



Stay One Step Ahead

Stay One Step Ahead

Understand the various ways fraudsters try to obtain your personal and debit card information. The more you know, the more you can stay one step ahead of fraud.

Personal information:

Phishing's a scam in which fraudsters pose as legitimate businesses to trick you into divulging your social security number, account numbers, passwords or other sensitive personal information.

Hiding behind the anonymity of emails and phone calls, the fraudsters pretend to be reputable financial institutions, credit card companies, online service providers, retailers, etc. They'll try and convince you there's an immediate need to update your financial information.

Steps to take:

- Remember: no legitimate business will request this type of information.
- Don't give out your personal information.

Card safety:

Follow these simple steps to keep your debit card and financial accounts safer.

Steps to take:

- Use your PIN whenever possible.
- Set up fraud alerts through online banking and mobile apps.
- Review financial accounts and statements regularly.
- Sign your card on the signature panel.
- Report lost or stolen debit cards to us immediately.

ATM security:

Be vigilant at ATMs. If something seems suspicious, contact us immediately.

Steps to take:

- Cover the PIN pad with your hand while entering your PIN.
- Use familiar ATMs in well-lit areas.
- Tug the card reader before inserting your card and look for skimmers.
- Don't use the ATM if the card slot or keypad look suspicious.

Online shopping:

When shopping online, be aware of ways to avoid undue risk and keep your personal information free from fraud.

Steps to take:

- Shop with trusted brands. Look for the green padlock icon and HTTPS:// to ensure you're on a secure website.
- Never give private information, such as your social security number, passwords, or birthdate to anyone online.
- Create strong passwords with more than eight characters, an uppercase letter and at least one number and/or special character.
- Use and update firewall software to protect your computer's information.
- Avoid free or special product offers — these are usually too good to be true.

If you suspect identify theft or fraud, contact us immediately so we can help!