



How to Keep Your Debit Card Transactions Safe

With Holiday shopping picking up, debit card scams and frauds are also on the rise. Debit cards may also be at risk of skimmers, devices disguised and attached to card readers or ATMs that steal your card number and personal identification number (PIN). It's important to be extra vigilant during this season to ensure that your debit card transactions are secure and protected. Don't be afraid to use a debit card; shopping with a [debit card](#) is convenient, safer than carrying cash, and is just as safe as using your credit card. With these safety tips in mind, you can enjoy crossing items off your gift list without fear of fraud.

Check your account activity often

The best way to be protected is to stay informed. Checking your bank account activity regularly, at least once a month, allows you to know right away when something doesn't look right. It's a good practice to keep your receipts and compare them to your account activity to make sure nothing is out of place. If you do notice unauthorized purchases on your account, debit cards can be easily frozen, canceled and replaced, even remotely if you're travelling. Using [mobile banking](#) is a great way to monitor activity on the go.

Use your debit card as credit

To prevent suspicious persons from stealing your PIN while out shopping, use your debit card as credit in stores to avoid having to enter your PIN. Using your debit card, in this way, provides you with the same protection and backing as a credit card provides. Your debit card is also equipped with an EMV chip that adds an extra layer of security when making transactions. The chip encrypts your information by creating a one-time code at a chip-enabled terminal to complete the transaction.

Protect your PIN

Your debit card PIN provides you with an additional verification step that increases security. But, don't carry your debit card PIN with you -- in your purse, wallet, pocket, or anywhere else. The best practice is to have it recorded in one secure location at your home and memorize it for use when making transactions. It's also a good idea to conceal the pad as best as you can when entering your PIN to prevent anyone else from seeing it. Be aware that scammers may go so far

as to go through discarded paper, so don't write your PIN on any papers that you may lose. A good practice is to shred any paper [bank statements](#) or containing important personal information. Treat your PIN like cash to keep your debit card transactions safe.

Use secure ATMs

Debit cards are at particular risk of skimmers, so use [ATMs](#) only at a bank or credit union, rather than at convenience stores, gas stations, or other stand-alone locations. These spots are more likely to have a skimmer attached and have fewer cameras and security measures.

Shop on secure websites

Online shopping is convenient, but make sure you're shopping on a secure website. Look for the closed padlock icon in the address bar of your web browser. It's also a good idea to shop only on your home's password-protected Wi-Fi. Public Wi-Fi and unsecured hotspots may be used by scammers to steal your personal information.

Stay aware of scams

Knowing the red flags for common scams can keep you secure, as scams are becoming more frequent and harder to detect. Be alert that scams can come through a variety of channels, including phone, email, social media, online, mail, and text. Watch out for anyone asking you to provide your debit card number, PIN, or bank account info over email, as no legitimate business will ask you to do that. Look for misspellings or poor grammar which is a common sign of a scam. If a communication is unusual or unprompted, pause and don't give out any personal information to an unknown sender, including your full name, birth date, or social security number. Don't respond to any scams or click on any unknown links; just immediately delete the communication.

Report fraudulent charges immediately

Like credit cards, debit cards are protected with limit liability under the Electronic Fund Transfer Act (EFTA), but the longer you wait to report fraudulent activity, the more likely it is you will have to pay for those transactions yourself. The faster you act, the better! Report [lost or stolen cards](#) or unauthorized transactions immediately to avoid any repercussions.