

ATM & Debit Card Safety Tips

Technology offers convenience, but it doesn't replace common sense. These habits can keep you and your money safe while you're using an ATM or Debit card.

1. Protect your PIN (Personal Identification Number)

- Choose a PIN that is unique. Use a number other than your birthday, Social Security number or other obvious number.
- Do not share your PIN or account number with anyone.
- Sign Immediately. As soon as your card arrives in the mail, sign the back and keep in a safe place.

2. Check out the environment as you approach the ATM.

- Avoid facilities in dark or remote places.
- Avoid free standing ATMs on street corners. It is best to use an ATM machine at a financial institution.
- If bystanders seem to be loitering rather than conducting business, go to another machine or come back later.
- If someone seems to take interest in you or your transaction, report suspicious behavior to the police – but leave the area first.
- When using a drive-through ATM, keep all doors locked and all windows up, except for the driver's window.

3. Examine the ATM before you use it.

- Never enter your PIN in any terminal that does not look genuine, has been modified, has a suspicious device attached, or is operating in a suspicious manner. See below for ATM Scams.

4. Be prepared to conduct your transaction when you approach the ATM.

- Have your card ready and know what transaction or transactions you want to conduct.
- Shield the screen and keypad with your body as you use the ATM to prevent others from seeing your PIN.
- Remove your cash, receipt and card after every transaction. Never leave receipts behind at the ATM.
- Have any deposits prepared before you approach the ATM. Make sure the ATM envelope has been accepted before leaving.

5. Pay attention to activity around the ATM as you leave.

- Secure any cash you withdraw before leaving the machine.

6. Report lost, stolen, or compromised cards IMMEDIATELY!

- If you believe that your card and/or PIN has been lost, stolen, compromised, or that someone has transferred money using your account without your permission.
- Examine your statements promptly to identify unauthorized transactions.

ATM Safety Tips:

- Never give your card to someone at an ATM for any reason.
- Never let anyone assist you at an ATM, even if they appear to be a bank official or security personnel.
- Beware of people standing close to you when you are conducting transactions at an ATM.
- Ensure you hide your pin when keying it into an ATM.
- Never use an ATM that looks tampered with or damaged.
- Always use an ATM in a well-lit area.

There are 4 places you should beware of using a debit card at all costs:

- Independent ATMs - You run the risk of skimmers. While skimmers can be found on bank ATMs, they're less likely because there are often security cameras in place.
- Pay at the pump - Be aware of panels on the pump that are loose or crooked. Skimmers aren't the only danger to your wallet. The gas station along with hotels and car rental businesses will put a hold on your account that could cause your checks to bounce. If you must pay with debit at gas station, go inside and pay at the cashier.
- When you're buying online - Credit card is a much better option. If you don't get your merchandise, you can do a chargeback during a 60-day window.
- At a restaurant - Keep your card in sight at all times even when processing. Giving your card to someone is like giving them your wallet.

SAFETY TIPS WHILE USING APPS

- It is not recommended to use cash apps with strangers.
- Use a credit card not your bank account gives you some recourse.
- Set a cash PIN and enable Touch ID/Face ID.
- Use different passwords for all accounts.
- Encrypted data and options like CVV entry add a layer of protection.
- Always enable two-factor authentication when available.
- Make sure your phone has a passcode lock.
- Set an account security password with your mobile network provider.
- Beware of phishing; do not open or click to unsolicited emails with links or attachments nor matter how legitimate they look.
- Never store cardholder data on any systems online.
- Always expect and look for notification after a transaction and verify its validity.