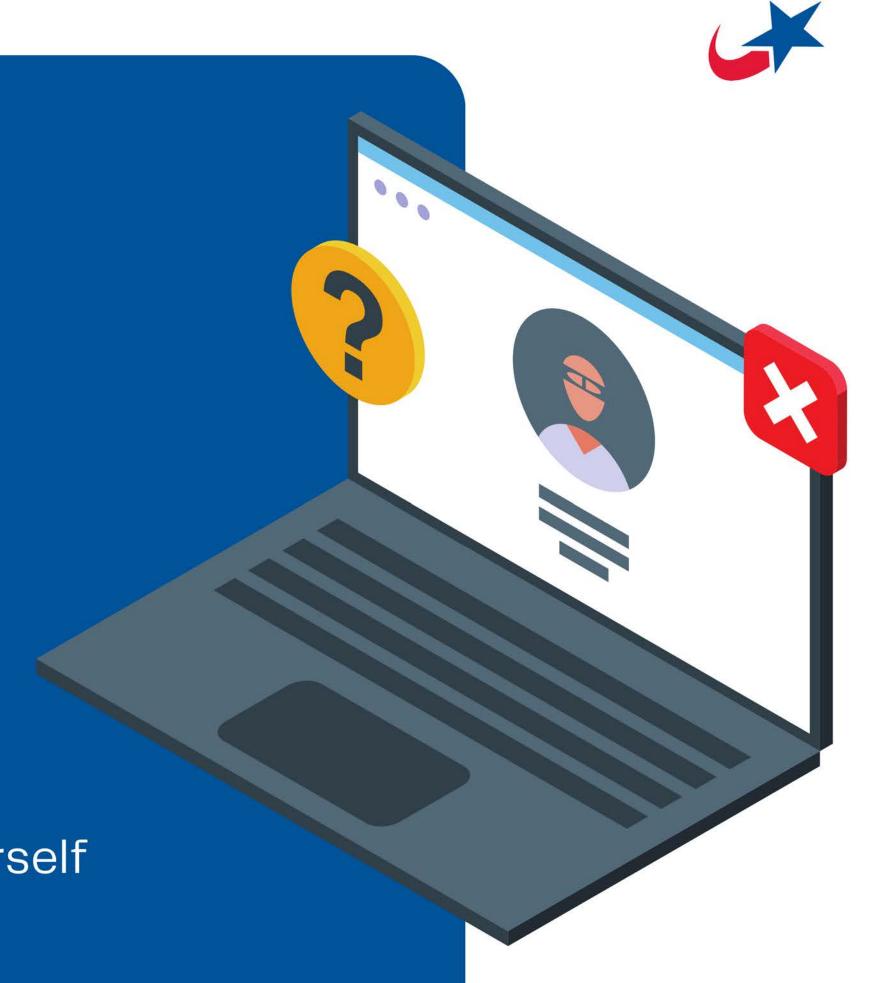
CAMPUS USA CREDIT UNION PRESENTS:

IMPOSTER SCANS

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?

\$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



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

Thu 2/23/2023 4:37 PM

Joe Member

Final Remindr: Notice of Tax Return

To Joe.Member@email.com



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.

To registe http://www.getyourprivateinfo.com/
register
Ctrl+Click to follow link

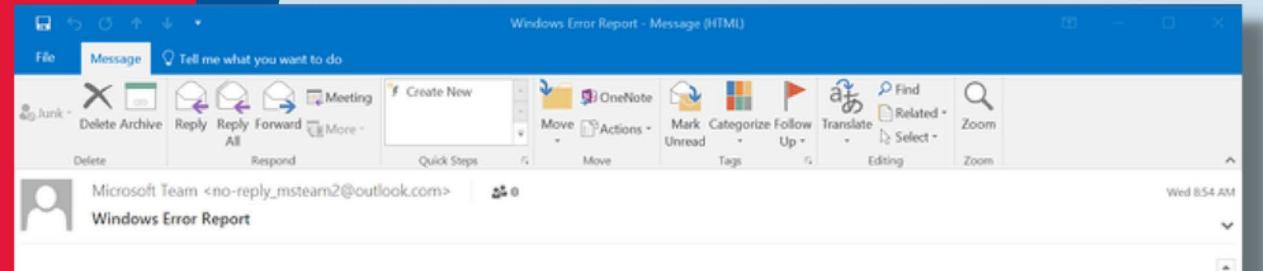
Get Started

IRS Email

Things to look for:

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





Windows User Alert

Unusual sign-in activity

We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign I.P Address was trying to make a prohibited connection on your network which can corrupt your windows license key.

