fraud prevention guide

canopy
credit union

what's inside

what is fraud & why it matters

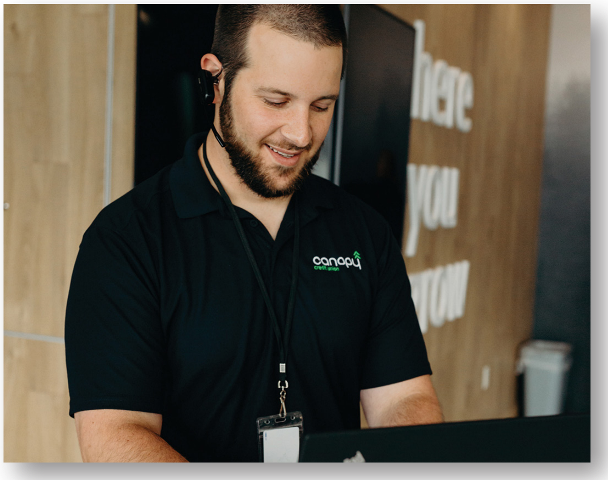
1.

Fraud is when someone uses deception to trick you into sharing personal information, sending money, or granting access to your accounts. These schemes can come through phone calls, emails, text messages, social media, or even face-to-face conversations.

At Canopy Credit Union, safeguarding your money is our highest priority. But often, the first line of defense is you. By protecting sensitive details like your debit card number, PIN, and online banking password, you help keep your finances out of the hands of fraudsters.

Staying alert, asking questions, and knowing the red flags makes all the difference in securing your account. And remember—you're never alone. If you're ever unsure, call Canopy Credit Union directly at (509) 328-2900. We're always here to answer your questions and offer guidance.

2. stay S.A.F.E.



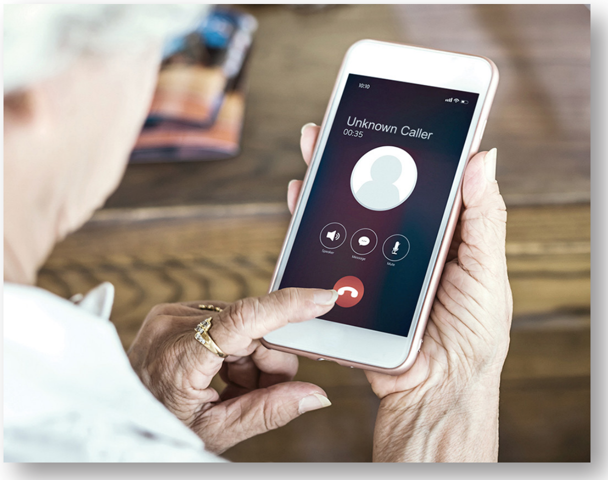
S: stay calm

Fraudsters thrive on fear. They may say your account is at risk, claim you'll be fined, or even arrested if you don't act immediately. If this happens to you, pause. Take a moment to breathe. The calmer you are, the harder it is for scammers to trick you into taking hasty actions.

A: ask for help

You never need to figure this out alone. If you're suspicious, cut off contact with whoever is asking you for information and call Canopy directly—even if the person calling you claims to be from Canopy Credit Union. We will never be upset with you for hanging up the phone and confirming our identity.

Fraud prevention can feel overwhelming, but it doesn't have to be. Remember this simple acronym: **S.A.F.E.**



F: find the facts

Scammers will try to deceive you by using fake information that looks official. Instead of taking their word for it, get verification through trusted sources. Modern technology can allow scammers to imitate Canopy's real phone number, so the best thing to do is dial Canopy's line directly at (509) 328-2900 for accurate information.

E: exit the conversation

You don't need to explain yourself to a scammer. Hang up the phone, delete the text, or close the email. Saying "no" is one of the strongest tools you have.

3. common scams to watch out for

Fraudsters may use different stories, but most scams follow familiar patterns. Here are some of the most common ones:

SPOOFED PHONE CALLS

The number on your caller ID looks like it’s from your credit union, the IRS, or another trusted organization. The caller insists they need information immediately to “verify” your account. Though they masquerade as a trustworthy source, this caller is a scammer in disguise.

ROMANCE SCAMS

Someone you connect with online quickly gains your trust and affection. Once you feel connected, they claim to have an emergency, such as medical bills, travel expenses, or family crises, and ask you to send money. Romance scammers trick innocent people into giving away money or sensitive information. Some romance scammers will impersonate celebrities or steal photos from real people.

GIFT CARD SCAMS

You’re told to pay a fee, fine, or bill using gift cards. The scammer may attempt to stay on the phone while you buy the cards, then ask you to share the numbers on the back. Once the scammer has the gift card information, they can use it to purchase whatever they want. If you pay a scammer through a gift card, reimbursement is rare—sometimes impossible.

