Seguridad de la información

MODALIDADES DE CIBERATAQUE

Te compartimos valiosa información sobre las técnicas que implementan los atacantes cibernéticos.

El atacante recolecta información de su posible víctima por medio de phishing e ingeniería social. Lo hace a través de redes sociales, enlaces enviados por correo electrónico, anuncios publicitarios o bases de contacto obtenidas ilegalmente.

Luego utiliza esa información para ponerse en contacto con su potencial víctima con el objetivo de obtener mediante engaño sus credenciales bancarias.

Para abordar a su potencial víctima, ganarse su confianza y generar un sentido de urgencia comúnmente emplea estas estrategias engañosas:

Método 1

Crea un perfil o cuenta falsa de Whatsapp haciéndose pasar por personal de atención al cliente de Banco Atlántida u otra institución financiera.

Con esa cuenta contacta a su potencial víctima.

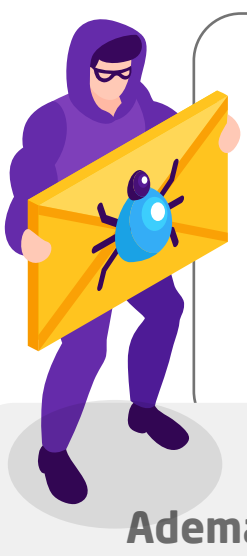
Le informa a su víctima que se han realizado supuestas "transacciones sospechosas" desde su cuenta hacia la cuenta de un tercero.

Luego de que la víctima confirma que no las reconoce, le indican que es necesario realizar un proceso para la cancelación de supuestas transacciones, el cual implica que verifique su información.

Método 2

Con una cuenta o perfil falso en redes sociales, se hace pasar como un potencial cliente interesado en realizar un negocio o comprar un producto o servicio que ofrece su potencial víctima.

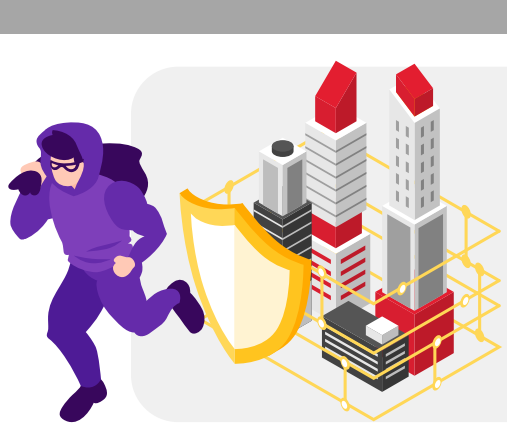
Al momento de "realizar la compra", le indica que hay problemas para efectuar el pago o transferencia y que deben contactarse con "personal de atención al cliente del Banco" quien es realmente otra cuenta falsa creada por el atacante o su cómplice.



Una vez que el atacante se ha ganado la confianza de la víctima, mediante phishing le envían un enlace, vía Whatsapp o correo electrónico, que los dirige a un sitio web falso diseñado para engañarle y robar sus credenciales bancarias.

Además, el atacante lo convence para que instale la aplicación AnyDesk con la que toma el control de celular de la víctima, y le guía para que ingrese su información confidencial en el sitio falso. App que también permite al atacante visualizar los mensajes SMS de la víctima.

Con las credenciales robadas, el atacante ingresa a la cuenta Atlántida Online de la víctima para realizar transferencias a otras cuentas dentro del mismo banco o a cuentas en otras instituciones del sistema financiero, así como retiros en efectivo, coordinándose para retirar el dinero rápidamente.



Cuando el cliente se percata de estos movimientos ya es demasiado tarde para evitar el robo.

Banco Atlántida