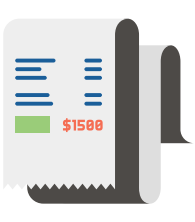
FROM GRASS ROOTS TO HIGH TECH: HOW FRAUDSTERS STEAL CREDIT CARD INFO

The war between credit card fraudsters and those providing protection against fraud is mounting. Fraudsters are finding sophisticated ways to commit crimes in a technological race to beat security measures. Here's a look at how the fraud and security sophistication levels have increased.

HOW THEY STEAL

STOLEN CARD
Fraudster steals wallet, goes on quick shopping spree.



DUMPSTER DIVING
Digging receipts and payment statements out of the trash.

"SCAM ARTISTS"
People are manipulated into giving up confidential information from fraudsters pretending to be your service providers.

SKIMMING
A skimming device is held near a credit card and reads info from the magnetic stripe.

SKIMMING II
Skimmers are placed over ATM or gas pump card readers.

BIN ATTACKS
Fraudsters use the Internet to generate new card numbers from existing ones.

MALWARE
A Malware program is loaded onto a computer or POS device that records passwords, account numbers.

GOING MOBILE
Hacking extends to increasingly popular mobile payment platforms.

LINK ALTERATION
Fraudsters may use an altered return address in a web page that is sent directly to consumers, and takes him/her to the hacker's website.

PHISHING
Using an email that looks like it's from a legitimate company, hackers may prompt you to log into a faulty portal, thus exposing your password or personal details.

STRATEGIC SHIFT
Fraudsters opt to create brand-new card accounts — in your name.

HOW WE PROTECT

SIGNATURE MOVE
Cashier compares signatures on credit card, driver's license to verify ID.

CANCELLATIONS
Credit cards cancelled, reissued after being reported missing.

PAPER SHREDDING
Reducing documents to confetti size leaves information unreadable.

TRACKING TRANSACTIONS
Software searches for unusual card behavior and issues alert.

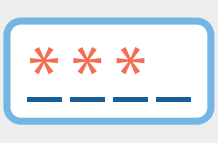
BLOCKING BIN ATTACKS
Software halts hackers who use bank ID Numbers to try to match legit card numbers.

PCI COMPLIANCE
A council sets standards encouraging businesses to be security-focused.

TOKENIZATION
Sensitive payment data replaced with unique token worthless to thieves.

CAPTCHA
Customer must identify distorted letters, numbers or select images on a payment page to prove they are human.

EMV (CHIP) CARDS
When an EMV or chip card is dipped into a terminal, card reader, or POS system, the chip and the equipment create a cryptogram to secure data.



VIRTUAL PIN PAD
A digital, onscreen keypad that prompts cardholders to manually enter their PIN means there's no physical keying for malware to record.

BIOMETRICS
Passwords replaced with fingerprints, facial scans, and/or voice recognition.

TO STAY UP TO DATE WITH THE LATEST TECHNOLOGY AND TRENDS, PARTNER WITH A TRUSTED AND REPUTABLE INTEGRATED PAYMENTS PROVIDER.