



Financial Fraud & Scams: How To Protect Yourself

Tuesday, February 13, 2024

Webinar Housekeeping



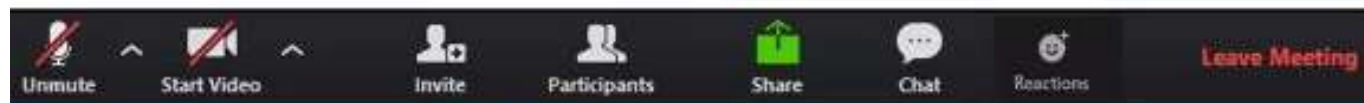
This webinar is being **recorded** and will be posted to our website.



Microphones have been muted and **cameras** are turned off for this webinar.



Please post comments and questions in the **chat** window. We will answer your questions during the Q & A portion of the presentation.



Disclosures

Sound representatives do not provide tax or legal guidance. For such guidance, please consult with a qualified professional. Information shown is for general illustration purposes and is designed to help protect consumers from becoming victims of identity theft. The information in this presentation is for informational purposes only. Any misuse of this information may be prosecutable by law.



What is Financial Fraud?

When someone takes money or assets from another individual through deception or criminal activity.



Popular Scam Tactics

- Cryptocurrency Scam
- Grandparents scam
- IRS Tax Scam
- Pig Butchering




Cryptocurrency Scams

Victims are contacted by scammers and encouraged to send money via crypto kiosks. Scammers may take advantage innocent people by:

- Blackmail
 - Scammers claim to have photos, video, etc.
- Business opportunity
 - Get rich quick
- Eviction notification
 - Pay now or you'll be evicted
- Investment opportunity
 - Unlicensed “financial advisor” reaches out for an investment opportunity

Grandparent Scam

- Fraudsters pretend to be a grandchild or another relative
 - They may say there is an emergency
 - Impersonate using AI voice recognition
 - Request to wire money
- 

IRS Tax Scam

- Email that includes the IRS logo
- “Third Round of Economic Impact Payments”
 - Claim an “important matter regarding your recent tax return filing”
 - Refund of \$976 once you submit the document
- Don’t click the “complete my information” button

Pig Butchering Scam

- Victim receives a call, text or message
- Fraudster begins to build relationship & trust with victim.
- The scammer will then encourage the victim to “invest” their savings in a phony investment.
- The victim will be instructed to deposit cash via crypto kiosk or wire transfer.
- Encouraged to purchase gift cards and provide card information

What is Spoofing?

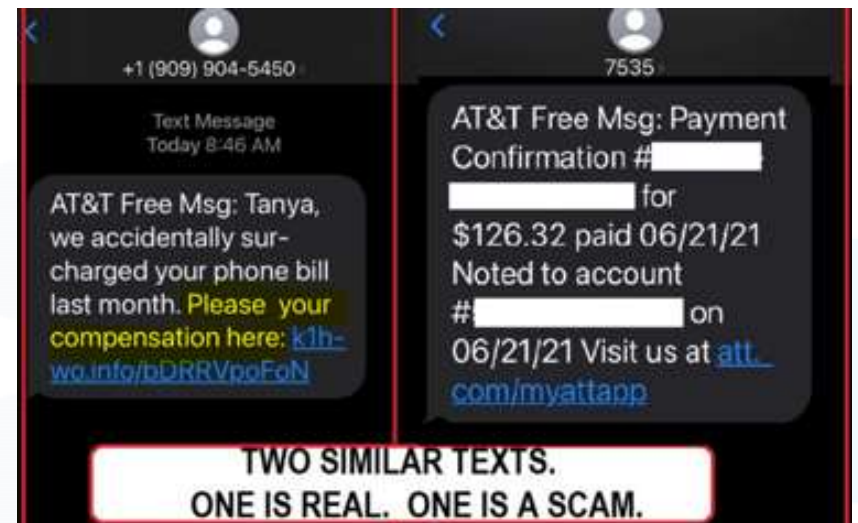
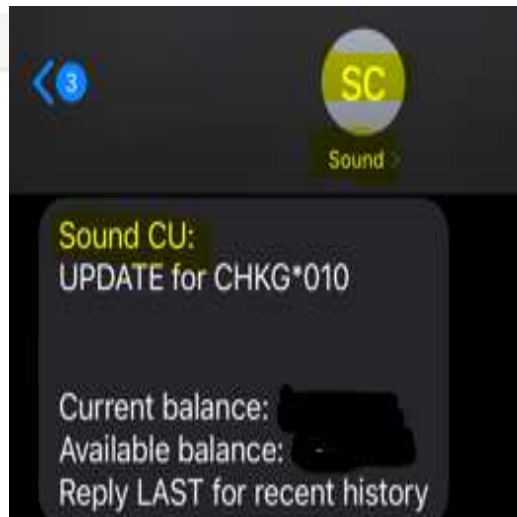
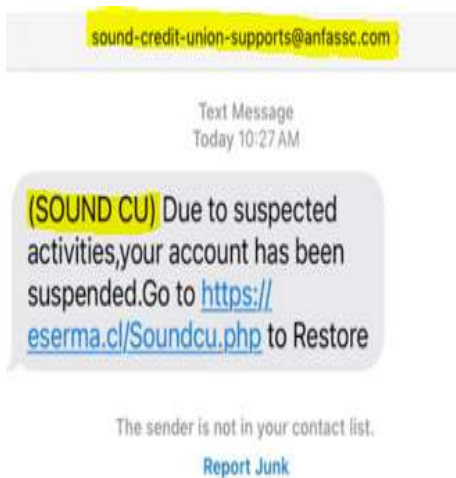
- The act of faking a virtual identity for hacking or security purposes.
- Typically, via:
 - Websites
 - Caller ID
 - Email
 - Text



