Phishing

¿Qué se entiende por phishing?

El phishing es una técnica de captación ilícita de datos personales (principalmente relacionados con claves para el acceso a servicios bancarios y financieros) a través de correos electrónicos o páginas Web que imitan/copian la imagen o apariencia de una entidad bancaria/financiera (o cualquier otro tipo de empresa de reconocido prestigio).

En términos más coloquiales, podemos entender el phishing como “pescando datos” o “pesca de datos”, al asimilar la fonética de la palabra “phishing” con el gerundio “fishing” (≈ pescando).

¿Cómo funciona el phishing?

La técnica del phishing utiliza el correo electrónico para ponerse en contacto con los usuarios, utilizando mensajes que imitan, casi a la perfección, el formato, lenguaje y la imagen de las entidades bancarias/financieras, y que siempre incluyen una petición final en la solicita a los usuarios la “confirmación” de determinados datos personales alegando distintos motivos: problemas técnicos, cambio de política de seguridad, posible fraude, etc.

Estos mensajes de correo electrónico siempre incluyen enlaces que conducen “aparentemente” a las páginas Web oficiales de las citadas entidades pero que, en realidad, remiten a “páginas Web piratas” que imitan o copian casi a la perfección la página Web de la entidad financiera, siendo su finalidad principal captar datos de los usuarios.

Dada la confianza que los usuarios tienen depositada en las entidades de las que son clientes, y por desconocimiento o simplemente ante la incertidumbre y temor creados, acceden a dichas páginas Web piratas, donde el defraudador o delincuente informático, obtiene los datos personales o claves de acceso personales.

Es a partir de este momento donde empieza el fraude:

1. Utilización del número de tarjeta y fecha de caducidad para compras por Internet (comercio electrónico).

2. Realización de transferencias bancarias no consentidas ni autorizadas.

3. Retirada de efectivo en cajeros con duplicados de las tarjetas.

Aspectos a tener en cuenta para evitar el phishing:

1.- Sospeche de cualquier correo electrónico con solicitudes urgentes de información personal, que utilice argumentos como:

-Problemas de carácter técnico.

-Detecciones de posibles fraudes.

-Cambio de política de seguridad.

-Promoción de nuevos productos y/o servicios.

-Premios, regalos, concursos, etc.

Además, este tipo de correos suele incorporar advertencias tales como: “si no realiza la confirmación/cambio solicitada, en el transcurso de --- horas/días se procederá al bloqueo/cancelación, de su cuenta bancaria/cuenta de cliente, etc...”; de forma que se fuerza una respuesta casi inmediata del usuario.

Dado que el phishing es una técnica de envío masivo de correos electrónicos a múltiples usuarios, es posible que reciba correos electrónicos de entidades o empresas de las que usted no es cliente, y en los que se solicita igualmente dichos datos. En estos casos, directamente, descártelos.

2.- Sospeche de los correos electrónicos que le soliciten información como: nombre de usuario, password o clave de acceso, número de tarjeta de crédito, fecha de caducidad, número de la seguridad social, etc.

3.- Los mensajes de correo electrónico de phishing no suelen estar personalizados, mientras que los mensajes de las entidades de las que somos clientes suelen estar personalizados.

4.- Evite rellenar formularios en correos electrónicos que le soliciten información financiera personal.

5.- No utilice los enlaces incluidos en los correos electrónicos que conducen “aparentemente” a las entidades, especialmente si sospecha que el mensaje podría no ser auténtico. Diríjase directamente, a través de su navegador, a la página Web de la entidad o empresa.

6.- Antes de facilitar cualquier dato sensible (datos bancarios, números de tarjetas de crédito, número de la seguridad social, etc.) asegúrese de que se encuentra en una Web segura.

Las páginas Web que utilizan protocolos de seguridad, que impiden la captación de datos por parte de terceros no autorizados, se caracterizan porque la dirección Web que aparece en la barra de navegación comienza con el protocolo “https” y en la parte inferior de la página aparece un candado.

Igualmente podemos comprobar la veracidad del protocolo de seguridad; para ello, podemos clickear dos veces en el candado de la parte inferior de la página, y nos aparecerá una ventana en la que se identifica a la compañía de certificación y al titular del protocolo, así como su validez.

7.- Asegúrese de tener el navegador Web actualizado y con los últimos parches de seguridad instalados.

8.- Si continua teniendo dudas acerca de la veracidad del correo electrónico, de su emisor o de su finalidad, no dude en ponerse en contacto con la entidad de la que es cliente.

9.- Por último, compruebe regularmente sus cuentas bancarias para asegurarse que todos los movimientos o transacciones son legítimos. En caso de detectar algo sospechoso, no dude en ponerse en contacto con su entidad bancaria.

¿Qué se puede hacer si se detecta el phishing o hemos sido defraudados a través de esta técnica?

En ambos casos, la mejor solución es denunciarlo directamente a la entidad bancaria de la que es cliente, así como a la policía (principalmente a la Brigada de Investigación Tecnológica – BIT – www.mir.es/policía/bit/index.htm).

Ambas, pondrán todos los medios a su disposición para la búsqueda y captura de los autores, así como para restituir los daños que le hayan podido ser ocasionados.

Fuente Microsoft.com