MMS o incluso el uso del correo postal.

Cómo funciona el ataque mediante la suplantación de identidad

El funcionamiento de este tipo de ataques para conseguir información relevante del usuario es muy sencillo. Lo primero que hace el atacante es crearse una apariencia de un ente de confianza.

El siguiente paso sería realizar el envío de los mensajes por algún medio de propagación, mensajes que irán destinados a miles de usuarios. Entre estos usuarios, habrá un cierto porcentaje que se fiarán del mensaje y seguirán las instrucciones que indique el mensaje. Hecho esto, el usuario habrá proporcionado información de gran valor al atacante. Las consecuencias de esto principalmente es:

- **Robo de dinero de la cuenta bancaria.**
- **Uso indebido de las tarjetas de crédito.**
- **Envío de publicidad en su nombre.**
- **Suplantación de identidad.**

Cómo detectar el phishing

Cuando recibimos un correo que pensamos que puede tratarse de un correo de suplantación de identidad, podemos fijarnos en varios aspectos para corroborar si se trata de un email bueno o de una estafa. Estos puntos son:

- **Revisar el campo "De" del correo:** En este campo es donde aparece la información de quién envía el mensaje. Si aquí aparece una dirección que no coincide con la empresa que envía el email, ya es un punto a favor para desconfiar de él. La pega es que este campo es fácilmente manipulable y en este tipo de correos suele aparecer una dirección que coincide con el dominio que con el que aparece en el mensaje.
- **Enlaces:** Si en el cuerpo del mensaje apareciese algún tipo de enlace, nos situaríamos encima de él sin hacer ningún clic. Ya sea en la parte inferior de nuestro programa de mail o bien mediante una pequeña ventana emergente, veremos la url hacia donde nos llevará ese enlace. Si esa dirección es extraña y no coincide con el contenido del email, entonces podemos afirmar que se trata de un correo phishing.

- **Faltas de ortografía:** Es muy importante que estemos pendiente de la información que contiene el email y detectar si incluye algún tipo de falta de ortografía o incongruencias gramaticales. De ser así, es un motivo más para desconfiar del correo.
- **Idioma no habitual**: si la empresa nos contacta en otro idioma al habitual, recibimos un correo de alguien en el extranjero o uno de nuestros conocidos nos escribe en otro idioma, también debemos sospechar.
- **Adjuntos**: si desconoces al remitente no conviene descargar los adjuntos, y si lo haces pasa el antivirus antes de abrirlos.

Consejos para protegerse del phishing

Como sucede ante toda situación en la que estamos expuestos a ser timados, lo primero de todo es hacer uso de nuestro sentido común. Si algo vemos que no nos termina de cuadrar, mejor ignorarlo que caer en las garras del atacante.

Además de lo que hemos dicho, es interesante tener presente siempre los siguientes consejos, muchos de los cuales estaréis cansados de escuchar.

1. No dar ningún tipo de datos bancarios nuestros por email. Las entidades nunca utilizan este canal para solicitar esta información, además de tratarse de datos a los que ellos ya tienen acceso desde sus equipos.
2. Ante cualquier duda debemos contactar con nuestra entidad o empresa para asegurarnos que realmente son ellos quienes han enviado esos correos.
3. Verificar que la página a la que se accede cuando se pulsa en los enlaces que llevan esos correos hace uso de un certificado de seguridad (https), ya que será síntoma de que la información enviada va encriptada.
4. Ante cualquier duda sobre un correo, lo mejor es ignorar ese mail y eliminarlo de nuestra bandeja de entrada.
5. Si pensamos que hemos sido víctimas de un phishing, ponerse en contacto con nuestra entidad y cambiar todas las claves que utilicemos.

Aunque el phishing sea uno de los mecanismos más utilizado para intentar captar la información privada del usuario, siguiendo estas simples recomendaciones y haciendo uso de nuestro sentido común evitaremos que roben nuestros datos.