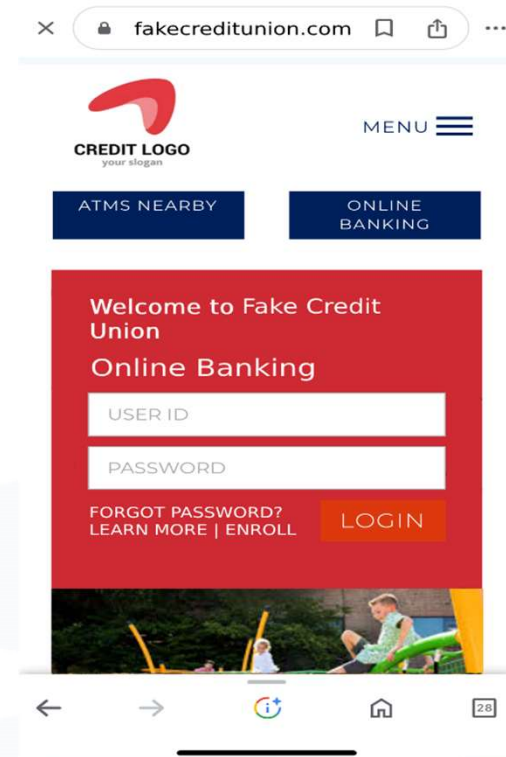
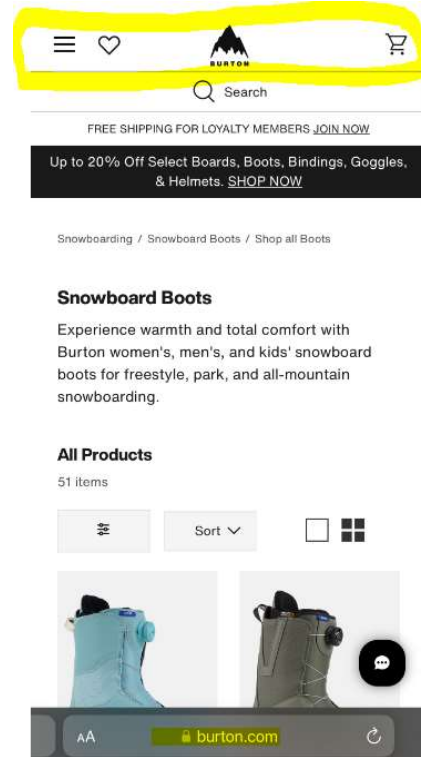
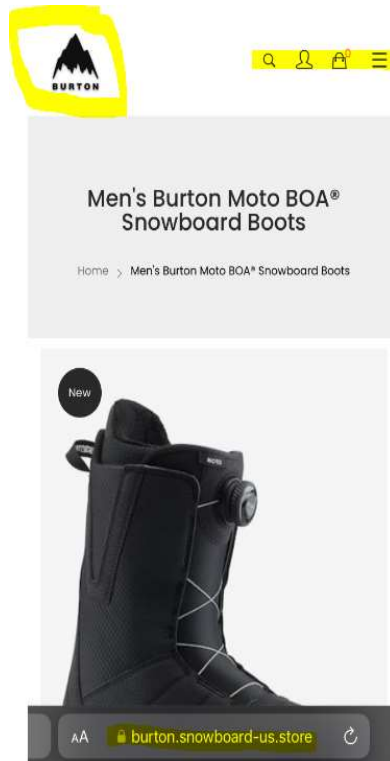
Banking Imposter Scam

- Phishing (Email)
 - Scammer sends email similar to Financial Institution (FI) communication
- Vishing (Phone)
 - Caller ID displays as name & phone number of FI
- Smishing (Text)
 - Criminals send you a text message
- Website
 - Nearly identical to the financial institutions' website. May have a pop-up window asking for online banking credentials.

