libn.com
powered by Long Island Business News

Skimming devices, which steal information from an ATM card's magnetic stripe, are difficult to detect.

Staying ahead of the thieves

By: Bernadette Starzee January 15, 2018 0

Banks, credit unions and convenience stores on Long Island have fallen victim to ATM skimming in the past year, part of a $2 billion problem worldwide, according to the ATM Industry Association.

In an effort to stay one step ahead of the criminals, Westbury-based NEFCU recently installed Diebold's ActivEdge card readers on ATMs at its 15 branches.

Criminals insert skimming devices on top of or inside card readers at banks, gas stations and stores with the goal of creating a copy of a user's ATM card.

"For cards with a magnetic stripe in the back, enough information is stored in that stripe to empower anyone to recreate the card," said Jojo Seva, chief technology officer for the credit union. "The graphics on the card, the embossed name and number are not important. Everything is in the magnetic stripe."

In order to capture what's on the magnetic stripe, "criminals put a false card reader on top of or inside the card reader on the ATM machine," Seva said. "They also install microcameras around the ATM, so while capturing the card information, they can also capture the PIN number entered by the cardholder's fingers."

While the PIN isn't necessary to use the recreated card to make purchases, "getting the PIN allows thieves to use the recreated card to get cash," Seva said. "Cash is king – it's untraceable."

Skimming devices have evolved over time.

"In the past, the skimming devices would be outside the card reader," he said. "But technology caught up, and ATMs were able to detect if something was installed on top of the card readers. But then a technology evolution on the skimmer side put the skimmer inside the card reader, where it's harder to detect. They're now called shimmers."

According to Seva, NEFCU's anti-skimming card readers read cards differently than traditional card readers. Rather than inserting the card the typical way, cardholders rotate the card 90 degrees, inserting the longer edge into the machine (like the landscape option versus portrait for printing, Seva said).

"Once it's in, there's a mechanism that scans the magnetic stripe from left to right, and there's no skimming device that exists today that can scan cards that way," he said. "Traditional card readers scan the card up and down."

In addition, Seva explained, there's also "encryption going on in which the card reader communicates with the CPU of the ATM, so that even if there's a device installed on there, it will not be able to capture the data."

Further, he noted, each card reader is uniquely paired with each ATM, "so you can't just uninstall one and put it on another, and no one can insert a fraudulent device to replace what's there," he said.

With the new technology, NEFCU is confident that "when a typical skimmer walks up to a machine, he'll take a look at it and not bother – he'll go to another institution," Seva said.

Like other banks and credit unions, NEFCU has captured the activities of thieves on their surveillance cameras and handed the videos over to police.

"A lot of thieves are pretty brazen," Seva said. "They don't even cover their faces."

Installing the new devices – which cost about $3,000 for all 15 branches – is only part of the process to foil skimmers.

"Our branch staff is diligent about inspecting the machines every day," Seva said. "But if a skimmer is installed after the branch closes at 6 p.m. and it's not detected until the following day, customers may have used the machine, so there will already be victims. To us that's a reactive way to handle the problem. We wanted to be proactive."

In an effort to combat skimming, the United States is slowly moving toward EMV chip technology.

"The way the chip works, it's not sending all of the information in the magnetic stripe back and forth with transactions," Seva said, noting that a code sent with a chip transaction can only be used once, so even if it's replicated, it can't be used to recreate a card.

However, he noted, the magnetic stripe is still the standard in the U.S., so credit unions and banks must continue to allow magnetic swipes to accommodate all card holders, Seva said.