CAMPUS USA credit union

HOLIDAY FRAUD AWARENESS

HOW TO SPOT AND PROTECT YOURSELF FROM SEASONAL SCAMS

Seminar Objectives

Common Scams

How do they do it?

What you can do

- How to Avoid Being Scammed
- Tips to Protect Yourself
- Who to Report it to

SPOOFING PHONE CALLS

- **Impersonation:** Scammers pose as representatives from banks, credit card companies, delivery services, or charities, often with urgent or alarming messages.
- **Phishing for Information:** Callers request sensitive details like Social Security numbers, credit card information, or bank account numbers.

Caller ID can be faked

Verify the legitimacy of the caller by hanging up and calling the organization back using the official phone number from their website or billing statement.

SPOOFING PHONE CALLS

An real-life example:

FTC says:

“Don’t answer calls from numbers you don’t recognize. If it’s important, they’ll leave a message.”

PHISHING EMAILS AND TEXTS

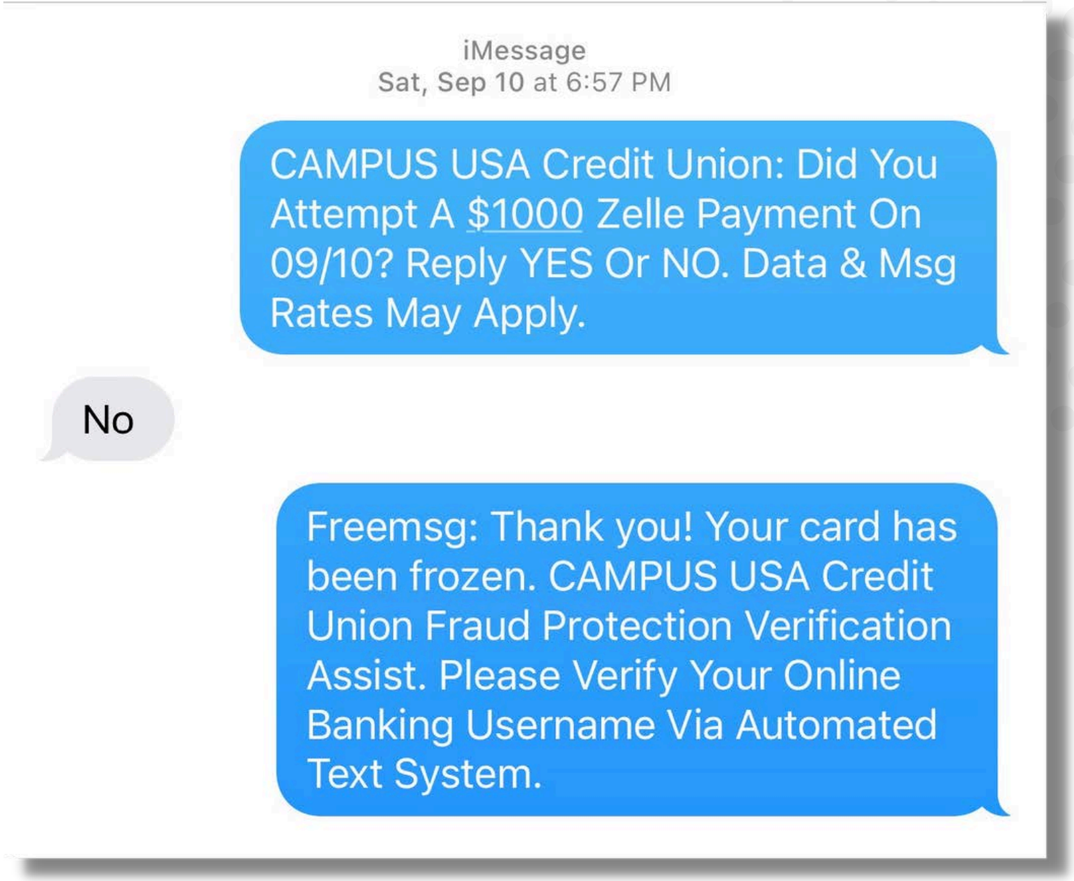
Scammers send fraudulent emails or texts pretending to be from well-known retailers, shipping companies, or charities.

