RECOMENDACIONES.

Como protegerse de la clonación o robo de tarjetas a través de internet y teléfonos móviles.

- ✓ No compartas tu contraseña con terceros, realiza personalmente tus transacciones financieras.
- ✓ La empresa y bancos NUNCA te solicitan tus datos financieros o números de tarjeta por teléfono o internet.
- ✓ No entregues tus datos personales por correo electrónico.
- ✓ Revise cuidadosamente la forma de pago en línea y las direcciones de los sitios web donde haya introducido información financiera.
- ✓ Establecer límites de gastos en las tarjetas de uso diario, si el banco lo permite.
- ✓ Tener una tarjeta virtual emitida con limites bajos y vincularla con Google/Apple/Samsung Pay.

TOMA EN CUENTA...

Ningún establecimiento debe almacenar información de tarjetas bancarias.

El robo de datos bancarios se está duplicado año con año.

Se ha demostrado que un atacante también podría intercambiar algunos datos con un teléfono bloqueado y luego usar registros modificados de ese intercambio para realizar pagos fraudulentos.

REFERENCIAS.

https://latam.kaspersky.com/blog/how-to-protect-emv-and-nfc-bank-cards/26092/

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

MÉTODOS MÁS EMPLEADOS PARA

MÉTODOS MAS EMPLEADOS

¡PROTÉGETE!

MÉTODOS UTILIZADOS PARA ESTE TIPO DE ROBO.

Los servicios de pago son cada vez más vulnerables ante ataques cibernéticos, por lo anterior, el objetivo es dar a conocer los métodos más comunes utilizados por este tipo de robo para que los usuarios conozcan como contrarrestarlos y evitar ser víctimas del robo de tarjetas bancarias.

Existen 3 métodos principales, los cuales son:

1 Clonación de tarjetas.

Se crea una copia exacta de las tarjetas bancarias para usarla para pagar en tiendas comerciales o retirar dinero en cajeros automáticos.

Los datos se leen con un dispositivo clonador de tarjetas llamado “skimmer”, que se instalaba en un cajero automático o en la terminal de una tienda.

Las tarjetas con chip no son tan fáciles de clonar, por eso los ciberdelincuentes infectan las terminales de pago con un código malicioso que copia los datos del usuario.

¡Protégete!

2 Robo de datos a través de internet.

Los estafadores buscan los datos de la tarjeta bancaria para realizar pagos online que incluyen:

- Número de tarjeta.
- Fechas de vencimiento,
- Código de verificación (CVV/CVC)
- Nombre del titular de la tarjeta,
- Número de pasaporte.

3 Robo de tarjetas y teléfonos de manera antigua.

Este método de robo es más notorio y flagrante, pero sigue siendo común, algunas de sus características son:

1. Los ciberdelincuentes utilizan una tarjeta robada para hacer pagos de baja denominación los cuales no requieren la introducción del código PIN.

2. Un teléfono siempre es un objeto valioso para los ladrones, más si tiene habilitado Google Pay, ya que se pueden hacer pagos con el teléfono.