FAMILY EMERGENCY SCAMS

You get a frantic call or text from someone claiming to be a loved one who says they’re in trouble and have an immediate need for money and secrecy. They could be a partner, child, or grandchild. The voice on the phone may sound exactly like the person you care about, but this caller is actually a scammer using technology—such as AI—to mimic the voice of someone you know in real life.

LOTTERY OR PRIZE SCAMS

You’re told you’ve won a prize or sweepstakes, but to collect it, you must pay taxes or fees up front. The prize never arrives, but the scammer receives your money. Sometimes scammers send a fake check and ask you to deposit it, then ask you to send money back.

TECH SUPPORT SCAMS

A pop-up on your computer says it's infected, or you get a call from "Microsoft" or "Apple" claiming they need remote access to fix the problem. While "helping" you, the scammer posing as a legitimate service charges you a fee or installs malware on your device.

EMAIL & PHISHING SCAMS

You get an email that looks like it's from a trusted source—your bank, a retailer, or even a coworker—asking you to click a link or enter your login. These messages often look professional but contain small errors or unusual requests. Clicking or "logging in" through the link compromises your device or account, putting your financial safety at risk.

If you recognize these tactics and suspect you may be dealing with a scammer, **report it.** Contact Canopy Credit Union and tell us everything. We are here to help and protect your account.

scam red flags 4.

Watch for these warning signs:

- Urgency or pressure: "Act now or lose your money!"
- Requests for secrecy: "Don't tell anyone, especially your credit union."
- Unusual payment methods: gift cards, wire transfers, cryptocurrency.
- Unfamiliar links or attachments in emails or texts.
- Caller ID tricks: number looks local or official but doesn't match the real source.
- Too good to be true offers: surprise prizes, sweepstakes, or inheritances.
- Requests for sensitive details: PINs, passwords, or one-time codes.

If you notice even one of these red flags, pause. Trust your instincts and reach out to Canopy—we'll help you confirm what's real and what's not.

if you suspect a scam

Stopping a scam early makes all the difference. If you're unsure about something you've received or experienced:

- Stop communication immediately. End the call, close the email, and ignore the text.
- Document the details. Write down the phone number and take screenshots. Don't click on any links.
- Report it. File a report with the Federal Trade Commission (FTC) and let Canopy know what happened.
- Check with us. We'll review your accounts and confirm if everything is secure.

5.

If you realize you've already given away money or information, remember you have nothing to be ashamed of. Scammers are professional manipulators, and many smart people have been caught in their traps. What matters most is acting quickly when you realize you may have been the victim of a crime.

Here's what to do:

1. **Call Canopy immediately.** We'll block cards, freeze accounts, and walk you through your options.
2. **Secure your information.** Change your online banking password, update your PINs, and check your account activity.
3. **Report it.** File a report with the Federal Trade Commission (FTC) at reportfraud.ftc.gov. If money has been sent, alert the local police.
4. **Protect your credit.** Place a fraud alert or freeze with the three major credit bureaus if your personal details were compromised.
5. **Talk it over.** Share what happened with trusted family, friends, or a Canopy team member. You'll find support and it may help protect others by speaking up.

if you've been scammed

6.

7. quick do's & don'ts

Do:

- Verify unusual requests through official channels.
- Set up account alerts so you know about changes right away.
- Call Canopy whenever something feels uncertain.

Don't:

- Share your PIN, online banking password, or security codes.
- Pay anyone with gift cards, wire transfers, or cryptocurrency under pressure.
- Let fear or urgency force you into quick decisions.

how scams play out: two different endings

8.

Most scams follow the same script. Here's what it looks like when fraudsters succeed—and what happens when you take the S.A.F.E. approach instead.

When the Fraudster Succeeds

1. **The Hook:** A call or message arrives claiming to be from your credit union.
2. **The Pressure:** The caller says your money is in danger and you must act immediately.
3. **The Ask:** They request your PIN, debit card number, or a one-time passcode.
4. **The Loss:** Once you provide it, they quickly move your money out of your account.

When You Stay S.A.F.E.

1. **The Hook:** You receive the same type of call or message.
2. **The Pause:** You stay calm and remember that urgency is a red flag.
3. **The S.A.F.E Choice:** Instead of sharing details, you hang up and call Canopy directly at our official number.
4. **The Win:** The scam is stopped. Your funds remain safe, and you gain confidence knowing you trusted your instincts.

helpful resources & contacts

When in doubt, start with us. We'll help you sort out what's real and what's not.

- Canopy Credit Union: (509) 328-2900
- FTC Fraud Reporting: reportfraud.ftc.gov
- AARP Fraud Watch Helpline: 877-908-3360
- Credit Bureaus (Equifax, Experian, TransUnion): add fraud alerts or freezes if needed
- Local Police: for reporting financial fraud or identity theft

9.

here you grow®

canopy
credit union

P.O. Box 2519 | Spokane, WA 99220
509.328.2900 | 800.541.4310
www.canopycu.com