# How to Spot and Avoid Credit Card Skimmers and Shimmers

Small devices called skimmers and the even more insidious shimmers can easily steal your credit and debit card information when you swipe. Here's how to protect yourself from these rare, but nasty, attacks.

Max Eddy
Updated March 2, 2021

I vividly remember the moment I realized how woefully insecure credit and debit cards are. I watched as someone took an off-the-shelf USB magnetic strip reader and plugged it into a computer, which recognized it as a keyboard. They opened a word processor and swiped the card. A series of numbers dutifully appeared in the text file. That was it: The card's information had been pilfered.

That same technology has matured and miniaturized. Tiny "skimmers" can be attached to ATMs and payment terminals to skim your data off the card's magnetic strip (called a "magstripe"). Even smaller "shimmers" are shimmed into card readers to attack the chips on newer cards.

Now there's also a digital version called e-skimming pilfering data from payment websites. Fortunately, there are many ways to protect yourself from these attacks.

## What Are Skimmers?

Skimmers are tiny, malicious card readers hidden within legitimate card readers that harvest data from every person that swipes their cards. After letting the hardware sip data for some time, a thief will stop by the compromised machine to pick up the file containing all the stolen data. With that information, he can create cloned cards or just commit fraud. Perhaps the scariest part is that skimmers often don't prevent the ATM or credit card reader from functioning properly, making them harder to detect.

Getting inside ATMs is difficult, so ATM skimmers sometimes fit over existing card readers. Most of the time, the attackers also place a hidden camera somewhere in the vicinity in order to record personal identification numbers, or PINs, used to access accounts. The camera may be in the card reader, mounted at the top of the ATM, or even in the ceiling. Some criminals go so far as installing fake PIN pads over the actual keyboards to capture the PIN directly, bypassing the need for a camera.

This picture is a real-life skimmer in use on an ATM. You see that weird, bulky yellow bit? That's the skimmer. This one is easy to spot because it has a different color and material than the rest of the machine, but there are other tell-tale signs. Below the slot where you insert your card are

raised arrows on the machine's plastic housing. You can see how the grey arrows are very close to the yellow reader housing, almost overlapping. That is a sign a skimmer was installed over the existing reader, since the real card reader would have some space between the card slot and the arrows.

ATM manufacturers haven't taken this kind of fraud lying down. Newer ATMs boast robust defenses against tampering, sometimes including radar systems intended to detect objects inserted or attached to the ATM. However, one researcher at the Black Hat security conference was able to use an ATM's onboard radar device to capture PINs as part of an elaborate scam.

## Are Skimmers Still a Threat?

While researching an update to this article, we reached out to Kaspersky Labs, and company representatives told us something surprising: skimming attacks were on the decline. "Skimming was and still is a rare thing," said the Kaspersky spokesperson.

The Kaspersky representative cited EU statistics from the European Association for Secure Transactions (EAST) as indicative of a larger trend. The EAST reported a record low in skimmer attacks, dropping from 1,496 incidents in April 2020 to 321 incidents in October of the same year. The effects of COVID-19 might have something to do with that drop, but it's nonetheless dramatic.

That doesn't mean skimming has gone away, of course. As recently as January, 2021, a major skimming scam was unearthed in New Jersey. It involved attacks on over 1,000 bank customers, with criminals attempting to make off with over $1.5 million.

## From Skimmers to Shimmers

When the US banks finally caught up with the rest of the world and started issuing chip cards, it was a major security boon for consumers. These chip cards, or EMV cards, offer more robust security than the painfully simple magstripes of older payment cards. But thieves learn fast, and they've had years to perfect attacks in Europe and Canada that target chip cards.

Instead of skimmers, which sit on top of the magstripe readers, shimmers are inside the card readers. These are very, very thin devices and cannot be seen from the outside. When you slide your card in, the shimmer reads the data from the chip on your card, much the same way a skimmer reads the data on your card's magstripe.

There are a few key differences, however. For one, the integrated security that comes with EMV means that attackers can only get the same information they would from a skimmer. On his blog, security researcher Brian Krebs explains that "Although the data that is typically stored on a card's magnetic stripe is replicated inside the chip on chip-enabled cards, the chip contains additional security components not found on a magnetic stripe." This means that thieves

couldn't duplicate the EMV chip, but they could use data from the chip to clone the magstripe or use its information for some other fraud.

The Kaspersky representative we spoke to was unequivocal in their confidence for chip cards. "EMV is still not broken," Kaspersky told PCMag. "The only successful EMV hacks are in lab conditions."

The real problem is that shimmers are hidden inside victim machines. The shimmer pictured below was found in Canada and reported to the RCMP. It's little more than an integrated circuit printed on a thin plastic sheet.

