Image credit: shieldyourpin.org

Did you know that someone can steal your card information without it ever leaving your possession?

Victims of credit and debit card skimming often don't even realize their information is in jeopardy until they see fraudulent charges or unauthorized withdrawals on their account. That's why it's important to be informed about ATM and point-of-sale security.

What are card skimmers?
Card skimmers are small devices placed by thieves onto point-of-sale card readers, such as the ones you use to pay at gas pumps. These skimmers capture and store all the information stored in your card's magnetic strip, including your card number, expiration date, and full name. Sometimes thieves even place a small camera nearby to record you entering your PIN. Thieves can then use this information to steal from you, create a counterfeit card and sell your information online.

Where are card skimmers found?
Unmanned ATMs aren't the only place where card skimmers can steal your information. Sometimes retail and restaurant workers, who regularly handle cards, use a skimmer to obtain your card information during a normal transaction.

How to identify a card skimmer
So how can you spot a card skimmer before it's too late? It can be tough to do since skimmers are built to blend in with the machine they're placed on. However, if you know what to look for, you've got a better chance of avoiding identity theft.

Check for signs of tampering:

1. Look at the ATM and wiggle the card reader and PIN pad. Also, look to see if the card reader or PIN pad are different colors than the rest of the ATM, or if the logos and arrows on the ATM do not line up with the card reader or PIN pad. If any of the components seem loose or out of place, contact the owner of the ATM and use a different ATM.

2. Check the panel. Skimmers typically fit right over the existing card reader, so if you notice that the reader sticks out past the face of the rest of the machine, don't use it. If you're at a gas station, you can compare your reader to the ones at nearby pumps to see if something is out of the ordinary.

3. Is the card reader unstable? The reader should be securely held in place. If it moves when you use it, that's a warning sign it could have a skimmer on it.

4. Is the security seal broken? Most gas stations place a security sticker across the gas pump to let you know whether the panel on the fuel dispenser has been tampered with. If the seal is broken, that's a sign that someone has broken into the panel. Don't use that pump and alert the gas station attendant.

5. Is the keypad abnormally thick? Skimmers can also place a fake keypad on top of the real one to capture your PIN and ZIP code. If you're having trouble pushing the buttons, stop using that card scanner.

Remember to shield your PIN. One way to protect your card information is to use your hand to shield your PIN number from being recorded while you type it on the keypad. If the fraudsters do not have your PIN, they can't access your cash.

It's also a good idea to monitor your account activity. If you suspect there is fraudulent activity on your account, report it immediately to VANTIV, our card services provider, at 1-800-808-6402 for assistance. Next, contact BVSCU to let us know about the suspected fraud on your account. We will deactivate the compromised debit or credit card, and send you a new card and PIN.

For more tips on how to prevent fraudulent charges on your account through card skimming, visit shieldyourpin.org.