CANALES ELECTRÓNICOS

FRAUDES ELECTRÓNICOS: INGENIERÍA SOCIAL

DEFINICIÓN

Es importante que conozcamos cuales son las amenazas y el fraude electrónico y como debemos protegernos.
El fraude electrónico no es más que es una manera de estafar a las personas a través de Internet o cualquier medio electrónico, con la finalidad de obtener información confidencial, especialmente de cuentas e instituciones bancarias.
Los delincuentes utilizan diferentes técnicas informáticas para atacar a los usuarios de los bancos. Lo que buscan es obtener los datos de las personas, ya sea información personal, de sus productos financieros (qué tarjetas de crédito tiene asociadas) o información de seguridad de sus cuentas (usuario y contraseñas de acceso).
Distintos tipos de amenazas y el medio en que podemos recibirlos:
Ingeniería social, phishing, ransomware, vishing, skimming, smishing, spyware, admare, malware, etc.

INGENIERÍA SOCIAL

La ingeniería social es una acción destinada a conseguir información de terceros a través de prácticas y técnicas relacionadas con la comunicación. Esto es, aprovecharse mediante engaños, y artimañas de la persona para lograr que esta nos brinde información voluntariamente.
Los ingenieros sociales son expertos en la técnica y ciencia de manipular a la gente haciéndola proveer información sensible como direcciones, teléfonos, números de tarjetas, etc. a través de la construcción de relaciones y aprovechando la tendencia natural de la gente a confiar y ser útil.

> Medios: Celulares, Teléfonos, Internet (Phishing, Redes Sociales, etc.), Persona a Persona.
> Objetivo: Obtener información suficiente que permita perpetrar un fraude en nombre de terceros.
> Tipo de Fraudes: Usurpación de Identidad, Uso de cuentas de terceros, Secuestros virtuales, Uso de tarjetas de terceros, y cualquier tipo de manipulación de la persona para obtener un determinado fin.

Aquí hay algunos de los trucos que emplean habitualmente:

- Llamar para decir que has ganado un premio o una suma en efectivo. Solo deberías pagar por el "envío" o un "gasto administrativo".
- Decir que son de tu compañía de Tarjetas de Crédito y pedirte que confirmes tus datos.
- Decir que son de otra compañía de Tarjetas de Crédito, te prometen una oferta especial o tasas de interés bajas si transferís el saldo de tu tarjeta a esa compañía.; para hacer esto necesitan tu número.
- Decir que representa a un importante centro de beneficencia y pedir por una donación. Este tipo de fraude es a menudo cínicamente empleado en las repercusiones de grandes desastres tales como el tsunami o el fenómeno del niño. También es con frecuencia llevado a cabo vía correo electrónico.

La forma más eficaz de protegerte frente a estas amenazas es mantenerte informado: saber cuáles son los peligros, qué se debe evitar y con qué hay que tener cuidado.

Consejos que pueden ayudarte a identificar las estrategias usadas en la ingeniería social y por tanto a evitar ser víctima de este tipo de ataques:

- Nunca reveles por teléfono o e-mail datos confidenciales (como claves de acceso, números de Tarjetas de Crédito, cuentas bancarias, etc.).
- Nunca hagas click en un enlace a una página web que te llegue a través de un e-mail en el que te piden datos personales.
- Desconfié de cualquier mensaje de e-mail en el que se te ofrezca la posibilidad de ganar dinero con facilidad.
- Si sos usuario de banca electrónica o de cualquier otro servicio que implique introducir en una web datos de acceso, asegúrate de que la dirección de la web es correcta.
- No confíes en las direcciones de los remitentes de e-mail o en los identificadores del número llamante en el teléfono: pueden falsearse con suma facilidad.
- Utiliza el sentido común y pregúntate siempre que recibas un mensaje o llamada sospechosa si alguien puede obtener algún beneficio de forma ilícita con la información que te solicitan.
- Se puede prevenir que tales planes tengan éxito si se sigue una regla muy simple. Nunca se debe dar información personal a alguien que llame salvo se verifique 100% la identidad de la persona.