How to Spot and Avoid Credit Card Skimmers

The moment I started seriously worrying about credit card and debit card skimmers wasn't when my entire bank account was transferred to Turkey, or when I had to get three credit cards in two months because of fraudulent charges. It was when I learned that stealing a credit card number is as easy as plugging in a magnetic strip reader into a computer and opening a word processor. Every swipe is read as a keyboard entry, with no extra setup required. More advanced devices to steal your information are installed by criminals directly on to ATMs and credit card readers. These are called skimmers, and if you're careful you can keep from being victimized by these insidious devices.

What Are Skimmers?
Skimmers are are essentially malicious card readers that grab the data off the card's magnetic stripe attached to the real payment terminals so that they can harvest data from every person that swipes their cards. The thief has to 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. Perhaps the scariest part is that some skimmers don't prevent the ATM or credit card reader from functioning properly.

Classic skimming attacks are here to stay, and will likely continue to be a problem even after banks make the shift to EMV chip cards, according to 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 told us. Now, months after the U.S. rollout of EMV cards, some merchants still require customers to use the magstripe.

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 the vicinity with a view of the number pad in order to record personal-identification-numbers, or PINs. The camera may be in the card 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. The same is true for credit card readers.

If you're at the bank, 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 insert 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, they 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. Credit card readers have more variation, but still: 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

Whenever you enter your debit card's PIN, Just assume there is someone looking. Maybe it's over your shoulder or through a hidden camera. Cover the keypad with your hand when you enter your PIN, 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 safe. 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 overlay 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 inside banks are generally safer

because of all the cameras, although some daring criminals do still succeed at installing them there. 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.

Whenever possible, don't use your card's magstripe to perform the transaction. For credit card readers, feel underneath the PIN pad for a slot to insert your card and its EMV chip to be read. When you use your EMV chip, the card is authorized on the device and your personal information is never transmitted. This forces criminals to attack the inner workings of EMV-enabled readers. While cracking EMV readers is possible, it's much harder than magstripe skimming.

If the credit card terminal accepts NFC transactions, consider using Apple Pay,Samsung Pay, or Android Pay. These services tokenize your credit card information, so your personal information is never exposed. If a criminal somehow intercepts the information, he'll only get a useless virtual credit card number.

Stay Aware

If you don't notice a card skimmer and your card data does get stolen, take heart. As long as you report the theft to your card issuer (for credit cards) or bank (where you have your account) as soon as possible, you will not be held liable for the lost amount and your money will be returned. Business customers, on the other hand, don't have the same legal protection and may have a harder time getting their money back.

Timely reporting is very important in cases of fraud, so be sure to keep an eye on your debit and credit card transactions. Personal finance apps like Mint.com can help ease the task of sorting through all your transactions. Also, try to use a credit card whenever possible. A debit transaction is an immediate cash transfer and requires making an FDIC claim whcih can take weeks to be processed. Credit card transactions can be halted and reversed at any time, and doing so puts pressure on merchants to better secure their ATMs and point-of-sale terminals.

Lastly, pay attention to your phone. Banks and credit card companies generally have very active fraud detection policies and will immediately reach out to you, usually over phone or SMS, if they notice something suspicious. Responding quickly can mean stopping attacks before they can affect you, so keep your phone handy.

Just remember: If something doesn't feel right about an ATM or a credit card reader, just don't use it. And whenever you can, use the chip instead of the strip on your card. Your bank account will thank you.

Fahmida Y. Rashid contributed to this story