These messages often contain links to fake websites designed to steal personal information or login credentials. They will also ask for your banking information.

PHISHING EMAILS AND TEXTS

Things to look for:

- **Your financial institution will NEVER ask you to verify your online banking credentials**
- **Use of fear and offering a resolution**



CAMPUS USA credit union

GIFT CARD SCAMS

Scammers contact victims by phone, email, or text, impersonating:

- **A government agency:** Claiming unpaid taxes, fines, or penalties must be paid immediately.
- **A tech support company:** Claiming the victim's computer is infected with a virus and needs fixing.
- **A family member or friend:** Pretending to be in trouble and needing urgent financial help.
- **A company representative:** Demanding payment for overdue bills or offering fake prizes.

CAMPUS USA credit union

GIFT CARD SCAMS

- The scammer instructs the victim to purchase gift cards from popular stores (e.g., Amazon, iTunes, Google Play, Walmart).

- Victims are told to scratch off the back of the card to reveal the PIN and share it over the phone, email, or text.

CAMPUS USA credit union

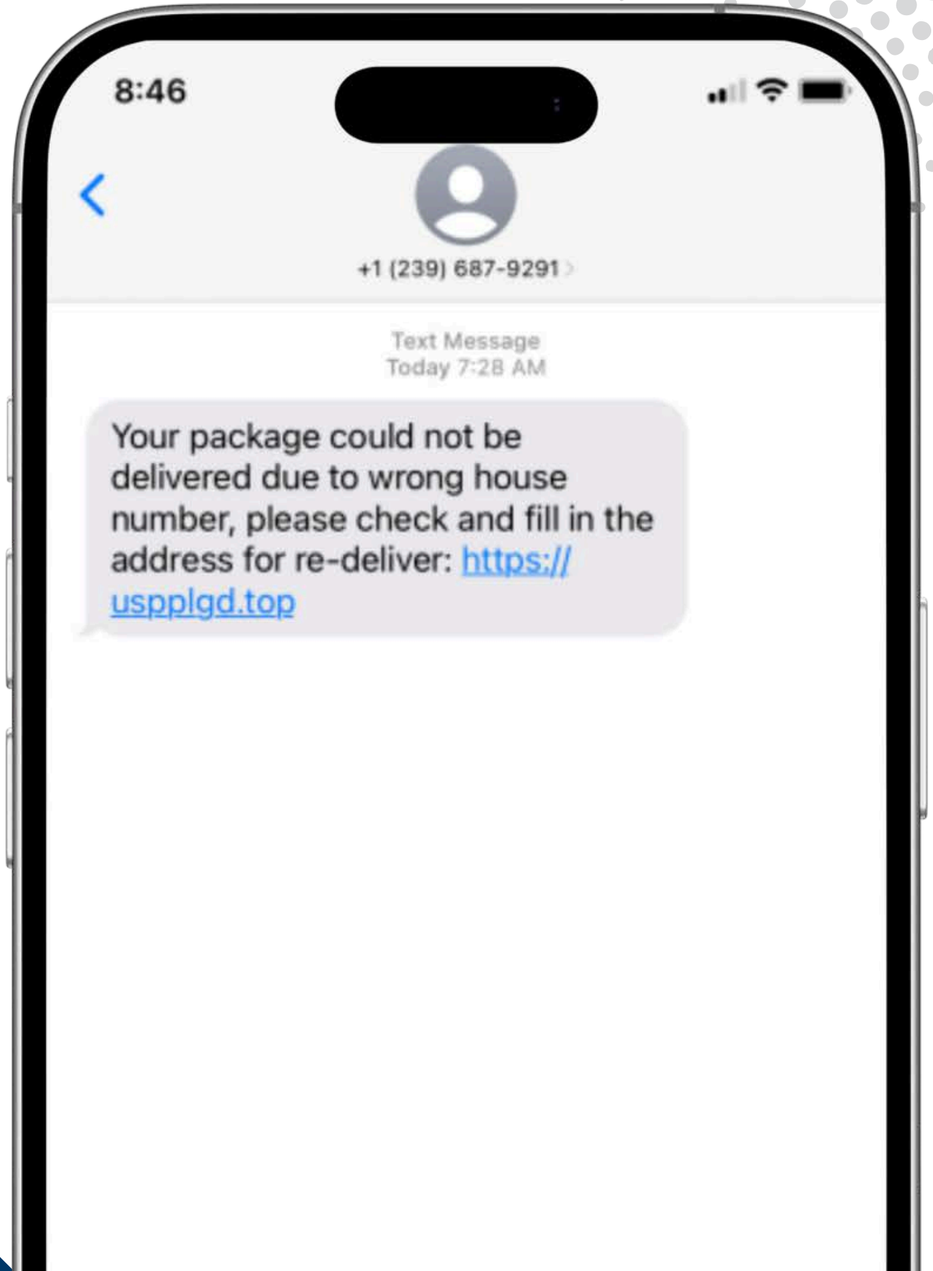
PACKAGE DELIVERY SCAMS

Scammers send fake notifications about a "missed delivery" or a "pending shipment," often asking recipients to provide personal information or pay a fee to receive their package.

CAMPUS USA credit union

PACKAGE DELIVERY SCAMS

Scammers send fake notifications about a "missed delivery" or a "pending shipment," often asking recipients to provide personal information or pay a fee to receive their package.



CHARITY SCAMS

Fraudsters set up fake charities or impersonate legitimate ones, preying on the goodwill of people during the holiday season. Donations made to these fake charities may never reach those in need.

CHARITY SCAMS

- Verify charities: Use trusted resources like Charity Navigator or the IRS website to verify legitimate charities.

- Give directly: Donate directly through official charity websites instead of through links in emails or social media ads.

SOCIAL MEDIA

Phishing

