RIESGOS

1.ROBO DE IDENTIDAD

El robo de identidad tiene lugar cuando alguien se hace pasar por otra persona para obtener acceso no autorizado a cierto tipo de información.

Modo de operar:

Algunas técnicas utilizadas para el robo de identidad son:
Robar su cartera.
Verificar la información de las cuentas bancarias que llega a su buzón de correo.
Observar las transacciones que realiza en los cajeros automáticos para conocer su número de identificación personal (NIP).
Revisar la basura en busca de recibos de tarjetas de crédito o solicitudes de préstamos.

Medidas preventivas:
Lleve consigo su tarjeta de crédito o débito únicamente cuando vaya a utilizarla.
Nunca tire sus estados de cuenta impresos sin triturarlos o quemarlos ya que estos tienen información que un defraudador puede utilizar para suplantar su identidad.
Asegúrese que recibe los estados de cuenta de sus cuentas bancarias, de no ser así, repórtelo inmediatamente a su banco.
Al ingresar su NIP en un cajero automático, cubra con una mano el teclado para que no pueda ser observado por personas extrañas.

2.INGENIERIA SOCIAL

Consiste en la manipulación de las personas a través de trucos o engaños para que voluntariamente realicen actos que normalmente no harían, con el fin de que divulguen Información confidencial sin que se den cuenta de que la están revelando.

Modo de operar:

El defraudador envía por correo o realiza de forma personal encuestas con supuestos fines estadísticos o mercadológicos.
El cliente proporciona los datos solicitados.
El defraudador obtiene la información.

Medidas preventivas:
Valide la identidad de la persona antes de proporcionar información personal.
Procure no contestar encuestas en las que se solicite información personal o relacionada con sus cuentas bancarias, niéguese de forma amable o elimine el correo electrónico recibido.

3.PHISHING

Es un ataque de ingeniería social a través de correo electrónico en el que se suplanta la identidad de un sitio web con la finalidad de robar datos personales como números de tarjetas de crédito, contraseñas o información de cuentas.
Generalmente los correos electrónicos contienen errores ortográficos, publicidad, premios, promociones y son de carácter urgente.

Modo de operar:
El cliente recibe un correo electrónico que aparenta ser enviado por un banco o una empresa reconocida y que solicita información personal.

RIESGOS

El cliente abre el correo electrónico e ingresa a las ligas adjuntas que lo remiten a un sitio web falso con la misma apariencia del sitio web original.
El cliente no identifica que ha ingresado a un sitio web falso.
El cliente ingresa los datos personales solicitados como usuario y contraseña de su banca Electrónica.
El atacante obtiene los datos personales del cliente.

Medidas preventivas:
Comuníquese con el banco o la empresa que solicita la información para validar la solicitud de la información o reportar dicha actividad.
Por ningún motivo proporcione la información solicitada por correo electrónico o llamada telefónica.
Comunique a sus familiares y amigos el origen de la solicitud de la información para evitar que sean víctimas de esta actividad.
Si usted siguió las instrucciones del correo electrónico recibido, debe cambiar su contraseña de inmediato y llamar al centro de atención a clientes de su banco para reportar dicha actividad.

4.PHARMING

Práctica delictiva que consiste en manipular el servidor DNS (Domain Name Server) al cual la víctima hace consultas, con el fin de desviar los datos enviados a través de internet hacia una página web falsa y de apariencia similar a la que se desea ingresar.
Generalmente la modificación del DNS se lleva a cabo a través de la instalación de software malicioso que es descargado por el usuario al consultar sitios web no confiables.

Modo de operar:
El cliente recibe correos electrónicos que aparentan ser enviados por bancos, personas conocidas o empresas de prestigio.
El cliente abre el correo electrónico e ingresa a las ligas adjuntas.
Se instala un programa malicioso en el equipo de cómputo del cliente que modifica archivos de configuración.
El cliente ingresa a la página web de su banco para hacer uso de su Banca Electrónica.
El acceso a la Banca Electrónica es redireccionado por el programa malicioso a un servidor que contiene un sitio web falso con apariencia similar al que se desea ingresar.
El cliente ingresa los datos personales solicitados como usuario y contraseña de su banca Electrónica.
El atacante obtiene los datos personales del cliente.

Medidas preventivas:
Evite instalar en su equipo de cómputo software de sitios de internet no confiables o de dudosa procedencia.
Nunca abra o ejecute ligas adjuntas a correos electrónicos de personas desconocidas. En mejor copiar la dirección y pegarla en la barra de direcciones de su navegador de internet.
Una vez que haya ingresado al sitio web que desea consultar, valide que la dirección web que se muestra en la barra de direcciones no muestra un nombre ajeno a la empresa que desea ingresar.

