Skimming Devices That Let Thieves Steal from Your Card Accounts Can Be Pretty Sophisticated

Author : David Gurliacci

Categories : Public Safety

Tagged as : Crime Prevention, Crime Prevention 2017, Crime Prevention Advice, Crime Prevention Advice 2017, Crime Prevention TipsCrime Prevention Tips 2017

Date : May 21, 2017

Greenwich police Detective Mark Solomon recently shared an overview of recent frauds using "skimming" that steal credit or debit card information from unsuspecting victims.

The devices can be disguised as parts of ATM machines or work inside gas pumps and other point-of-sale devices.

Even the machines on train station platforms have been rigged by greedy criminals eager to access credit card information.

The machines often are set up by criminals, frequently in gangs of 20 to 30 members from Eastern Europe.

———————

— This article previously was published by Greenwich Free Press.

———————

Solomon is a member of the Connecticut Financial Task Force — which includes the IRS, the U.S. Postal Service, state police and local agencies — said it's a challenge to keep on top of the ingenious strategies that target credit card and bank account information.

People should be extra vigilant over the weekends when banks are closed but ATMs in their lobbies are open — especially holiday weekends, which give criminals an extra day to get their work done, he said.

"Europe is a crystal ball for the future," Solomon said. He also explained that criminal gangs often use juveniles to install skimming devices because they won't be charged as adults if caught. Children as young as 13, 14, and 15 are often accomplices in these crimes.

When caught skimming, police often refer the matters to federal criminal courts, where perpetrators are charged with bank fraud and aggravated identity theft, and sentences can run consecutively for a total of several years.

Solomon advises people to use one card to gain access to an ATM lobby and then a different card at the actual ATM machine.

Skimmers prefer to get both passwords and information on magnetic strips on the back of cards. They even sometimes install cameras inside smoke detectors in ATM foyers to see customers' information.

There are other strategies to foil these criminals, who often use an "overlay" over a PIN pad. An overlay can have a replica over the authentic PIN pad, sometimes secured with double-sided tape.

People should check to see if a PIN pad on an ATM, or even a gas pump or store point-of-sale device, is firmly in place, Solomon said. "Wiggle it and make sure nothing moves," he said.

Gas Pump Skimming

Criminals can connect to the Bluetooth device inside a gas pump, capture magnetic strip data and store it. Then they use the their Bluetooth device to transmit and receive the data from the gas pump. There is nothing on the outside visible to the customer or gas station employee.

In Greenwich, thieves successfully used a 3-inch device inside a gas pump.

Often thieves install their skimming devices after midnight or after hours over a weekend. Then they will drive up in a U-Haul and block the employees' view of the pump. From there, the skimming device can be installed in as little as 45 seconds.

"It's a cat-and-mouse game," Solomon said, adding that the technique originated in California and made its way to the east coast.

Gas pumps are kept locked, but many are locked with generic keys.

This will eventually change, but for now is an invitation to criminals who then access customer's PIN code and card data, then go straight to the ATM and withdraw cash.

Solomon said these techniques are even taught online via YouTube.

The good news is there are some prevention measures for gas stations, including "secure seals" which are placed over the lock mechanisms. Gas stations also are moving away from generic keys and seals that are easily counterfeited.

Some seals will say "void" if they have been tampered with. The state Department of Consumer Protection has emailed gas stations with information about how to ensure that seals are not counterfeited.

If employees at a gas station detect a skimmer they are advised not to touch it, and call law enforcement immediately, Solomon said.

Point-of-Sale Skimming

This takes place when a customer uses a card in a store where a criminal has slipped a card reader "overlay" over the device.

Solomon said this is common among criminals from Eastern Europe who distract the cashier or teller and put their overlay over the device.

"You are actually putting your PIN number into the counterfeit PIN pad," Solomon aid.

This technique is happening more and more often. Solomon said often the thieves use 3D printing technology here in the US to make the overlays.

Protecting Your PIN

Solomon said it's not enough to put your hand over a PIN pad while you key in your password.

It's important to have your free hand hover very low over the hand that is keying in the password, he said,

adding that thieves install tiny cameras very low to the PIN pad.

In addition to holding your free hand over the PIN pad, Solomon advises wiggling the pad to make sure it is not loose. If it is loose, that is a sign that there may be a counterfeit overlay.

Private ATMs at Restaurants and Convenience Stores

People are vulnerable at ATM machines in restaurants and convenience stores, because those machines typically don't have surveillance cameras, Solomon said.

Criminals will insert skimmers into those ATMs that are undetectable from the outside of the machine.