PHISHING

Una de las amenazas más frecuentes en la web es el phishing. El término phishing viene del inglés fishing, que se pronuncia igual y que significa pescar. En este caso no se pescan peces, sino datos personales como nombres de usuario, contraseñas o datos de cuentas bancarias.

Este incidente tiene dos caras:

Podemos recibir un email, una llamada telefónica o un mensaje, con el que intentarán robarnos los datos personales, es decir, seremos los «pescados».

Un sitio web puede ser atacado para suplantarse por otra entidad y enviar correos maliciosos como phishing, con los que se quiere robar datos personales de usuarios o clientes de la entidad suplantada, es decir seremos «la caña del pescador».

Bajo el nombre de phishing se conoce por una parte a la **estafa** que podemos sufrir, generalmente a través de un mensaje fraudulento de correo electrónico, con el que el ciberdelincuente pretende capturar de forma ilícita nuestros datos personales: como contraseñas de acceso a nuestros sistemas o datos de nuestras cuentas bancarias.

Y también se denomina así al **ataque** que podríamos sufrir en **nuestro sitio web**, que consiste en suplantar a una entidad para redirigir a los usuarios a mensajes fraudulentos, que podrían ser enviados desde la misma página suplantada.

Para hacer frente a esta amenaza, en su empresa debe:

- Proteger su sitio web para impedir que sea objeto de este tipo de ataques.
- Concientizar a los usuarios para evitar que **«piquen»** en el anzuelo del email fraudulento y prevenir que entreguen información sensible como contraseñas de acceso a sistemas, a sitios web o a cuentas bancarias.

El «enganche» de estos mensajes suele ser su remitente, que posee un aspecto similar a un correo legítimo, acompañado de un tono de urgencia, adulador o amenazante.

Todas estas son técnicas de ingeniería social y sólo podemos hacerles frente mediante la prevención y capacitación. Usualmente, el **"gancho"** viene en forma de enlace o archivo a descargar. Estos enlaces podrían iniciar la descarga de malware o llevarnos a páginas en las que nos pedirán nuestras credenciales. Por su parte, los archivos adjuntos podrían contener malware o programas descargables. En ambos casos, si hacemos clic estamos muy cerca de quedar atrapados. Aprenda a identificar las páginas fraudulentas. Y si descarga un fichero o archivo por error, lo mejor será eliminarlo.

central 2511-5000
ci5000@ucr.ac.cr
www.facebook.com/ciucr/
twitter.com/ciucr
UNIVERSIDAD DE COSTA RICA
CI
Centro de **Informática**