CAMPUS USA CREDIT UNION PRESENTS:

IMPOSTER SCAMS

How to identify and protect yourself from social engineering scams

Seminar Objectives

What are Imposter Scams?

- Different types of Social Engineering
- Definitions
- What is the damage to consumers

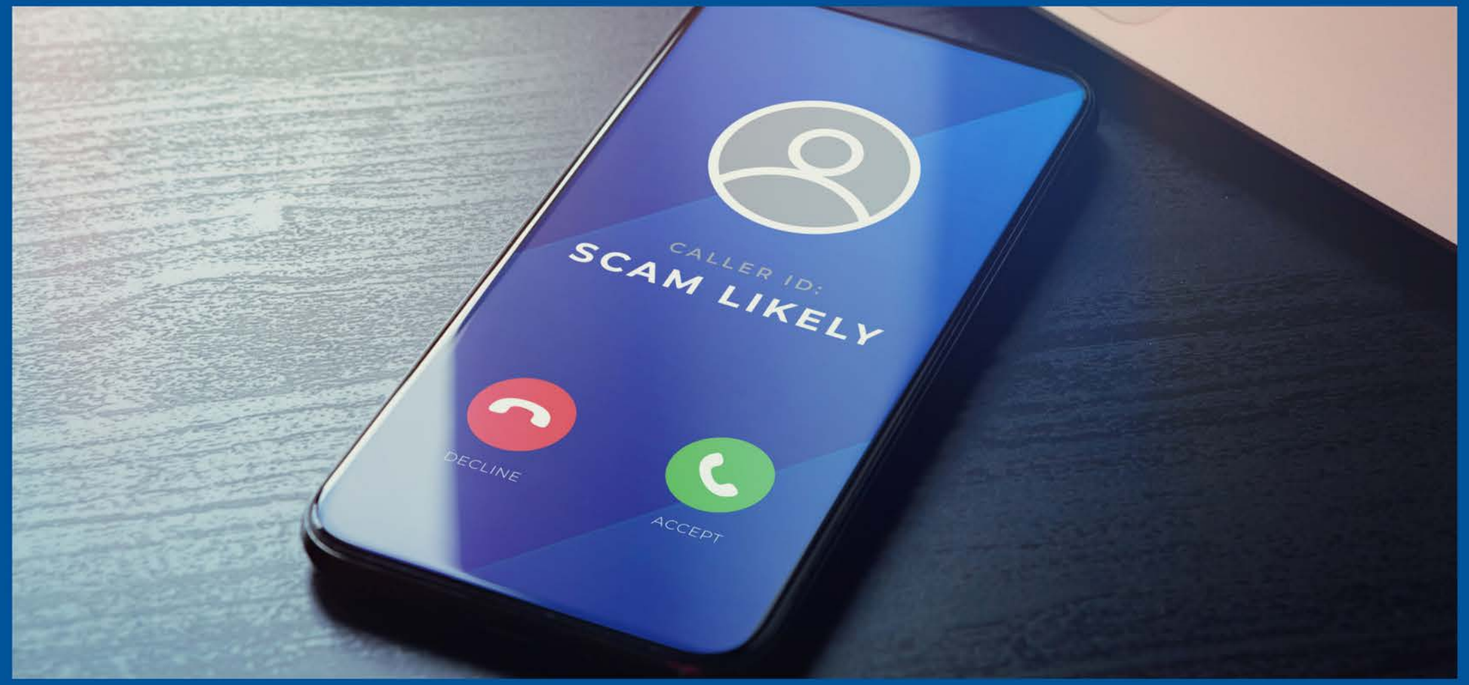
How do they do it?

- Online methods
- Texting/Phone methods
- Step-by-step

What can you do to prevent it?

- Remain diligent
- Be proactive
- Be aware of trending practices

IMPOSTER SCAMS DEFINED



Impostor scams are exactly what they sound like , Fraudsters pose as someone or a business to try to convince you to send them money (or give up information)**

Imposter Scams are a form of Social Engineering

Spoofing

Uncovers sensitive information to conduct malicious activities.

Phishing

Tricks victims into directly providing access to their personal data.

Types of Social Engineering Schemes

- Phone number/Caller ID Spoofing
- Text Message Spoofing
- Computer Pop-ups
- Malicious Emails
- Employment Opportunities
- Website Spoofing

How much have consumers lost?

