Advertiser Disclosure (https://www.elitepersonalfinance.com/advertisement-disclosure/)

ATM Skimmers? Here is What You Need to Know!

ElitePersonalFinance (https://www.elitepersonalfinance.com/author/elitepersonalfin/)

Last Update: August 31, 2021

- Credit Cards (https://www.elitepersonalfinance.com/category/credit-cards/)
- Fraud (https://www.elitepersonalfinance.com/cate

It's always frustrating when you know there are ways your identity could get stolen, yet there's nothing you can do to stay safe. ATM skimming is one of the few ways you could become a victim without having much control over whether it happens.

If you fear this identity theft threat, then here are some things you might want to know!

What is ATM Skimming?

"ATM skimming" is defined as the act of grabbing debit or credit card information from unsuspecting ATM users.

This tactic could get used to stealing someone's debit card or credit card information. The skimming could occur at an automated bank machine, in a gas station ATM, or even at the point-of-sale payment device in a retail store or restaurant. It can happen at home or when traveling abroad, though tourist destinations are 'plucking grounds' for identity thieves.

These criminals are also getting smarter. Gone are the days of sticking tape in the card slot and watching over a stranger's shoulders for their PIN. The threats are much more real now; fraudsters even have the power to force ATMs to give out all their cash at once. So, ATM skimming has evolved to include many different types of vulnerability-exploiting technology.

Common Examples of ATM Skimming Techniques

Regardless, the ways a criminal can pull off ATM skimming techniques are limited. There are specific approaches that these fraudsters rinse and repeat. The illicit practices have proven to work, and card companies are far from creating an infrastructure that prevents wide-scale attacks.

ATM Overlay

How does it work?

ATM overlay consists of a device that is placed over the keypad of an ATM. It is used to capture your PIN while you enter it. Yet, it's hard to detect that the machine can read your PIN entry.

How can this be prevented?

Banks face around $1 billion per year in losses due to ATM skimming schemes. Most of the time, the bank machine user will not tell any skimming equipment was installed. Only security footage and guards have a real shot at stopping the crime. But, avoiding the less public and small business-owned machines is a good way to lower your exposure to all potential ATM skimming threats.

Black Box Hack

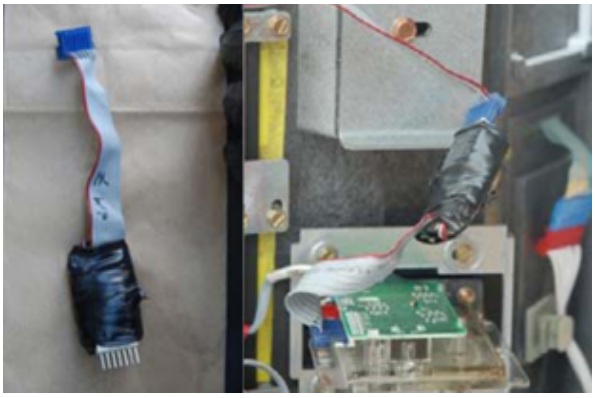
How does it work?

A hacker sets up a smartphone to breach the security of an ATM system. It orders the machine to give out money by writing and executing a command from the smartphone. The command is done remotely, but the device must first get installed into the machine.

How can this be prevented?

These devices must be installed into ATMs before they can work. This means it's more of a threat to machines that are not monitored well. As such, you can see a drastic reduction in your risk exposure by sticking to machines in populated locations.

Bluetooth Skimmer



How does it work?

An almost invisible skimming device gets set up inside of the machine. It grabs the information and sends it to a nearby device through Bluetooth technology. The information gets relayed to the identity thief, who then can start to create the stolen cards.

How can this be prevented?

The best thing you can do is avoid using your credit card at gas pumps. This tactic is not as common, but it is a growing threat. Just last year, 13 were indicted after a year-long Bluetooth skimming spree against gas pumps all across the country. Yet, this tactic has caused quite a ruckus in recent months with the developing Bluetooth skimming investigation.

Card Skimmer

How does it work?

A device is installed in or over the card reader slot and grabs information from every card that enters it. It's typical to see this combined with a hidden camera or keypad overlay. When the two pieces of information are put together, the fraudster can create their own copy of the card and cash out the compromised account.

How can this be prevented?

You can feel around the card reader slot for any abnormalities. A mounted panel is often easy to detect, even when installed flush with the normal panel. By wiggling around the card reader slot a bit, you should have a feel for whether there's any additional equipment installed. If warning signs are there, look for another ATM to use. You can also contact the machine's support number if you are confident the machine was compromised in any way.

Hidden Camera

How does it work?

As you would imagine, this technique involves hiding a camera to steal PINs. The hidden camera could be placed within a fake panel mounted to the machine or even placed nearby. For example, a brochure holder right next to the ATM often serves as an easy spot to hide a camera.

How can this be prevented?

You really have to take the time to examine the machine and its surroundings. Watch out for any tiny holes in the machine's panels and look for possible equipment positioned in your peripherals. Further, take extra precautions and use your other hand to keep your button presses as hidden as possible.

