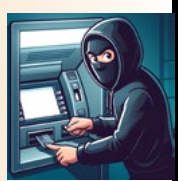
BVS PUBLIC ADVISORY: DETECT ATM & GAS PUMP SKIMMERS

As a leader in wireless, cybersecurity and fraud detection technology, Berkeley Varitronics Systems is dedicated to combating skimming crimes in conjunction with local, state and federal law enforcement. Our innovative devices help financial institutions, retailers, and law enforcement detect and prevent skimming threats.

Sheriff Jeff Diederich from Williamson County Sheriff's Office demonstrates Skim Scan

How Do Skimming Crimes Occur?



Criminals install hidden electronic skimming devices at ATMs and Point-of-Sale (POS) terminals to steal cardholder data. These attacks frequently occur at high-traffic locations such as gas stations, grocery stores, and pharmacies. Stolen card data is re-encoded onto counterfeit cards and used for fraudulent ATM withdrawals and purchases. Often, this stolen data is sold in bulk to criminal organizations.

Types of Skimming Devices

ATM Skimming Devices

Criminals place sophisticated skimming devices deep inside ATM card readers, making them virtually undetectable to the naked eye. These devices capture data from magnetic stripes and even Europay, Mastercard, and Visa (EMV) chips. While ATM manufacturers continuously improve security, criminals adapt their methods to bypass these measures.

ATM Pinhole Cameras

Tiny, discreet cameras are often installed on ATMs to capture users entering their PINs. These "pinhole cameras" can be as small as the tip of a pen, making them difficult to spot.

POS Terminal Skimming Devices

Criminals craft plastic overlay shells that seamlessly fit over legitimate POS terminals. These overlays can cover the entire terminal or just the keypad and EMV reader slot, recording all card data and PINs entered.


Police Deputy Chief Bobby LaPenna from Bedford Police demonstrates Skim Scan

How to Protect Yourself from Skimming

Use ATMs in secure locations
Those inside banks, near security cameras, or close to drive-up windows are less likely to be targeted.

Check for signs of tampering
Look for broken lights, raised PIN pads, loose components, or unusual stickers.

Shield your PIN entry
Cover the keypad with your hand to block hidden cameras.

Inspect POS terminals
If a terminal feels loose, notify store personnel and avoid using it.

Opt for credit over debit
Credit transactions provide extra security and do not expose your checking account.

Sign up for transaction alerts
Receive real-time notifications for card activity to detect fraud faster.

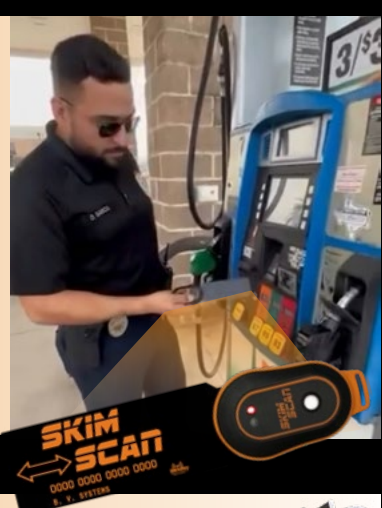
Use contactless payments
EMV chip and NFC-enabled cards reduce the risk of skimming.

Investigator Kaiser with Sanford PD demonstrates Skim Scan at the fuel pump

What to Do If You Suspect Skimming?

Merchants & ATM Owners
Immediately take the terminal out of service and contact corporate security or law enforcement.

Cardholders
Report suspicious activity to your bank's fraud department, deactivate your card, and monitor transactions.



How to Report Skimming Crimes

If you suspect skimming activity, report incidents to local law enforcement or file a complaint with the Internet Crime Complaint Center (IC3) at https://www.ic3.gov.

Berkeley Varitronics Systems remains committed to fighting financial fraud with our industry-leading skimmer detection technology. Protect your business and customers today with Skim Scan, Skim Swipe, and Shim Swipe.

Berkeley Varitronics Systems offers skimmer detetcion solutions for ATMs, Fuel Dispensers, POS terminals and other card readers.