

How is ATM card information stolen? How to protect your ATM card?

According to Securedaily, many criminal cases have used the skimmer device at the ATM stop to steal. This is where users insert credit or debit cards to access ATMs.

According to Securedaily, many criminal cases have used the skimmer device at the ATM stop to steal. This is where users insert credit or debit cards to access ATMs.

1. Protection of ATMs: Do not lose new cows to worry .

In Vietnam, the situation of withdrawing money through ATM cards is increasingly complicated. The crooks often take advantage at midnight or on holidays, when both customers and banks are not paying attention, or there is little support to carry out the act of stealing money. The trick used is to install the skimmer device into an ATM card reader.



What is skimmer?

Skimmer is a tiny device that allows hackers to capture and capture actions when card users perform without requiring hackers to know too much about high-tech tricks or computers. Typical recently used ATM Skimming devices have the function of capturing data contained on the strip from the back of the ATM card as well as the number of PINs that the user entered when performing the transaction.

The path to the step of crime

To steal such information, cyber criminals have installed skimming devices on the **ATM Card Card Access Control** and a camera pinhole hidden at the ATM keyboard. The kimmer device on the ATM door will record the information of ATM cards and the camera pinhole is responsible for recording the PIN that the victim entered. Using this information, thieves can easily withdraw victims' cash in minutes.

How to protect yourself?



On the bank side:

To prevent, limit the risk of loss to users when performing transactions at ATMs. Banks must equip devices to prevent and copy card holder information at ATMs such as: *Flaudulant Device Inhibitor* for NCR; **USCRT** (*Unti Skimming Card Reader Throat*) device for Wincor Nixdorf machine; **Enhanced Card Benzene** for Diebold machines, etc. With this device, criminals will not be able to install additional devices attached to the card reader at an ATM. Translate.

ATM firms like **NCR, Wincor, Diebold, Triton** . also have blocking solutions. In the last 1 or 2 years, banks in Vietnam have implemented anti-fraud technologies at ATM. In addition to the hardware modules FDI, USCRT and Enhanced Card Benz, the ATM card reader itself has built-in features to prevent information theft on ATM cards. However, ATM cards use a magnetic slot that is prone to read theft if there is a reader (*not necessarily ATM*).

For customers who withdraw money at ATM:

1. Do not expose ATM card passwords, account number information, account holder names or store in unsafe places.
2. Always cover the keyboard when entering the ATM card's PIN / PIN.
3. ATMs should be chosen near banks, protected and many people withdraw to minimize risks.
4. When withdrawing money, check the keyboard and look around the ATM to see if anything is wrong. If you find the keyboard stiffer than usual or have any suspicious signs, you should no longer use the ATM and need to report it to the bank for inspection.
5. If you suspect that your password or PIN has been compromised, you need to change your password immediately.
6. It is recommended to register for a service to change bank account balances via mobile phones to quickly detect cases of irregular withdrawals and notify banks immediately.
7. Withdrawing money without using ATM cards at ATMs that are suspected to be unsafe and risky. Currently Techcombank is a bank that provides cash withdrawal services at ATMs without a card, you may consider using this service.

See more:

1. Basic banking services: accounts, cards, account numbers

2. How to calculate bank loan interest rates in May
3. Online banking account security methods
4. How to check which bank branch of your ATM card?

You finished reading the article "**How is ATM card information stolen? How to protect your ATM card?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