Sign-in details:

Country/region: Lagos, Nigeria IP Address: 293.09.101.9

Date: 09/07/2016 02:16 AM (GMT)

If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately. 1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your Reference no: AZ- 1190 in order for technicians to assist you better.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

Review recent activity

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 <u>NEVER</u> ask you to verify your online banking credentials
- Use of fear and offering a resolution

iMessage Sat, Sep 10 at 6:57 PM

CAMPUS USA Credit Union: Did You Attempt A \$1000 Zelle Payment On 09/10? Reply YES Or NO. Data & Msg Rates May Apply.

No

Freemsg: Thank you! Your card has been frozen. CAMPUS USA Credit Union Fraud Protection Verification Assist. Please Verify Your Online Banking Username Via Automated Text System.

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

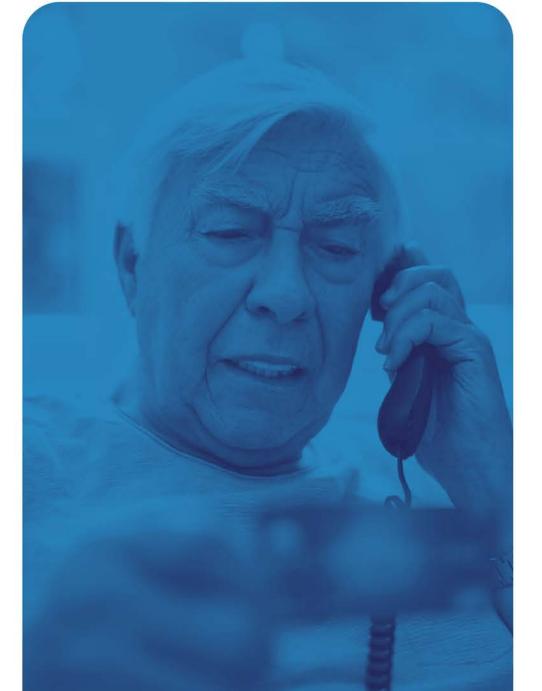
Utility Company

IRS

Charities

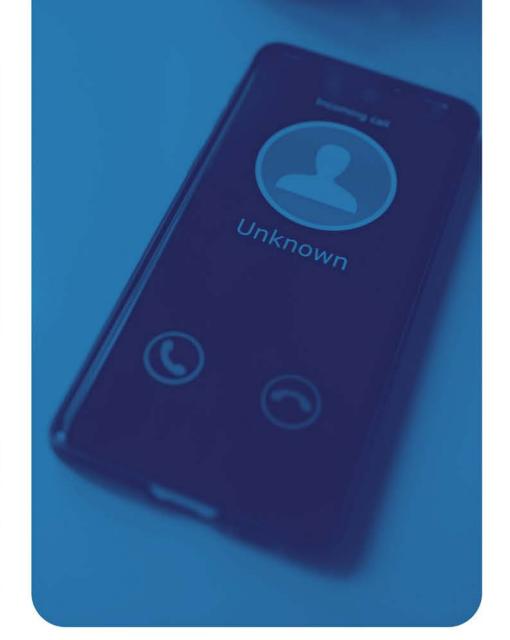
Person to person payment companies

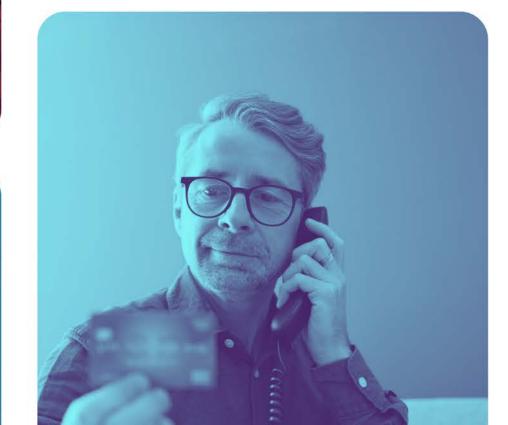
How do they do it?

















Fraudster Tactics

- 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.
- 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.
- 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.
- 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









Set up two-factor (or multifactor) 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

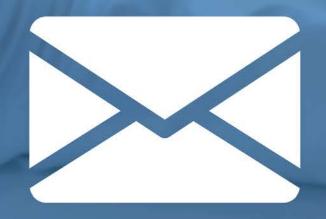
www.ic3.gov



Federal Trade Commission

www.consumer.ftc.gov

Printable resources



email



www.campuscu.com

Thank you for joining us!

Questions or comments?

feedback@campuscu.com



