TIPS FOR SPOTTING A SCAM

Scammers *PRETEND* to be from an organization you know.

Scammers often pretend to be contacting you on behalf of the government. They might use a real name, like the Social Security Administration, IRS, Medicare, or make up a name that sounds official. Some pretend to be from a business you know, like a utility company, a tech company, or even a charity asking for donations.

Scammers say there's a *PROBLEM* or a *PRIZE*.

They might say you're in trouble with the government. Or you owe money. Or someone in your family had an emergency. Or that there's a virus on your computer. Some scammers say there's a problem with one of your accounts and that you need to verify some information. Others will lie and say you won money in a lottery or sweepstakes but have to pay a fee to get it.

Scammers *PRESSURE* you to act immediately.

Scammers want you to act before you have time to think. If you're on the phone, they might tell you not to hang up so you can't check out their story. They might threaten to arrest you, sue you, take away your driver's or business license, or deport you. They might say your computer is about to be corrupted. Anyone who pressures you to pay or give them your personal information is a scammer.

Scammers tell you to *PAY* in a specific way.

They often insist that you pay by sending money through a money transfer company or by putting money on a gift card and then giving them the number on the back. Some will send you a check (that will later turn out to be fake), tell you to deposit it, and then send them the money back.

Campus Federal will NEVER contact you from our 888-769-8841 or via text message, email or phone to ask for your account number, password or PIN. If you suspect you have been a victim of fraud, contact a Campus Federal representative **IMMEDIATELY** at **888-769-8841**.

HOW TO **PROTECT YOURSELF** FROM COMMON SCAMS

Block unwanted calls, emails, and text messages.
Take steps to block unwanted calls and to filter unwanted emails and text messages.

Don't give your personal or financial information in response to a request that you didn't expect.
Legitimate organizations will not call, email, or text to ask for your personal information, like your Social Security, bank account, or credit card numbers.

Stop and talk to someone you trust.
Before you do anything else, tell someone — a friend, a family member, or Campus Federal — what happened. Talking about it could help you realize it's a scam.

CAMPUS FEDERAL®

CampusFederal.org/learn/ | 888.769.8841

Federally Insured by NCUA and is an Equal Housing Lender.

To learn more, scan this code

To report fraud,
talk to a Campus Federal representative at 888-769-8841

Sources: Federal Trade Commission. "How to Avoid a Scam." 2020 https://consumer.ftc.gov/articles/how-avoid-scam | "Mobile Payment Apps: How To Avoid a Scam When You Use One." 2022 https://consumer.ftc.gov/articles/mobile-payment-apps-how-avoid-scam-when-you-use-one | "How to Recognize and Avoid Phishing Scams." 2022 https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams | "How to Spot, Avoid, and Report Tech Support Scams." 2022 https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams | "What You Need To Know About Romance Scams" 2022 https://consumer.ftc.gov/articles/what-you-need-know-about-romance-scams

COMMON TYPES OF SCAMS

PHISHING

Scammers use email or text messages to try and steal your passwords, account numbers, or Social Security numbers. If they get that information, they could get access to your email, bank, or other accounts. Or they could sell your information to other scammers. Scammers launch thousands of phishing attacks like these every day — and they're often successful.

If you get an email or a text message that asks you to click on a link or open an attachment, answer this question:

Do I have an account with the company or know the person who contacted me?

If the answer is "**NO**," it could be a phishing scam.

If the answer is "**YES**," contact the company using a phone number or website that you know is real — not the information in the email. Attachments and links might install harmful malware.

ROMANCE

Romance scammers create fake profiles on dating sites and apps or contact you through popular social media sites like Instagram or Facebook. The scammers strike up a relationship with you to build up trust, sometimes talking or chatting several times a day. Then, they make up a story and ask for money.

How to Avoid Losing Money to a Romance Scammer:

Here's the bottom line — Never send money or gifts to a sweetheart you haven't met in person.

If you suspect a romance scam:

- Stop communicating with the person immediately.
- Talk to someone you trust. Do your friends or family say they're concerned about your new love interest?
- Search online for the type of job the person has plus the word "scammer." Have other people posted similar stories? For example, search for "oil rig scammer" or "US Army scammer."
- Do a reverse image search of the person's profile picture. Is it associated with another name or with details that don't match up? Those are signs of a scam.

TECH SUPPORT

Tech support scammers often call and pretend to be a computer technician from a well-known company. They say they've found a problem with your computer. They typically ask you to give them remote access to your computer and then pretend to run a diagnostic test. Next, they try to make you pay to fix a problem that doesn't exist.

Two Things To Know To Avoid a Tech Support Scam:

- Legitimate tech companies will not contact you by phone, email, or text message to tell you there's a problem with your computer.
- Security pop-up warnings from real tech companies will never ask you to call a phone number or click on a link.

MOBILE PAYMENTS

Some scammers may try to trick you into sending them money through a mobile payment app. That's because they know once you do, it's hard for you to get your money back.

Scammers might pretend to be a loved one who's in trouble and ask you for money to deal with an emergency. Others might say you won a prize or a sweepstakes but need to pay some fees to collect it.

Keep this advice in mind if you send money through a mobile payment app:

- Don't send a payment to claim a prize or collect sweepstakes winnings.
- Don't give your account credentials to anyone who contacts you.
- Protect your account with multi-factor authentication or a PIN.
- Before you submit any payment, double-check the recipient's information to make sure you're sending money to the right person.
- If you get an unexpected request for money from someone you do recognize, speak with them to make sure the request really is from them — and not a hacker who got access to their account.

At Campus Federal, your safety is our highest priority. We've partnered with Merchants Information Solutions, Inc. to offer you identity theft monitoring, resources, and recovery services with Fraud Defender at campusfcu.merchantsinfo.com/