http://www.radialistas.net/clip.php?id=1400318

CAPACITACIÓN Fraude electrónico

RESUMEN
Ojala nunca te hayan pescado con el anzuelo del fraude en Internet.

¡TE PESCARON!

Los farsantes pescadores que cada día salen a la web para atrapar incautos pescaditos están al acecho. ¡Y cada día hay más practicando el “phishing”!

“Phishing” es una palabra relativamente nueva que viene del verbo inglés fish, que significa pescar.

¿Cómo pescan estos ciberdelincuentes? Muy sencillo.

Los pescadores del fraude lanzan sus anzuelos a Internet en forma de supuestos emails de un banco. En ellos solicitan, con cualquier excusa, las claves de acceso a la cuenta.

El confiado pescado muerde la carnada, se creé el mail y responde o entra en la página web que le indican, facilitando los datos al ladronzuelo que al instante le desvalija la cuenta.

Seguro que has recibidos cientos de estos mails, pero ojala nunca te hayan enganchado con el anzuelo del fraude en Internet.

De todas formas, no serías el primero, ni la última. Muchos han sido pescados.

Te estarás preguntando si el negocio es rentable. Sí, y mucho. Este tipo de pesca se asemeja más a lanzar una red que una caña de pescar.

El envío es masivo e indiscriminado. A veces le correo le llega a gente que no tiene cuenta en ese banco. Pero como se envían millones de correos, con que 100 incautos piquen ya es ganancia.

Supongamos que a cada uno le roban 1.000$. Estamos hablando de cien mil dólares, y podríamos seguir multiplicando.

Por eso es importante estar alerta y tomar precauciones para no caer en la trampa.

1. Ningún banco envía correos electrónicos solicitando claves o datos de las cuentas.

Por lo general, sólo mandan promociones de servicios o confirmaciones de pagos y transacciones.

Por eso, nunca respondas ningún correo que te manden pidiendo información privada ni entres a páginas donde te soliciten estos datos.

2. Las compañías y bancos más suplantados para el "phishing" son la página de compras en Internet eBay, la empresa de pagos en línea PayPal y bancos como el Citibank, BBVA, Caja Madrid, Banco de Venezuela, Bank of América…

Desconfía de todos los mails que tengan este origen.

3. Si sospechas que el correo electrónico recibido del banco es cierto, primero llámales y confirma que es un correo verdadero y que realmente te solicitan alguna información.

Pero llama a los números que vienen en la guía telefónica, porque hay una nueva modalidad de "phishing" llamada "vishing".

En el falso email te indican que llames a un número telefónico "gratuito" por algún problema en la tarjeta de crédito o en la cuenta bancaria.

Una vez que muerdes este anzuelo y llamas, solicitarán tus datos privados para suplantar tu identidad y extraer tu dinero de la cuenta o hacer compras en Internet con tu tarjeta.

4. La mayor parte de estos correos no están personalizados con tu nombre, ya que son correos enviados masivamente.

Si alguna vez tu banco se pusiera en contacto contigo, de seguro personalizaría el correo con tu nombre.

5. Las páginas que usan los bancos para operaciones en línea, o las páginas para pagos en Internet, son sitios seguros. Estas direcciones, si te fijas en la barra del navegador, empiezan por "https" y en la parte de abajo aparece un candadito. (*Imagen*)

Navegadores como Firefox, te avisarán inmediatamente si navegas en una web segura que pudiera ser fraudulenta.

No se trata de desconfiar de todo lo que encuentres en el océano de Internet, sino de tomar mínimas seguridades para que no te pesquen.

Como dice el refrán, pescaditos precavidos… ¡valen por dos!

BIBLIOGRAFÍA

http://seguridad.internautas.org/html/451.html
http://www.antiphishing.org/

INTERACTÍVATE

¿Quieres saber más sobre otras amenazas en Internet?
http://www.nomasfraude.com/spain/sabias_que/amenazas/