POPULAR BANK

Guía de seguridad de la información
Pistas de Seguridad

TIPOS DE FRAUDE

ENTREGA DE INFORMACIÓN A TERCEROS

***Pharming* - Redirección página-en-red**

Es una práctica consistente en redirigirlo de una página en internet, mediante la manipulación de su dirección electrónica, hacia otra página falsa, creada con el objetivo de estafarle, recabando sus datos confidenciales. El "*Pharming*" es especialmente peligroso puesto que el usuario no es consciente de que se le está redirigiendo hacia una página falsa.

***Phishing* - Pesca electrónica**

Es el envío de correos electrónicos para suplantar la identidad de una entidad bancaria o de comercio virtual, y obtener así sus datos confidenciales bajo el alegato de que:

- Requieren confirmación rápida de sus datos personales y confidenciales,
- Insisten en actualizar sus datos personales y confidenciales,
- Alertan de que su(s) producto(s) financiero(s) será(n) cancelado(s) si usted no remite los datos que piden,
- Ofertas irresistibles por un tiempo exageradamente limitado, creando la ilusión de oportunidad.
- Le informan de que se han agregado nuevos beneficiarios a sus cuentas.

Como el mensaje de correo electrónico se envía masivamente al grupo de direcciones electrónicas que tengan los defraudadores, muchos receptores ni siquiera son clientes de la entidad suplantada.

***SMSishing* - Pesca celular**

Deriva de combinar SMS y phishing, y no es más que otro modo de engaño a través de mensajes SMS al teléfono móvil. Un malhechor le envía un mensaje de texto para inducirlo a que usted proporcione sus datos financieros; también puede solicitarle que pulse en algún enlace para, al final, robar los datos que usted ingenuamente ha facilitado y realizarle el fraude.

***Vishing* - Pesca Telefónica**

"*Vishing*" es una práctica criminal fraudulenta en donde se hace uso del Protocolo Voz sobre IP (VoIP) y la ingeniería social para engañar personas y obtener información delicada como puede ser información financiera o información útil para el robo de identidad.

ATAQUE VÍA PROGRAMAS O EQUIPOS

"*Keylogging*" - Capta teclas

Deriva del inglés "*key*" (tecla) y "*logger*" (registrador). Son sotfwares maliciosos diseñados para registrar las pulsaciones que se realizan sobre el teclado, almacenarlas en archivos y enviarlas a sus creadores.
Éstos Estos programas pueden ser distribuidos a través de un troyano o, bien, como parte de un virus o gusano informático.

***Malware* - Programa malicioso**

Abreviatura de programa malicioso, "*malicious software*", por su definición en inglés. Estos programas incluyen a los virus, spyware, troyanos, gusanos, "*keyloggers*", etc., que se diseñan para infiltrarse, auto ejecutarse, dañar el sistema operativo de una computadora, robar información, etc.

"*Skimming*" - Capturador de tarjetas

Se refiere a un dispositivo que se instala en las ranuras del cajero automático con la finalidad de capturar la información de la banda magnética en su tarjeta de débito o crédito, tan pronto usted la introduce. A veces funciona junto a una cámara oculta o a un teclado transparente, que se superpone al teclado del cajero, con el fin de capturar su PIN.

***Spyware* - Programa espía**

Dentro de la categoría "*malware*", es el tipo de programa que se instala en una computadora al descargar o instalar algún programa. Estos programas realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas, etc.

HOMBRE EN EL MEDIO

"*Eavesdropping*" - Escucha oculta

Término que se refiere a quien escucha secretamente lo que se dice en privado. En el contexto de la seguridad, se aplica a ataques de escuchas para obtener información.

"*Sniffing*" - Captura en-línea

Olfatear o sorber, por su significado en inglés.
Son aplicaciones diseñadas para capturar tramas (trafico) en las redes, son almacenados para su análisis posterior, sin necesidad de poseer acceso a ningún sistema de la red.

Hay dos clases: "*Sniffing software*" y "*Sniffing hardware*". El primero es un programa que captura la información en línea y el otro es un dispositivo que se instala en, o cerca de un equipo, para interferir su transmisión de datos.

"*Spoofing*" - Simulador de datos

En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad, generalmente con usos maliciosos o de investigación.

"*Reply attack*" - Envíos interceptados
Es un ataque en el cual se intercepta un paquete de datos y se reenvían al servidor receptor. Así, un hacker intercepta la comunicación y puede obtener el usuario y contraseña que le permitan entrar a un sistema sin autorización.

OTRAS ESTRATEGIAS

"*Carding*" - Caza de tarjetas

Se refiere al uso desautorizado y masivo de tarjetas de débito y crédito para adquirir, fraudulentamente, bienes y servicios. El término ha evolucionado recientemente para incluir todo un conjunto de actividades que rodean el robo y uso de números de tarjetas para hacer fraudes como "*Pharming*", "*Phishing*", "*Scamming*", "*Skimming*", "*Smsishing*", "*Spoofing*", etc.

Scamming – Artimaña

Sinónimo de estafa.

Funciona cuando el usuario recibe un correo electrónico a través del cual se le promete trabajo, una importante suma de dinero, ampliación de sus relaciones personales, etc., donde se le pide que abra una cuenta bancaria con la finalidad de recibir dinero y transferirlo a otras cuentas, recibiendo comisiones por esta tarea.

El "*Scam*" tiene su origen en los "*Hoaxes*", o cadenas de correos electrónicos, con contenidos falsos y engañosos cuyo tópico solía ser enfermedades incurables, cadenas de solidaridad o de suerte, leyendas urbanas, etc.

"*Spamming*" - Correos inesperados

Es la denominación que reciben los mensajes de correo electrónico no solicitados y de remitente desconocido, habitualmente de carácter publicitario, que se envían en cantidades masivas. Afecta al receptor cuando satura su buzón y le consume ancho de banda de forma innecesaria.
Detrás de los spams también hay publicidad falsa que incita al cliente a comprar productos que no se recibirán, difundir phishing o "*malware*".