How to Spot and Avoid Credit Card Skimmers

Fahmida Y. Rashid

Oct 15th, 2014

www.pcmag.com/article2/0,2817,2469560,00.asp

With all the recent headlines about point-of-sale malware infecting retailers and restaurants around the country, it's easy to forget the more common way cyber-criminals steal credit and debit card numbers: card skimmers. If you ever swipe your card at a gas station pump, withdraw cash from an ATM, or buy tickets from a vending machine, then you are at risk.

Cyber-criminals install skimmers, which are essentially malicious card readers that grab the data off the card's magnet stripe, on to the real payment terminals so that they can harves data from every person that swipes their cards. The thief has t come back to the compromised machine to pick up the file containing all the stolen data, but with that information in hand he can create cloned cards or just break into bank accounts to steal money.

"Classic skimming attacks are here to stay," and will likely continue to be a problem even after banks make the shift to chip-and-PIN cards, said Stefan Tanase, a security researcher at Kaspersky Lab. Even if the cards have a chip, the data will still be on the card's magnetic strip in order to be backwards-compatible with systems that won't be able to handle the chip, he said.

The typical ATM skimmer is a device smaller than a deck of cards that fits over the existing card reader. Most of the time, the attackers will also place a hidden camera somewhere in th vicinity with a view of the number pad in order to record personal-identification-numbers. The camera may be in the ca reader, mounted at the top of the ATM, or even just to the side inside a plastic case holding brochures. Some criminals may install a fake PIN pad over the actual keyboard to capture the PIN directly, bypassing the need for a camera.

The above picture is a real-life skimmer in use on an ATM. You can see how the arrows are very close to the reader; that is a sign a skimmer was installed over the existing one, since the real card reader would have some space before the arrows.

When you are pumping gas or grabbing some money for lunch out of the ATM, the last thing you want to worry about is your card information getting stolen. Here are some tips, straight from the experts.

Check for Tampering

When you approach an ATM, check for some obvious signs of tampering at the top of the ATM, near the speakers, the side of the screen, the card reader itself, and the keyboard. If something looks different, such as a different color or material, graphics that aren't aligned correctly, or anything else that doesn't look right, don't use that ATM.

It's a good idea to quickly take a look at the ATM next to yours and compare them both. If there are any obvious differences, don't use either one, and report the suspicious tampering to

your bank. For example, if one ATM has a flashing card entry to show where you should enter the ATM card and the other ATM has a plain reader slot, you know something is wrong. Since most skimmers are glued on top of the existing reader, that will obscure the flashing indicator.

If the keyboard doesn't feel right—too thick, perhaps—then there may be a PIN-snatching overlay, so don't use it.

Wiggle Everything

Even if you can't see any visual differences, push at everything, Tanase said. ATMs are solidly constructed and generally don't have any jiggling or loose parts. Pull at protruding parts like the card reader. See if the keyboard is securely attached and just one piece. Does anything move when you push at it?

Skimmers read the magnetic stripe as the card is inserted, so give the card a bit of a wiggle as you put it in, Tanase advised. The reader needs the stripe to go in a single motion, because if it isn't straight in, it can't read the data correctly. If the ATM is the kind where it takes the card and returns it at the end of the transaction, then the reader is on the inside. Wiggling the card as you enter it in the slot won't interfere with your transaction, but will foil the skimmer.

Think Through Your Steps

Just assume there is someone looking at your PIN, whether it's over your shoulder or through a hidden camera. Cover your hand when you enter the number sequence on the PIN pad, Tanase said.

Even if you don't notice the skimmer and swipe your card, covering your hand when you enter your PIN can keep you saf Obtaining the PIN is essential, since the criminals can't use the stolen magnetic stripe data without it, Tanase said. Of course, that assumes the attacker is using a camera and not an overla to obtain your PIN.

Criminals frequently install skimmers on ATMs that aren't located in overly busy locations since they don't want to be observed installing malicious hardware or collecting the harvested data. The ATMs in banks are generally safer becaus of all the cameras, although some daring criminals do still succeed. The ATM inside a grocery store or restaurant is generally safer than the one that is outside on the sidewalk. Stop and consider the safety of the ATM before you use it.

The chances of getting hit by a skimmer are higher on the weekend than during the week, since it's harder for customers to report the suspicious ATMs to the bank. Criminals typically install skimmers on Saturdays or Sundays, and then remove them before the banks reopen on Monday.