- **Fake Profiles:** Fraudsters create profiles posing as friends, family, or well-known organizations to gain trust and ask for personal details.
- **Phishing Links:** Sending direct messages or posting links that lead to fake websites designed to capture login credentials or other sensitive information.

SOCIAL MEDIA

Quizzes or Surveys

- Fraudsters use engaging quizzes like "What's your spirit animal?" or "Find out your celebrity twin!" These often ask for seemingly harmless details, but the questions (e.g., "What was the name of your first pet?") mimic security questions used for account recovery.

Fake Giveaways or Contests

- Scammers promise cash prizes, gift cards, or other rewards in exchange for filling out forms that require personal information like names, addresses, phone numbers, or bank details.

CAMPUS USA credit union

PROTECT YOURSELF FROM FRAUD

📞 **Verify the Caller:** Hang up and call the official number to confirm.

📱 **Don’t Trust Caller ID:** Caller ID can be faked!

🔗 **Don’t Click on Unfamiliar Links:** Scammers use these to steal your info.

💳 **Never Pay with Gift Cards or Wire Transfers:** Real businesses and agencies don’t ask for payment this way.

⏳ **Scammers often try to make you act fast:** Slow down, take your time, and verify before responding to urgent requests.

CAMPUS USA credit union

PROTECT YOURSELF FROM FRAUD

🌐 **Limit What You Share Online:** The more personal information you share online, the easier it is for scammers to target you.

🔒 **Use Strong, Unique Passwords:** Don't reuse passwords. A strong, unique password for each account helps protect against scams if one account is compromised.

🎁 **Beware of "Too Good to Be True" Offers:** If a prize or offer sounds too good to be true, it probably is.

🛑 **Report Scams to Authorities:** Report it to the Federal Trade Commission (FTC) or your local law enforcement.

🤔 **Trust Your Instincts:** If something feels off or too good to be true, trust your gut! Scammers use fear and excitement to manipulate – stay alert.

OTHER RESOURCES

Internet Crime Complaint Center

www.ic3.gov

Federal Trade Commission

www.consumer.ftc.gov

Thank you for joining us!

Questions or comments?

feedback@campuscu.com