SCAM SURVIVAL GUIDE

PSECU®

STAY ONE STEP AHEAD OF FRAUD

Knowing the warning signs can help you recognize a potential scam before you act.

When something doesn't feel right, remember:

STOP.

Pause before you respond, share information, send money, or click.

VERIFY.

Confirm the request using an official app, website, or phone number you trust.

PROTECT.

If something doesn't feel right, end the conversation and contact PSECU at 800.237.7328.

KEY RULES TO HELP YOU STAY PROTECTED

✓ DO

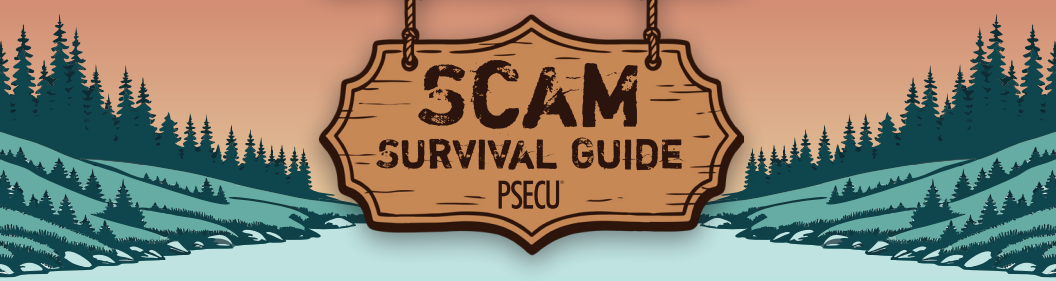
- ✓ Slow down and ask questions.
- ✓ Be skeptical of urgency, secrecy, and threats.
- ✓ Discuss major financial decisions with someone you trust.
- ✓ Review your account activity and keep alerts turned on.

✗ DON'T

- ✗ Share passwords, PINs, or one-time passcodes.
- ✗ Give personal information during unsolicited contact.
- ✗ Allow unexpected remote access to your device.
- ✗ Move money to a "safe" account at someone else's direction.

SURVIVAL TIP: TELL THE WHOLE STORY

Always be completely truthful with PSECU, even if someone tells you to keep the situation secret. Complete, accurate information can help us understand what happened and determine how to help protect you and your account.



KNOW THE MOST COMMON SCAMS

Imposter Scams

Scammers may pose as PSECU, law enforcement, government agencies, or other trusted organizations by spoofing their phone numbers. Never share verification codes or account information during a call you didn't initiate.

Investment Scams

Be skeptical of investment advice from someone who promises high or guaranteed returns. Scammers often require putting money into crypto currency or a fake trading platform. Research investments independently before sending money.

Job Scams

Fake employers may ask you to pay fees upfront, deposit a check, purchase equipment, or move money through your personal account. Verify job opportunities through the employer's official website.

Tech Support Scams

These often start as a fake email, pop-up, or unsolicited call posing as well-known tech companies, using alarming messages, flashing warnings, and claims of illegal activity to pressure you into acting quickly. Never call numbers provided in these messages or give remote access to your device, as scammers can steal sensitive information.

Friendship & Relationship Scams

Scammers often build trust through wrong-number texts and cloned or compromised social media profiles before asking for money or advertising deals that seem too good to be true. Be cautious with new and existing contacts and watch for signs that someone may not be who they claim to be.

Think You've Encountered a Scam?

Stop contact and don't send additional money. Save relevant messages, receipts, and screenshots, and contact PSECU promptly if your account or personal information may be involved.

Know Where to Get Help

PSECU: 800.237.7328 • Fraud Resources: PSECU.com/fraud
Internet-Based Crime: IC3.gov • Identity Theft: IdentityTheft.gov

Stop. Verify. Protect.