FTC reported **$5.9 billion** in losses in 2021

an increase of $2.4 billion over 2020

1 in 5 people reported a loss due to imposter scams

Average victim **loses $500** and spends **30 hours** to resolving the crime

$3.56 billion lost to online fraud in the first six months of 2022

41% of adults age 20-29 who have reported fraud, end up losing money in a fraud case, compared to only 18% seniors

Spoof/Imposter scams have the highest percentage of reported cases, with more than **361,000 complaints** filed totaling **$1.33 billion** in losses

Red Flags

- Misspelled words
- Oddly phrased sentences
- Weird Spacing
- Poor grammar
- Offers to fix your account
- Text message with verification code
- Refunding money
- Requests for username and/or password

IRS Email

Thu 2/23/2023 4:37 PM

Joe Member

Final Remindr: Notice of Tax Return

To Joe.Member@email.com

Department of the Treasury
Internal Revenue Service

Just because there is a logo does not mean it is legitimate.

Claim Your Tax Refund Online

Dear Taxpayer,

If it looks too good to be true, it probably is.

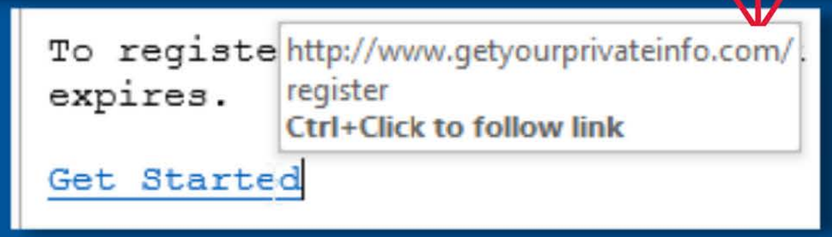
We identified an error in the calculation of your tax return from the last payment, amounting to $574.11.

In order for us to return the excess payment, you need to create a e-refund account and we will transfer the payment to your specified bank account.

To register for an account, click "Get Started" below to claim it before this offer expires.