Malware

How does it work?

Malware gets installed in the ATM through an infected USB stick. This stick contains all the right viruses to trigger the ATMs cash balance to show. Even worse, the user can trigger the machine to dispense cash from a remote distance. This is similar to the Black Box attack, except the criminal does not need to install the hardware inside the machine.

How can this be prevented?

ATM owners need to take a proactive approach to ensure their customers are not at risk of malware attacks. This is especially true for those who have yet to upgrade from Windows XP, which is now unsupported by Microsoft. In fact, European victims alone lost over $1.32 million from ATM malware attacks (http://www.pcworld.com/article/2908332/use-of-windows-xp-makes-european-atms-vulnerable-to-malware-attacks.html). The machine user has no real way to avoid becoming a victim of an ATM malware attack.

Businesses outside of the United States are not always well monitored and regulated. Sometimes it's easy for a 'bad apple' employee to slip through the cracks, whether a police officer or a McDonald's manager.

Real Cases of Identity Theft by ATM Skimming

Identity thieves are everywhere, so you do not have to leave your city to put yourself at risk of an ATM skimming attack. This is easy to notice by looking at some of the more recent ATM cases skimming identity theft. Many victims resulted from a few bad actors, showing how dangerous these skimming devices can be if left in the wrong hands.

Below are some examples of real, sizable cases of ATM skimming identity theft.

- **International ATM Fraud (June 2013) – over 5,000 victims**

Zoltan Deak, Marius Zegrean (https://www.fbi.gov/philadelphia/press-releases/2015/romanian-national-admits-to-international-atm-skimming-scheme) were all working together in an organized identity theft crime ring. The group installed ATM skimming equipment into machines in many locations worldwide, though most were in Europe. While there's no telling how many victims there really were, the number of card numbers found on Deak and Zegrean accounted for close to 5,000 victims.

- **New York ATM Fraud (Dec 2007 – June 2009) – over 1,400 victims**

Radostin Paralingov received 21 months imprisonment as a result of his involvement in a large-scale ATM skimming scheme. These devices were running on ATMs located at banks all around New York City. The result was over $1.8 million in losses spanning across over 1,400 victims.

- **Atlanta ATM Fraud (Fall 2007 – July 2008) – around 400 victims**

Romulus Bacian and Marius Csapay (https://www.fbi.gov/atlanta/press-releases/2009/atl110909.htm) joined an organized identity theft crime ring to defraud at least 400 bank customers in Atlanta. This was done by installing skimming devices into many different ATMs across the greater Atlanta region. This scheme was run with two parts of equipment – an ATM overlay grabbed card numbers and an undetectable camera placed to record the customer's PIN entry. In total, over $200,000 was believed to have been stolen by the pair.

- **New York Gas Pump Fraud (March 2012 – March 2013)**

13 fraudsters were indicted due to an ATM skimming identity theft spree that cost victims over $2.1 million. The scheme started with installing Bluetooth skimming devices in gas pumps across parts of the United States. The stolen information was used to create cards containing real consumer data, which was later cashed out. This case brought much attention to Bluetooth skimming devices, which could be the next biggest threat to ATM security.

Here's How You Can Keep Safe from ATM Skimmers!

No one approach will guarantee you protection from ATM skimming attacks, but there are definitely some rules you can follow to lower your risk exposure.

- **There are other options**

It would help if you rarely use an ATM unless it's an absolute emergency. Just go into your bank and manage your transaction with an actual teller. Or, limit yourself to using machines at major financial institutions that are kept under 24/7 surveillance.

- **Sometimes you can tell**

Most of the time, ATM skimming tactics go unnoticed. The ways of detecting these devices often require GPS tracking, Free2Move beacon scanning, and so on. Yet, looking for color disparities, abnormal depths, intentional tiny holes, and other signs of compromise can help you spot a malicious ATM before it's too late.

- **Cards and vacations**

You must understand that an identity theft attack made while traveling is hard to detect and almost impossible to stop. Before going on a business trip or vacation, make sure you exchange the currency of your destination. It's better to have an abundance and have to swap back when you return than to have to rely on an ATM that could compromise your identity.

- **Cameras and placement matter**

Every ATM skimming criminal will first spot out machines that are easy for them to target. The biggest factors they must look for include a lack of video surveillance and a distraction from onlookers. As someone looking to use an ATM, apply the opposite logic and stick to monitored machines in public areas.

- **Bank cards hold many risks**

Your credit card is different because your debt stops when the card gets compromised. You are better off paying with cash whenever possible, as anyone problem with your bank account could lead to many more. Yet, an attack against your bank card could leave you unable to make your debt payments.

ATMs were not designed to be safe because the cards they support are vulnerable. Chip and pin technology does help, but there are always new ways for identity thieves to target ATMs. If you want to stay safe from ATM skimming threats, you need to stop taking risks. And, as unfortunate as it is, that starts with no longer using a non-secure payment method, in this case, your debit or credit card!