5.KEYLOGGER

Es un código malicioso que se instala en el equipo de cómputo de un usuario con el objetivo de almacenar toda la información que se escribe en el teclado de un equipo de cómputo, la cual es enviada de forma no autorizada a un espía informático.

Modo de operar:
El cliente recibe a través de correos electrónicos o ventanas de información invitaciones para descargar un software.

RIESGOS

El cliente descarga el software.
El cliente instala el software descargado en su equipo de cómputo, desconociendo que adicionalmente se instala un código malicioso.
El código malicioso se ejecuta, captura y envía al defraudador todos los datos que el cliente teclee en su equipo de cómputo.
El cliente ingresa los datos personales solicitados como usuario y contraseña de su banca Electrónica.-El atacante obtiene los datos personales del cliente.

Medidas preventivas:
Evite instalar en su equipo de cómputo software de sitios de internet no confiables o de dudosa procedencia.

6.SCREENLOGGER

Es un tipo de código Troyano que se diseña y se instala en la computadora del usuario y que recolecta las pantallas a las que accesa el usuario enviando estas al defraudador, normalmente se adquiere visitando sitios no seguros para adultos o de violencia

Modo de operar:
El cliente recibe a través de correos electrónicos o ventanas de información invitaciones para descargar un software.
El cliente descarga el software.
El cliente instala el software descargado en su equipo de cómputo, desconociendo que adicionalmente se instala un código malicioso.
El código malicioso se ejecuta, captura y envía al defraudador pantallas que el cliente está viendo o accesando en su equipo de cómputo.
El cliente ingresa los datos personales solicitados como usuario y contraseña de su Banca Electrónica.
El atacante obtiene los datos personales del cliente.

Medidas preventivas:
Evite instalar en su equipo de cómputo software de sitios de internet no confiables o de dudosa procedencia.

7.SMISHING

Es una modalidad de fraude variante del phishing que utiliza técnicas de ingeniería social a través del envío de mensajes de texto dirigidos a usuarios de telefonía móvil para obtener información de un cliente.

Modo de operar:
Un defraudador envía un mensaje de texto al celular de un cliente, suplantando la identidad de una empresa de telefonía móvil.
El cliente recibe un mensaje de texto en el que se indica que debe ingresar a una dirección web para cancelar la supuesta activación de un servicio o proporcionar datos personales.
El cliente ingresa a la dirección indicada en el mensaje de texto y proporciona la información solicitada.
El atacante obtiene los datos personales del cliente.

Medidas Preventivas:
Nunca proporcione datos sobre sus tarjetas de crédito o débito a través de mensajes SMS aún cuando parezca que la solicitud proviene de una institución confiable.
Valide con el proveedor del servicio que envío la solicitud de la información la validez del mensaje recibido.

Acuda personalmente a las instalaciones del proveedor del servicio para proporcionar cualquier tipo de información personal solicitada.
Elimine el mensaje recibido y no instale ningún tipo de software en su celular.

8.VISHING

Es una modalidad de fraude variante del phishing que utiliza el Protocolo Voz sobre IP (VoIP) y la ingeniería social para obtener información de un cliente. Su nombre proviene de una combinación de “voz” y “phishing”.

Modo de operar:
Un defraudador envía un correo electrónico o deja una grabación en la contestadora telefónica del cliente en la que utilizando el nombre de una institución bancaria se indica un número telefónico al que debe comunicarse para solucionar un problema relacionado con sus cuentas.
El cliente realiza la llamada al número indicado y escucha una grabación que simula ser de una institución bancaria, en la que se solicita el número de tarjeta de crédito o débito y clave secreta para ingresar.
El cliente ingresa por medio del teclado del teléfono su número de tarjeta de crédito o débito y su clave secreta.
El defraudador obtiene la información solicitada.

Medidas Preventivas:
Nunca proporcione datos sobre sus tarjetas de crédito o débito cuando se reciba una llamada telefónica, aún cuando parezca que la solicitud proviene de una institución confiable.
Valide con su banco la solicitud de información recibida vía telefónica.
Acuda a una sucursal bancaria siempre que se requiera proporcionar sus datos personales y de su tarjeta de crédito o débito.
Elimine el mensaje recibido y no regrese la llamada al número proporcionado.