

Victim of Fraud?

Act as soon as possible | Inform your financial institution immediately if you believe your account or personal information has been compromised or stolen.

Protect your accounts | If your account has been compromised, change your passwords, cancel your debit or credit card, or in some instances, close your account and reopen a new one.

Protect Yourself

Identifier Word | Determine a safe word and share it with your family. When you receive a questionable call, ask the caller to confirm the word. Do not share this word with anyone.

Account Access | Limit access to your financial accounts by considering the number of joint owners on your account and who you grant access to.


Secure Passwords | Use a minimum of 12 characters, a mix of lowercase and uppercase letters, and add special characters and symbols to secure your online accounts.

Online Resources

Banzai! Financial Education | Visit westconsin.banzai.org/wellness for dozens of free online financial education resources.

BaZing | As a benefit of WESTconsin's Preferred Checking account, members have access to WESTconsin Rewards, which includes Credit Monitoring, Payment Card Fraud Resolution, Identity Restoration, and Identity Monitoring. Visit westconsincu.org/personal/preferred-checking/ to learn more.

Federal Trade Commission | If your personal identifiable information has been compromised, visit identitytheft.gov to report the fraud and start a recovery plan.



Scams, Schemes,

And everything in-between

WESTconsin[®]
CREDIT UNION

Phishing

Phishing is when scammers impersonate a person or business to gather sensitive information or access to a person's funds through a credit card or bank account. Phishing scams can include emails, texts, and even fake websites. Often, you'll get an email or text informing you that there's been a problem with your account or an offer for a great deal from a company you know and trust.

TIP: Navigate to a separate browser or use a different device to visit the official website to review your account or check out the offer.

Grandparent Scams

Grandparent scams occur when a scammer impersonates a grandchild or relative, convincing the victim that they are in trouble or in danger. Scammers will request a wire transfer, money transfer, or even gift cards to help them out of trouble. Scammers will often research the victim and their family members on social media prior to calling to provide identifying information that could make the scam seem more believable.

TIP: Hang up the phone and call the person in question or a family member to verify the legitimacy.

Things to Remember

Scammers are professionals and use advanced technologies and various tactics to perpetuate fraud. Keep an eye out for:

- ✓ **Spoofing:** Scammers can use fake Caller ID to appear as a legitimate phone number. Just because a name or business appears on your Caller ID does not make it a legitimate caller.
- ✓ **Artificial Intelligence** can be used to impersonate voices over the phone.
- ✓ **Smishing and Email Phishing:** Fraudsters will often use text messages and emails, posing as reputable companies or financial institutions, to convince victims to reveal personal information such as passwords, one-time codes, or credit card numbers. Fraudsters often promise prizes and gifts in spam messages. Be skeptical of any email or text claiming you've won a prize.

REMEMBER, hang up and directly call the person or company in question. *WEST*consin Credit Union will never ask for your account number or Social Security number over the phone.

Charity Scams

In charity scams, donations are solicited for fake charities and are often designed to pull on your heartstrings, mostly profiting on major tragedies or natural disasters.

TIP: Never make donations over the phone and instead, ask the caller to send you more information. If it's a legitimate organization, this won't be a problem.

Medicare Scams

The Medicare scam often involves a caller pretending to work for Medicare or a healthcare insurance provider. The caller may ask for your personal or financial information to continue services, add additional benefits, or activate your Medicare card.

REMEMBER, Medicare will never call you and ask for your bank account information.

Romance Scams

A romance scam occurs when a scammer adopts a fake identity to gain the victim's affection and trust. Romance scams start in a few different ways, but most commonly start online on legitimate dating apps or websites. Scammers will spend time getting to know the victim and developing trust before asking for a loan or for access to their finances.

REMEMBER, never assume a person that you have only met online is who they say they are.

Malware or Ransomware

Some scams will install malware or ransomware on your device when you click harmful links. When this happens, your device could be infected with a virus that steals your information or forces you to pay to regain access to your sensitive information. Harmful links can come from:

- ✓ Popups
- ✓ Ads
- ✓ Posts on social media
- ✓ Emails
- ✓ Messages from the accounts of friends or family that have been hacked.

TIP: You should always be wary of clicking on any link that someone sends you unprompted, particularly if they use generic language or don't sound like themselves.