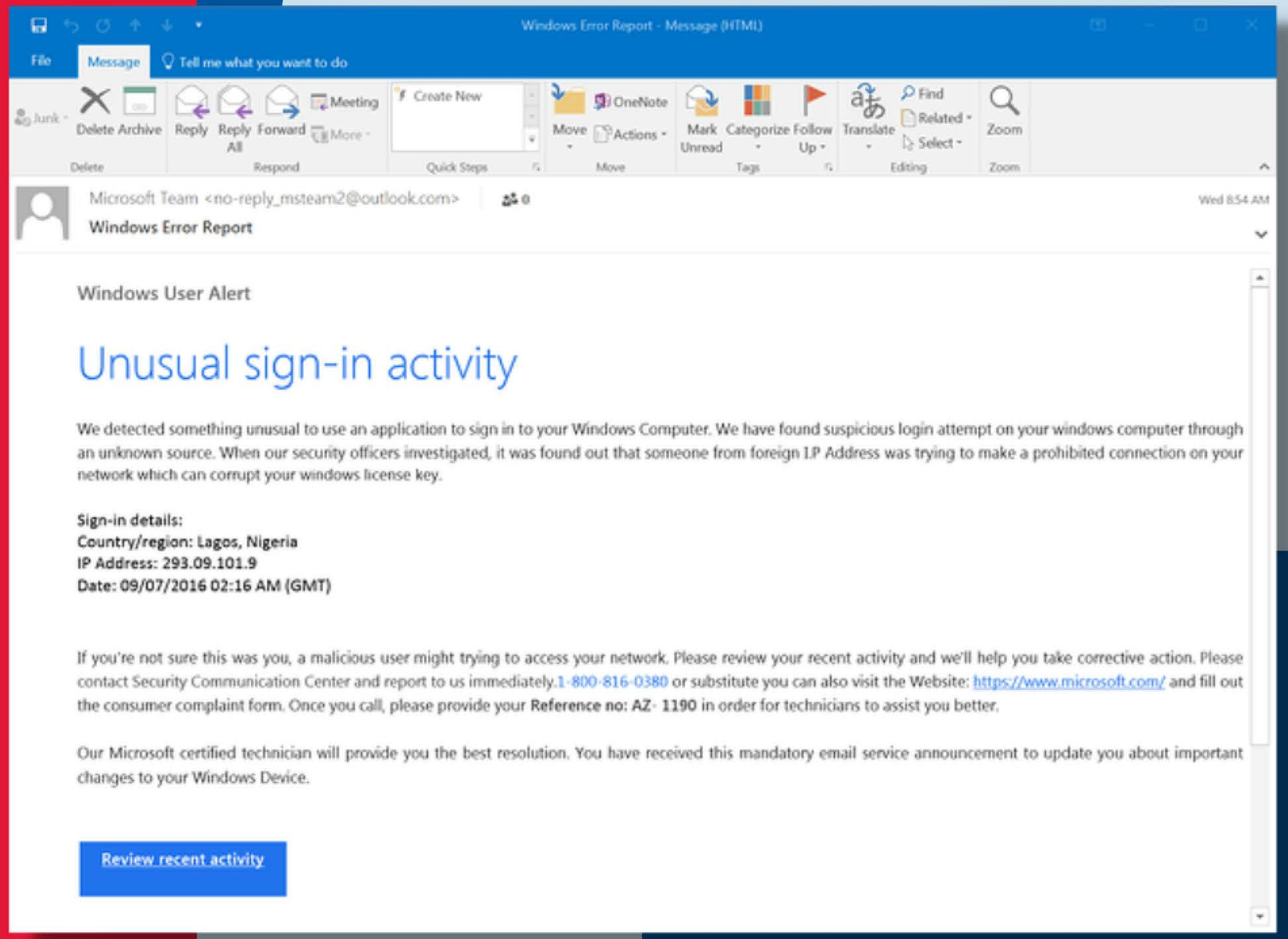
Get Started

Hover over links.



Things to look for:

- Fake Logo
- Offer is "too good to be true"
- Link to accept offer
- Misspellings
- Claim before expiration

