Business

This won't protect your PIN from being stolen

The statement

When using an ATM, customers should "press the cancel button twice before inserting the card. If anyone has set up the keypad to steal your pin code, this will cancel that set up."

Facebook posts, on Jan. 16

The ruling

This post claimed to be a "message from a banker" and was flagged as part of Facebook's efforts to combat false news and misinformation.

We couldn't find any reports from cybersecurity, banking or law enforcement organizations that recommend pressing the cancel button twice to prevent information from being stolen.

We spoke with Vassil Roussev, a professor of computer science at the University of New Orleans and director of its Cyber Center, an institution dedicated to research and instruction in the area of Information Assurance.

"There are relatively simple electronic devices made by different criminal groups that get reproduced and sold, and there's a fairly large number of them, so it is possible that some very simple ones could be disturbed by something like this," Roussev said, "but it should not, in any way, be taken as a safety precaution. It won't hurt you, but I would place zero value on this type of advice."

Roussev explained that many designs, particularly keypad overlays, which attach a fake keyboard over an ATM's real one, may record everything that is pressed, so pressing cancel twice or 50 times would make zero difference.

He went on to recommend that people take actual safety precautions, such as not using random ATMs or ones where they don't trust the physical security, because those are targeted by scammers most often.

Typically, crooks will use a variety of techniques to capture customers information. Here are some of the most common ones compiled from the American Bankers Association and NCR, an ATM developer.

Skimming: A slim device containing a microprocessor and flash memory that is attached to a card reader slot that copies card information as it passes the device. Once the information is captured, criminals use the details to create a cloned card.

Cash trapping: A contraption inserted into the cash-dispensing slot that blocks an ATM's shutter so that bills cannot be presented to the customer. The criminal then retrieves the cash once the customer leaves.

Card trapping: The stealing of the physical card itself through a device fixed to the ATM.

Unlimited cash-out: Malware manipulates system controls, inflates account balances and removes daily transactions limits, enabling criminals to withdraw an unlimited amount of cash.

Hidden camera: To record customer keystrokes, like the entry of a PIN, or the card's information.

Here are some of the best practices financial institutions suggest people exercise when using an ATM:

- When you're alone, avoid using ATMs in deserted areas, or ones that are obstructed from view or poorly lit.
- Be aware of your surroundings. If you notice anything out of the ordinary or suspicious, cancel your transaction and leave immediately.
- If it looks like someone has tampered with the ATM equipment in any way, don't use it and report it.
- Type in your PIN discreetly and shield the screen and keypad so others can't see.
- Put your cash, card and receipt away immediately. Count your money later where others can't see.
- When using a drive-up ATM, keep your doors locked, windows up and your engine running.
- When using an enclosed ATM that requires your card to open the door, avoid letting anyone follow you inside.
- While many ATMs are available 24 hours a day, try to go during the day.

While pressing the "cancel" button twice before using the machine doesn't have any drawbacks, customers shouldn't expect it will keep their information safe.

This claim is Pants on Fire!

Samantha Putterman, *PunditFact staff writer*

Read more rulings at PunditFact.com.