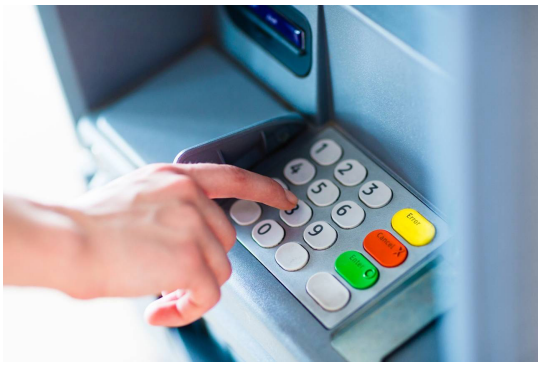
THE WALL STREET JOURNAL.

BUSINESS | JOURNAL REPORTS: TECHNOLOGY

How to Keep Thieves From Stealing Your PIN at the ATM

'Skimmers' put cameras near the machines to capture your information. But there are ways to protect yourself.



Experts say you should always cover the PIN pad at an ATM, even at a drive-through machine. PHOTO: ISTOCK

By Chris Kornelis
June 4, 2019 10:00 pm ET

Your debit cards are in danger.

Crooks are using how-to videos on YouTube and online tech marketplaces to get the skills and hardware they need to steal card data.

Most of these criminals work in groups that scope out ATMs and gas pumps, then add a piece of hardware—called a skimmer—to the ATM to capture your card information when it's swiped or inserted. This could be an attachment to the card reader that looks like a piece of the ATM, or it could be tiny, difficult-to-detect hardware placed deep inside the ATM.

JOURNAL REPORT

- Read more at WSJ.com/journalreporttech

MORE IN CYBERSECURITY

- The Quantum Threat to Encryption
- Our Emotional Attachment to Our Passwords
- Can the Sound of Your Typing Be Decoded?
- The Tussle Over Facial Recognition

Then they put a camera somewhere near the keypad to see people's PINs—such as on a false panel on the ATM or in the underside of the hood over the keypad.

Later, a member of the criminal group comes back to retrieve the skimmer device and harvest its data. Sometimes, though, the hardware is connected to a nearby computer via Bluetooth and the crooks can collect its information in real time, so they don't have to risk getting caught picking up the hardware.

"Criminals are very adept at grabbing advances in technology and using it, because their motive is making money," says Daniel Cuthbert, head of cybersecurity research at Santander. "What that means is, we're seeing the same concepts you'd expect in good manufacturing moving over to criminality."

Here are four steps to take to decrease your chances of getting skimmed:

Think twice about off-brand ATMs

Experts say small, no-name ATMs—the kind you might find in a convenience store or a gas station—are ripe for compromise, for several reasons.

For one thing, there is a lack of oversight. Jay Rosenberg, senior security researcher at Kaspersky Lab Global Research and Analysis Team, says that these ATMs are far less likely to be monitored as much as a high-traffic ATM in, say, Midtown Manhattan.

What's more, no-name ATMs are often free-standing and not built into the wall, like those at banks. That means they're easier to get inside of and thus more susceptible to skimming and other crimes, says Brian Krebs, who covers computer security and cyber crime at krebsonsecurity.com. (In fact, if you can see the top of an ATM, that's a big warning sign, he says.)

That said, third-party ATMs are hardly the only machines to look out for. Says Mr. Rosenberg: "I'm pretty sure every type of ATM has had skimmers on them."

Cover your pin (even at the drive-through)

Criminals need your card information and PIN, so they install tiny cameras to watch you entering your numbers.

"I always tell people: Cover the freaking PIN pad when you enter your PIN," says Mr. Krebs. "Having your bank-account card or account number exposed kind of sucks, but having the PIN exposed is a lot worse."

That's because without your PIN, criminals can't make ATM withdrawals, even if they can often make purchases at retailers that don't require a PIN.

And don't forget about bank drive-throughs, as awkward as that might be. Since it is obviously harder to get both hands out of the window at the drive-through, it makes it an optimal location for crooks' cameras to pick up PINs.

Don't use your debit card to access a vestibule ATM

Criminals have found a way to capture your card information at an ATM without inserting a device onto the ATM: They put one on the mechanism you use to access ATMs inside a vestibule. But Mr. Krebs says you don't actually need to use a bank card to get into a vestibule. Any old piece of plastic with a magnetic stripe should do, such as a grocery-store club card.

Track your transactions

Criminals skim because it works. Mr. Rosenberg suggests setting an alert on your debit-card and credit-card accounts to get notifications every time a transaction is made. (He says you can opt out of alerts for recurring purchases, like subscriptions.) That way, if your card is compromised, you'll know when the first purchase or transaction is made.

Mr. Kornelis is a writer in Seattle. He can be reached at reports@wsj.com.

Appeared in the June 5, 2019, print edition as 'When You Punch In Your PIN at an ATM, Somebody May Be Watching.'

- **Retirement**
- **Small Business**
- **Technology**
- **Wealth Management**