How Debit Card Fraud Happens — and How to Avoid It

For many people, debit cards are the perfect plastic. They offer most of the conveniences of credit cards with no risk of accumulating debt.

But like credit cards, debit cards are vulnerable to rip-off artists. And debit card fraud is particularly scary because thieves can withdraw money directly from your checking account.

Here's how debit fraud happens and how to protect yourself.

How identity thieves operate

Debit card fraud can be sophisticated or old-school. Thieves use techniques including:

- **Hacking.** When you bank or shop on public Wi-Fi networks, hackers can use keylogging software to capture everything you type, including your name, debit card account number and PIN.
- **Phishing.** Be wary of messages soliciting your account information. Emails can look like they're from legitimate sources but actually be from scammers. If you click on an embedded link and enter your personal information, that data can go straight to criminals.
- **Skimming.** Identity thieves can retrieve account data from your card's magnetic strip using a device called a skimmer, which they can stash in ATMs and store card readers. They can then use that data to produce counterfeit cards. EMV chip cards, which are replacing magnetic strip cards, can reduce this risk.
- **Spying.** Plain old spying is still going strong. Criminals can plant cameras near ATMs or simply look over your shoulder as you take out your card and enter your PIN. They can also pretend to be good Samaritans, offering to help you remove a stuck card from an ATM slot.

Smart ways to protect yourself

Adopt these simple habits to greatly reduce your odds of falling victim to debit card fraud:

- **Be careful online.** Shop and bank on secure websites with private Wi-Fi. If you must shop or bank in public, download a virtual private network to protect your privacy.
- **Monitor your accounts.** Review your statements and sign up for text or email alerts so you can catch debit card fraud attempts early.

- **Don't ignore data breach notifications.** The majority of identity theft victims received warnings that their accounts might have been breached but did nothing. If you get one of these messages, change your PIN and ask your provider to change your debit card number. You can also ask one of the major credit card bureaus to place a fraud alert on your file.
- **Inspect card readers and ATMs.** Don't use card slots that look dirty or show evidence of tampering, such as scratches, glue or debris. And steer clear of machines with strange instructions, such as “Enter PIN twice.”
- **Cover your card.** When using your debit card or typing your PIN at an ATM, block the view with your other hand. Go to a different location entirely if suspicious people are hanging around the ATM, and if your card gets stuck, notify the financial institution directly rather than accepting “help” from strangers.

Even if you've taken precautions, debit card fraud can still happen. If your card gets hacked, don't panic. Tell your bank or credit union right away so you won't be held responsible for unauthorized charges, and file a complaint with the Federal Trade Commission.