It's important to be proactive and keep your debit card accounts safe to avoid identity theft. Here are five tips to help you protect your debit/credit cards so that you can keep your account and personal information safe.

Debit/Credit card safety tips:

- **Start early**
- **Don't share account information**
- **Stay secure online**
- **Watch out for phishing**
- **Report fraud ASAP**

How to protect your debit/credit card

1. Start early

By setting a good security foundation early, you can potentially avoid identity theft and credit card fraud.

- **Choose a secure PIN:** Never use personal information, such as part of your social security number or the date of your birthday for your PIN (personal identification number).
- **Turn on account alerts:** Turn on account alerts to be notified of potential fraud on your card via phone, text or email. You can get alerts to detect charges that are unauthorized in addition to other suspicious activity.
- **Sign the back of your card:** Sign the back of your card as soon you receive it. This can allow merchants to compare the card signature with the receipt signature to make sure they match.

2. Don't share account information

Be cautious of sharing account information as it can easily fall into the wrong hands.

- **Never email account information**: You should never email your debit/credit card number or account information. If a merchant asks you to, you should immediately be suspicious.
- **Don't say account information where others can hear it**: If you need to give your debit/credit card information over the phone, be sure to do it in a private space.
- **Never give your social security number:** You'll never need to give out your social security number for everyday purchases. If someone asks you for it, you should be suspicious.
- **Shred docs or go paperless:** Don't just throw out old debit/credit card statements and bills; shred them so no one can get a hold of your account information. Better yet, go paperless.

3. Stay secure online

Be mindful of the best security practices for shopping online, which include:

- **Never store debit/credit card information on a website:** If a website asks if you'd like to store your information, say no. You should also avoid storing your card information on autofill on your computer.
- **Only shop https:** The 's' after http stands for 'secured' and means that the information you're sharing is encrypted.
- **Never use public WiFi:** With public WiFi, anyone will be able to view your encrypted data. You should only shop online on a secure network.
- **Use an online payment system:** Online payment systems like PayPal can add an extra layer of security to your online transactions.
- **Log off when you're finished:** Always be sure to log out of a website whenever you're finished. This is especially true if you're using a shared computer.

TEXAS PEOPLE FEDERAL CREDIT UNION

4. Watch for phishing

Phishing refers to fraudulent attempts to steal your account information. Examples of phishing include forged links or emails from addresses that you don't recognize. To avoid becoming a phishing victim, be sure to:

- **Never give out information on a call you didn't initiate:** If you get a call from your bank asking you for your account information, you should immediately be suspicious. Your bank will never call or text you for information to verify your account, send you a link claiming to be a new version of their online app or ask you for password security information like the street you grew up on. Even if the number calling you appears to be from your bank, it can still be a phishing scam.
- **Don't click on links from addresses you don't recognize:** A common phishing technique is to send a link that appears to be from a legitimate bank or company. If you click the link, your data could be stolen.
- **Report suspicious emails immediately:** If you receive a suspicious email, report it immediately. Some hints that an email is fraudulent include typos, extra spaces and an email address that varies only slightly from a legitimate address.

5. Report fraud ASAP

If you notice fraud on your account, report it to your credit union as soon as possible.

- **Call your credit union immediately:** Report fraud to your credit union as soon as you can. If you clicked on a link from an email that turned out to be a phishing scam, forward a copy of it to your credit union so they have as much information as possible to help you.
- **Double check receipts:** Always double check receipts and make sure they match what's posted on your account. This can help you quickly spot unauthorized charges.
- **Never leave receipts behind**: Never just throw out or leave receipts behind. File what you need to keep and shred the rest to help protect your private information.
- **Always keep a list handy:** Maintain an updated list of your debit/credit cards and their account numbers, as well as the customer service numbers of your credit union. This will be enormously helpful if your cards are ever stolen.