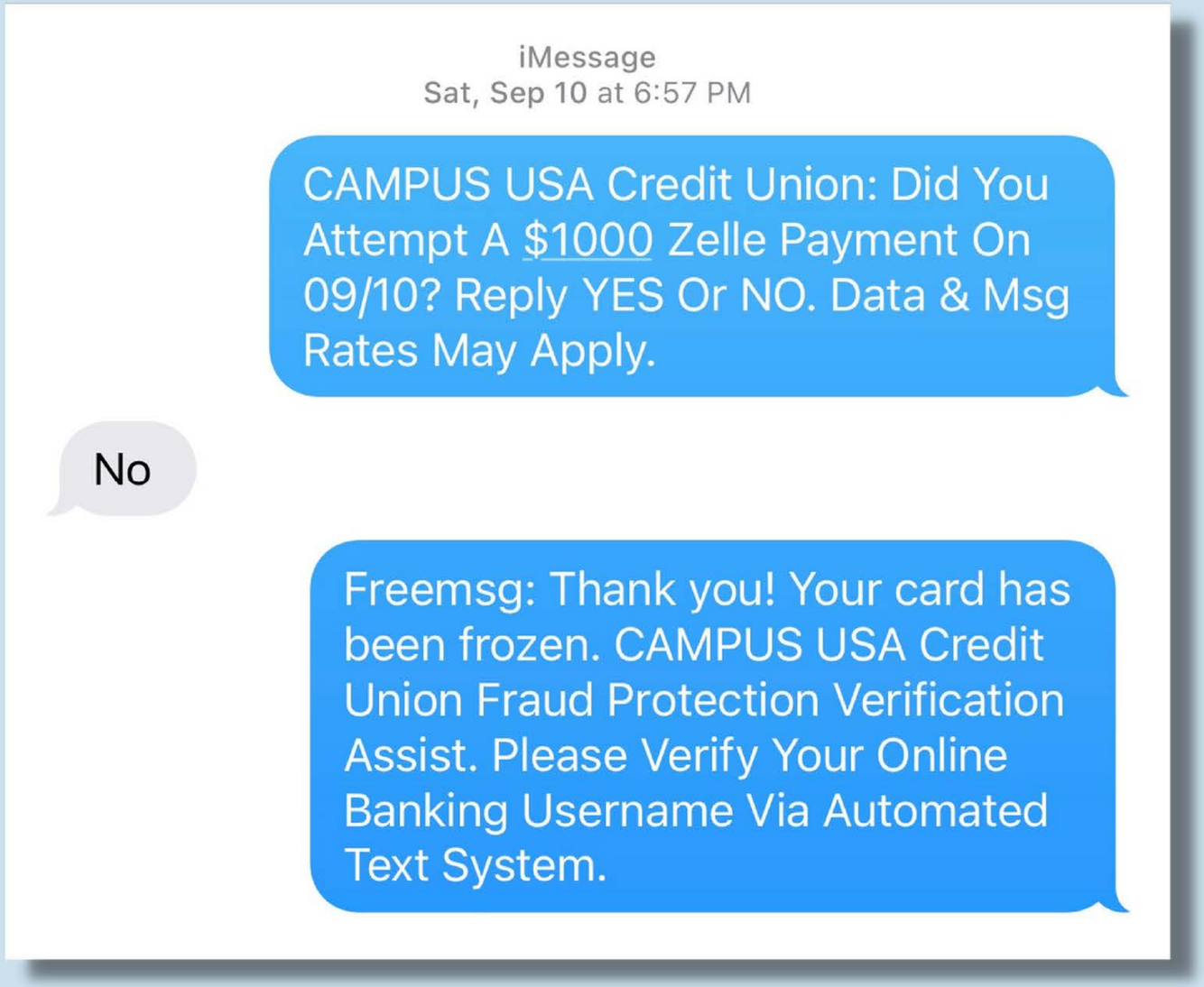


Microsoft Email

Things to look for:

- **Email address**
- **Use of fear**
- **URL to "fix" the issue**

Banking Text Message



Things to look for:

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

Phone Calls

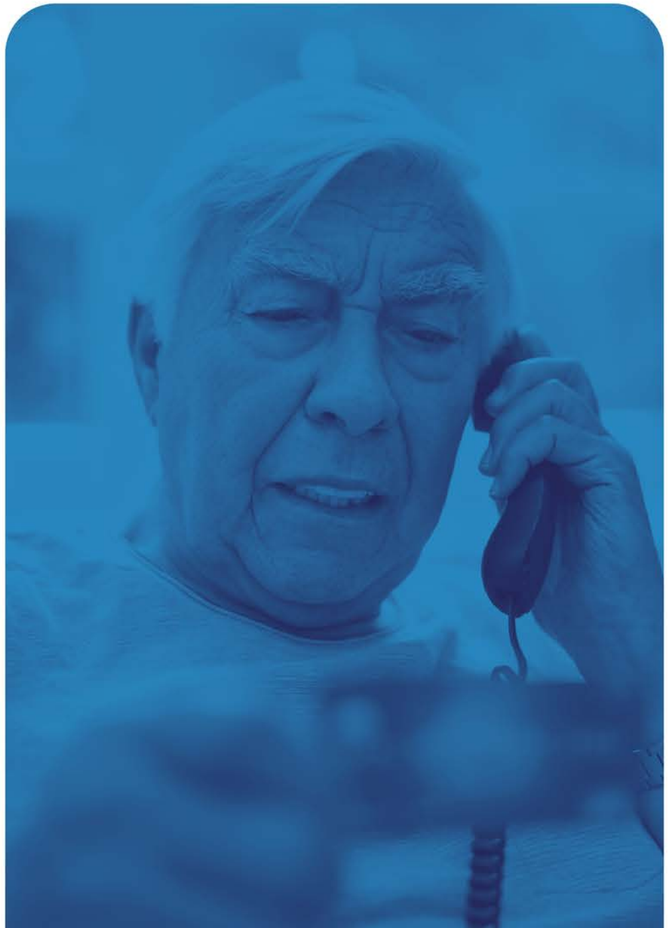
Things to look for:

