



Plastic Card Protection Basics... Stay Safe by Staying Alert

Protecting yourself can be as simple as keeping your eyes and ears open. Here are some proactive steps to keep your financial information secure.



General Information

Do regular reviews

You can catch unauthorized transactions early by checking your account details regularly — at least once a week.

Get your credit report

It's your credit, so make sure no one else is using it. Check to ensure there aren't activities listed that you didn't initiate.

Card and PIN safety

Report lost or stolen cards immediately.

Sign your card on the signature panel as soon as you receive it.

Protect your cards as if they were cash.

Don't leave your credit cards in the glove compartment of your car. An alarmingly high proportion of all credit card thefts occur in glove compartments.

Never write down your PIN—memorize it. Also, never use your PIN as a password.

Ensure that you get your card back after every purchase.

Always check sales vouchers for the correct purchase amount before you sign them, and keep copies of your vouchers and ATM receipts.

Always check your billing statement and verify the amounts of your purchases.

Make a comprehensive list of all your cards and their numbers and store it in a safe place.

Don't volunteer any personal information when you use your credit card, other than by displaying personal ID as requested by a merchant.

Don't lend your card to anyone. You are responsible for its use. Some credit card misuse can be traced directly to family and friends.

Never disclose your PIN to anyone. No one from a financial institution, the police, or a merchant should ask for your PIN.

ATM safety

Using your Debit card at the ATM is a convenient and safe way to get cash. Just be sure to keep in mind the following safety tips:

Watch your surroundings

If the machine is poorly lit, or in a hidden area, use another ATM.

Guard your PIN

Keep a lookout for suspicious activity. Always guard your PIN and transaction amount, and immediately cancel your transaction and leave if you see something suspicious.

Keep your card ready

Avoid counting cash, or rummaging through personal items, while standing at the ATM.

Be safe at the drive-thru

When using a drive-through ATM, lock car doors and other windows—when walking up, never leave your car running or unlocked.

Take your receipt

Always take your receipt. It contains personal information that could be helpful to thieves.

Avoid strangers

When using an indoor ATM that requires your card to open the door, avoid letting unknown people in with you.

Online safety

The Web can be a great place to find information, but be extra cautious about the information you give. Here are just a few tips on what to think about while online.

Never send account information, such as your account number or PIN, in the body of an email. You never know who could be intercepting it.

Beware of phishing emails. These are emails that appear to be from your credit union or an online merchant asking you to provide your account information. These emails are bogus. Reputable financial institutions and merchants will never ask for any account or personal information in an email.

Never click on Internet links within emails. Instead, type the known URL.

Before making purchases online, be sure that the site has built-in security features to protect your account information. All reputable merchant sites use encryption technologies that will protect your private data from being read by others as you conduct an online transaction.

When using a public computer to shop online or access your account(s), always remember to log off and quit the browser when you are finished. All it takes for someone to view your personal information is simply hitting the back button.

Protect information by only using a computer that has a firewall in place.

Implement anti-spyware and anti-virus software updates as soon as they're available.

Mail and phone safety

Mail and telephone solicitations bring many tempting offers, but not all are legitimate! Be especially careful about deals that sound too good to be true, and keep the following advice in mind:

Never give your account information to anyone claiming to be from Visa or your credit union unless you initiated the call.

Be wary of high-pressure sales tactics, especially if the sale must be completed immediately.

Record the name, address, and phone number of the soliciting organization, and obtain names of other customers who can supply references.

Ask questions. The fewer questions a telemarketer can answer, the less likely that he or she is calling from a legitimate business.

Do not give your account number, including the codes on the signature panel, to anyone over the phone unless you initiated the call. When in doubt, consult the Better Business Bureau or the U.S. Postal Inspection Service.

Notify the Post Office immediately if you change your address.

Make sure your mailbox is secure, and promptly remove delivered mail.

Call the Post Office immediately if you are not receiving your mail.

If you are told of a forwarding order placed on your mail without your knowledge, go to the Post Office to check the signature and cancel the order.