ATM Fraud On The Rise: Staying Safe While Getting Cash

Scammers seem like they're in every part of the economy. If you make a purchase online, scammers are trying to get your credit or debit card number. If you check your email, scammers are trying to get you to download spyware. You might think you're safe conducting all your business in cash, but scammers are waiting in one location you can't get around: the ATM.
ATM fraud has long been a concern, but new advances in technology means consumers need to be more aware. Reports of ATM fraud saw a five-fold increase between 2015 and 2016. In addition, industry experts report that nearly $2 billion is lost each year due to ATM skimming. Through a variety of tactics, scammers are increasingly going after ATM-using consumers. Their targets are usually PINs, card numbers and account details. Watch out if you see any of the following at your ATM.

1.) ATMs in weird locations
The convenience of cash comes in handy in many situations. If you're out at a bar, being able to pay for a round in cash is quick and easy. At a restaurant, leaving a tip in cash can make a server's night much easier. Exchanging money between friends is a pain with credit or debit cards, but a breeze with cash. It can be tempting to use whatever ATM is handy when the need arises.
That temptation comes with some risks, though. ATMs in financial institutions are regularly monitored and maintained, not to mention covered by security cameras. A cash machine in a dimly lit corner of a bar, on the other hand, may not get that same kind of attention. Most of these machines are privately owned and the operators assume very little liability for their safety. Whenever possible, use ATMs in secure locations, like financial institutions. They're safer, better maintained and more reliable. If you must, choose ATMs in highly visible and public areas to minimize your chances of encountering a tampered machine. Only use machines inside private businesses as a last resort.

2.) Recent work
Two very common modifications are used in many ATM scam efforts. The first is a duplicate keypad on top of the existing one. This keypad relays PIN information to a third party, enabling fraud at a later time. The second is a phony card reader. This reader processes your card information, then sends it somewhere other than the machine you're using. These scams have become both more common and harder to detect as 3-D printing technology has improved and become more accessible. Molded plastic devices that fit like the original parts can be manufactured and purchased over the internet for a few hundred dollars.
There are a few telltale signs that you can use to tell the difference. First, keypads tend to wear over time. If a very old machine has bright, shiny keys, that's a sign that something's been modified. The same is true of card readers. Over time, from handling and use, card readers will develop scuffs and scratches. New-looking card readers should also be a red flag. Second, even the best molded plastic device will fit imperfectly. Scammers have to install devices in a hurry to avoid detection, so they may resort to quick fixes like electrical tape or plastic glue. Both of these will leave small signs of modification.
It's better to be safe than sorry. If you have any suspicion that an ATM has been modified, don't use it, and report your suspicion to the machine owner if possible. Exposing yourself to fraud is a lot worse than the inconvenience of finding another machine.

3.) Nearby strangers
Rather than use a lot of high-tech machinery, some scammers rely on their own senses to rip you off. Getting in line behind you, the scammer will attempt to watch you enter your PIN. If

successful, either the scammer or an accomplice will mark you for pickpocketing and then use your ATM card to clean out your account.

Even more insidious, some scammers use a distraction accomplice. Such a person might drop a bag right behind you just after you enter your PIN. They might also engage you in conversation, either offering help or asking for it. While you're distracted, the scammer grabs your card and replaces it with a phony, or just takes the cash you've withdrawn and runs.

To protect yourself from these scammers, always cover your hand when entering your PIN. Get as close as possible to the machine to obstruct potential viewing of your transaction. Keep an eye out for anyone sitting by the machine on a laptop or tablet, as they may be monitoring a camera that's designed to capture your PIN.

Most importantly, stay focused at the ATM. Ignore anyone who approaches you until you've finished your transaction and make sure you keep possession of all your belongings. They may think you're rude, but that's better than being robbed.

If you think you've been the victim of ATM fraud, it's important you report it immediately. If you report the scam within two days, your liability is capped at $50. Waiting to report the scam could mean you're responsible for all the bills the criminal racks up, so keep a close eye on your account and report any suspicious activity immediately.