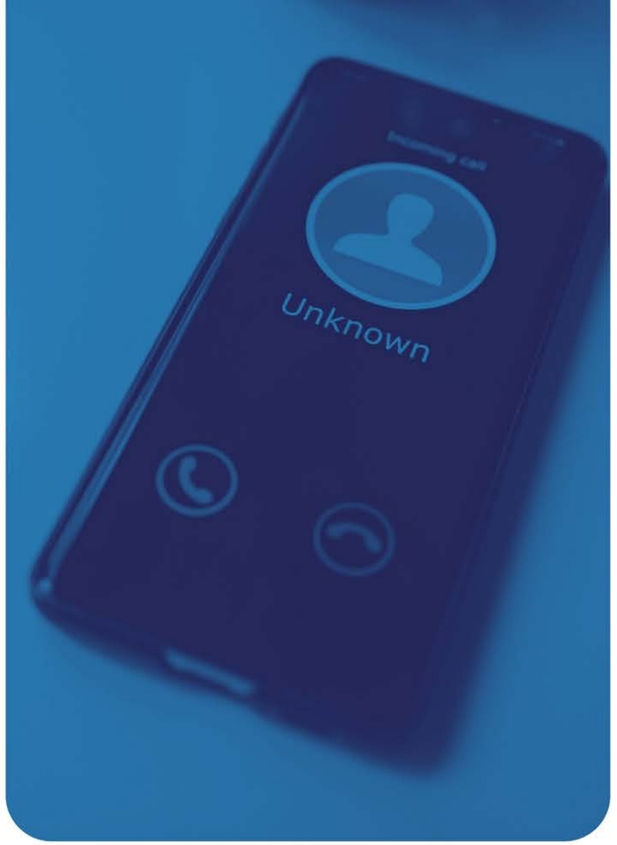
- Phone call from Court Services, Utility Companies, Financial Institutions, Police Departments, or an "authority"
- Use of fear to manipulate consumer to do something
    - Provide username
    - Click links in text
    - Share Code
    - Payments over the phone in gift cards or wire transfers

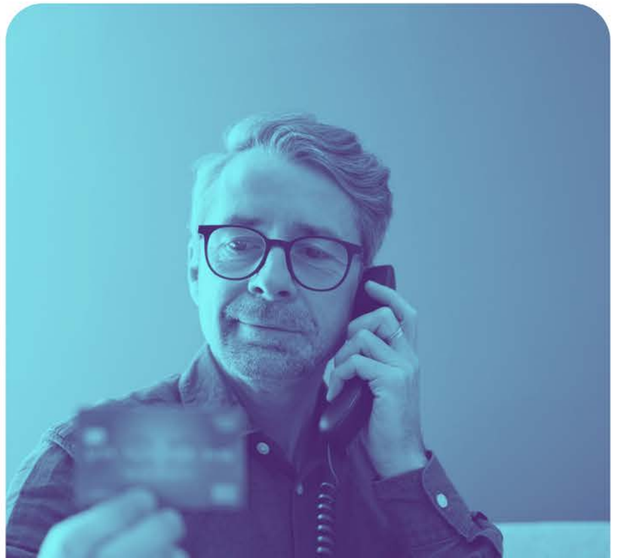
COMMON ENTITIES TO BE SPOOFED:

- Anti-Virus Software
- Microsoft
- Financial Institutions
- PayPal
- Utility Company
- IRS
- Charities
- Person to person payment companies

How do they do it?







Fraudster Tactics

1. **Fraudsters Pretend to be from an organization you know.**
   They use technology to change the phone number that appears on your caller ID. So the name and number you see might not be real.

2. **There is either a problem or a prize.**
   They might say you're in trouble, there is a problem with your account, or say you won money.

3. **Fraudsters pressure and scare you to act immediately.**
   They want you to act before you have time to think or research. They might even threaten you.

4. **Fraudsters will request you pay in a specific way.**
   They insist that you pay by wiring money, buying gift cards and giving them the info on the back, or send via Crypto Currency.

Protect Yourself

Always be diligent

Use a reputable Antivirus Software

Don't let curiosity get the best of you

Hover over the URL before clicking

Set up two-factor (or multi-factor) authentication on your accounts

Turn on spam filters

Keep your security software, browser and operating system up to date

Use your browser's pop-up blocker

Look up the company's phone number and call directly

Other Resources

Internet Crime Complaint Center

www.ic3.gov

Federal Trade Commission

www.consumer.ftc.gov

Printable resources

email

www.campuscu.com

Thank you for joining us!

Questions or comments?

feedback@campuscu.com

CAMPUS USA credit union