## Check for Tampering

Checking for tampering on a point-of-sale device can be difficult. Most of us aren't in line at the grocery store long enough to give the reader a good going over. It's also harder for thieves to attack these machines, since they aren't left unattended. ATMs, on the other hand, are often left unwatched in vestibules or even outdoors, making them easier targets.

While most of this article discusses ATMs, keep in mind that gas stations, payment stations for public transit, and other unattended machines are also ripe for attack. Our advice applies in these circumstances, too.

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.

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. If there are any obvious differences, don't use either one—instead, 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 slot, you know something is wrong. Most skimmers are glued on top of the existing reader and will obscure the flashing indicator.

If the keyboard doesn't feel right—too thick or off-center, perhaps—then there may be a PIN-snatching overlay. Don't use it. Look for other signs of tampering like holes that might hide a camera, or bubbles of glue from a hasty machine surgery.

Even if you can't see any visual differences, push at everything. ATMs are solidly constructed and generally don't have any 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. If anything moves when you push at it, be concerned.

## Think Through Your Transaction

Whenever you enter a debit card PIN, assume there is someone looking. Maybe it's over your shoulder or through a hidden camera. Even if the ATM or payment machine seems otherwise fine, cover your hand as you enter your PIN. Obtaining the PIN is essential. Without it, criminals are limited in what they can do with stolen data.

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 (although there are always exceptions). Indoor ATMs are generally safer to use than outdoor ones, since attackers can access outdoor machines unseen. Stop and consider the safety of the ATM before you use it.

Whenever possible, don't use your card's magstripe to perform the transaction. Most payment terminals now use magstripe as a fallback and will prompt you to insert your chip instead of swiping your card. If the credit card terminal accepts NFC transactions, consider using Apple Pay, Samsung Pay, or Android Pay.

These contactless payment services tokenize your credit card information, so your real data is never exposed. If a criminal somehow intercepts the transaction, he'll only get a useless virtual credit card number. Some Samsung devices could emulate a magstripe transaction through the phone. This technology is called MST, but it has now been discontinued.

One scenario that often requires using your magstripe is paying for fuel at a gas pump. These are rife for attacks, because many don't yet support EMV or NFC transactions, and because attackers can gain access to the pumps without being noticed. It's much safer to go inside and pay the cashier. If there isn't a cashier on duty, use the same tips for using ATMs and investigate the card reader before you use it.

## From Skimmers to Shimmers to E-Skimmers

Not surprisingly, there's a digital equivalent called e-skimming. The 2018 British Airways hack apparently relied heavily on such tactics.

As Bogdan Botezatu, Director of Threat Research and Reporting at Bitdefender, explained, e-skimming is when an attacker inserts malicious code into a payment website that snatches away your card information.

"These e-skimmers are added either by compromising the online store’s administrator account credentials, the store’s web hosting server, or by directly compromising the [payment platform vendor] so they will distribute tainted copies of their software," explained Botezatu. This is similar to a phishing page, except that the page is authentic—the code on the page has just been tampered with.

"e-skimming attacks are increasingly becoming adept at evading detection," said Botezatu. "The more time an attacker maintains this foothold, the more credit cards they are able to collect."

Combating this type of attack is ultimately up to the companies who run these stores. There are a few things consumers can do to protect themselves, though. Botezatu suggested that consumers use security suite software on their computers, which he said can detect malicious code and prevent you from entering your information.

Alternatively, you can avoid entering your credit card information all together with virtual credit cards. These are dummy credit card numbers that are linked to your real credit card account. If one is compromised, you won't have to get a new credit card, just generate a new virtual number. Some banks, like Citi, offer this as a feature so ask yours if it's available. If you can't get a virtual card from a bank, Abine Blur offers masked credit cards to subscribers, which work in a similar way. Apple Pay and Google Pay are also accepted on some websites, too.

Another option is to enroll in card alerts. Some banks will send a push alert to your phone each time your debit card is used. This is handy, since you can immediately identify bogus purchases. If your bank supplies a similar option, try turning it on. Personal finance apps like Mint.com can help ease the task of sorting through all your transactions.

## Stay Aware

Even if you do everything right and go over every inch of every payment machine you encounter (much to the chagrin of the people behind you in line) you can be the target of fraud. But 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. 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.

Also, try to use a credit card if it makes sense for you. A debit transaction is an immediate cash transfer and can sometimes be more time consuming to correct. Credit card transactions can be halted and reversed at any time. Doing so puts pressure on merchants to better secure their ATMs and point-of-sale terminals. Overuse of credit has its own pitfalls, though, so be careful.

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, don't use it. Whenever you can, use the chip instead of the strip on your card. Your bank account will thank you.

Source: https://www.pcmag.com/how-to/how-to-spot-and-avoid-credit-card-skimmers