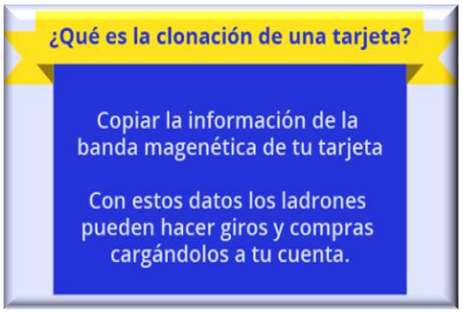
¡CARDING! ¿QUÉ ES Y COMO EVITARLO?

El *Carding* es una forma de estafa online a través de la cual los ciberdelincuentes acceden a los datos de las tarjetas bancarias (débito o crédito), para realizar pequeñas compras con ellas. De esta manera, evitan que la víctima detecte que se está realizando un uso fraudulento de la tarjeta.

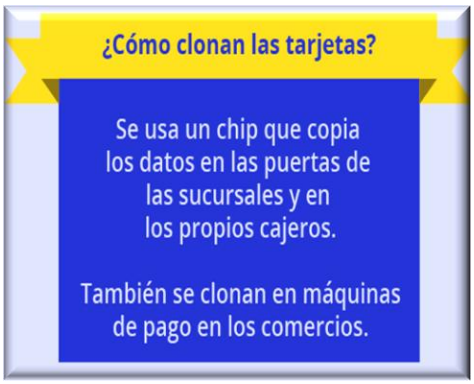
¿Cómo Funciona?



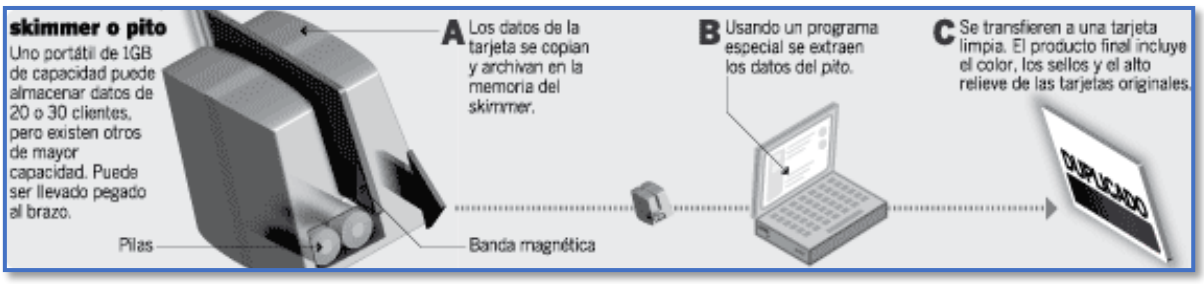
La estafa del *Carding* funciona en dos fases:

La primera es cuando los ciberdelincuentes obtienen los datos de la tarjeta bancaria sean de crédito o de débito, para conseguirlo pueden usar métodos como el phishing o clonar directamente la tarjeta o los números de la misma. Las tarjetas pueden ser clonadas en cajeros automáticos y también en establecimientos comerciales, en virtud que el delincuente en un descuido del cliente puede deslizar la tarjeta en un dispositivo para clonar (skimmer). *"Por eso es muy importante estar atento y no perder de vista la tarjeta al momento de hacer el pago"*

Una vez conseguido los datos, los ciberdelincuentes se dedican a realizar compras, como por ejemplo en establecimientos de comida rápida, productos de belleza, suscripciones a canales de streaming y similares.

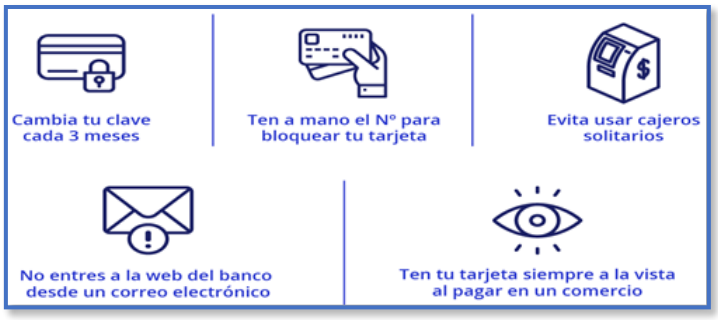


La mayoría de estas compras suelen ser online y/o telefónicas, el objetivo de los ciberdelincuentes es que estos pagos pasen desapercibidos para el usuario durante el mayor tiempo posible.



Telf: 2236-092 / Conmutador 3955-900
dntic.direccion@policiaecuador.gob.ec
Dirección Nacional de Tecnologías de la Información y Comunicación
Departamento de Seguridad de las TIC´s

CONSEJOS PARA PROTEGERSE DEL CARDING



La principal recomendación para evitar la clonación de tarjetas de crédito es tener máxima precaución. A continuación, se detallan unos consejos útiles:

En general

- ✓ No confiar las tarjetas bancarias a otras personas, es un producto personal.
- ✓ Nunca utilizar redes abiertas o computadoras públicas a la hora de realizar pagos o gestiones bancarias online.
- ✓ Activar las notificaciones de consumo y pagos de tarjetas en el celular, para monitorear y detectar oportunamente cualquier movimiento inusual.
- ✓ No proporcionar datos de las tarjetas o cuentas bancarias por teléfono, especialmente ante llamadas entrantes.
- ✓ Comprar siempre en sitios seguros en internet, verificar que las páginas cuenten con el protocolo de seguridad “https”, así como un candado cerrado en la barra de dirección (a la izquierda de ella).

En cajeros automáticos

- ✓ Revisar que no exista ningún objeto adicional en el cajero, los delincuentes que se dedican a este tipo de delitos instalan aparatos electrónicos como si fueran parte del cajero.
- ✓ Nunca acepte ayuda de nadie antes, durante o después de la transacción.
- ✓ Antes de entrar a la cabina (cajero), mirar alrededor para identificar si hay personas con actitud sospechosa.
- ✓ Al introducir la clave, tapar las teclas para evitar que otros puedan mirarla.
- ✓ Usar cajeros automáticos que estén ubicados en zonas concurridas y con vigilancia permanente.

Si sufre este tipo de fraude electrónico o cualquier otro, reportar inmediatamente la situación a la institución bancaria, para que le guíen en el proceso a seguir.