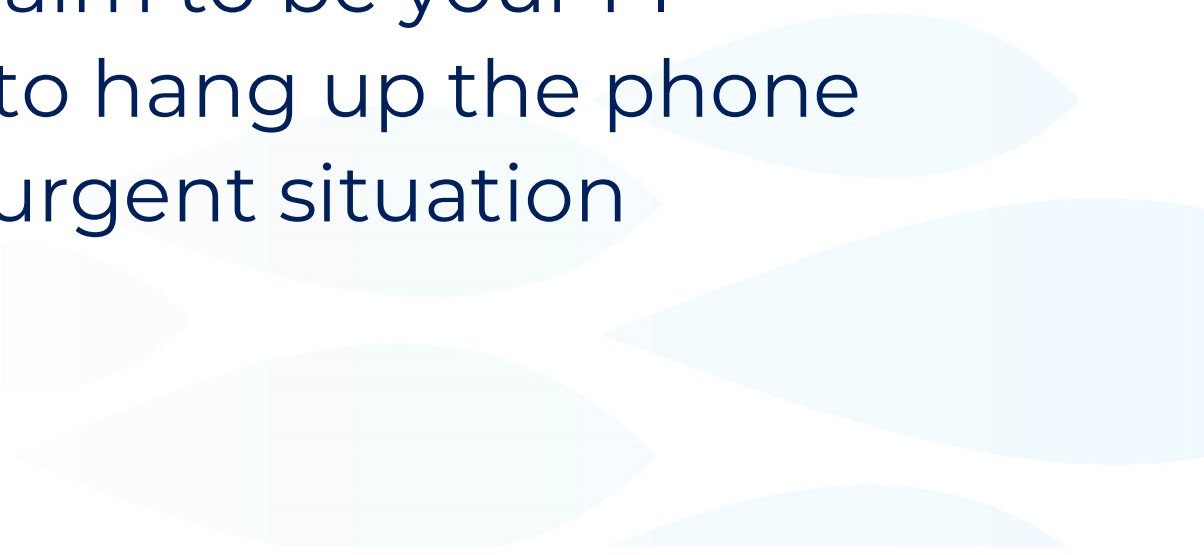
Imposter Text Examples



Imposter Website Examples



Banking Imposter Red Flags

- Scammer requests sensitive information
 - Threatening comments
 - Misspelling or improper wording
 - May or may not claim to be your FI
 - Pressure you not to hang up the phone
 - Scammer claims urgent situation
- 

Protecting Yourself

- Do not give out you SS #, account #, PIN, password or verification code.
- Hover your cursor over links
- Verify website
- Delete suspicious emails
- Avoid answering unknown calls/texts
- Hang up the phone
- When in doubt contact your FI

Protecting Yourself

- Use an antivirus program
- Enable a Windows firewall
- Utilize a secure browser
- Never give out password information



When Not to Send Money or Virtual Currency

- **Never** send to someone you don't know.
- **Never** send if circumstances seem unusual.
- **Never** send if someone paid you with a check and instructed you to send it back to them.
- **Never** purchase gift cards and give card numbers to a person over the phone or via text/email.

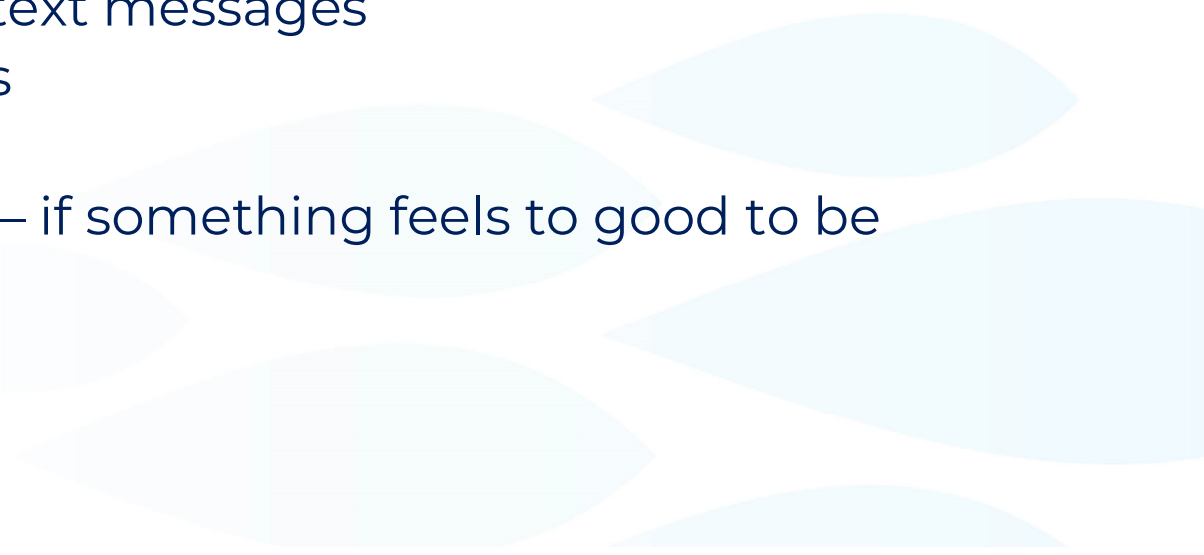
What To Do If You Become A Victim

- Contact your financial institution
- Confide in friend or family member who may be able to assist
- Change your passwords
- File a complaint with the Federal Trade Commission
www.reportfraud.ftc.gov
- Check your credit report at www.annualcreditreport.com
- File a cyber crime complaint with the FBI at www.IC3.gov

How Does Sound Protect our Members?

- Transport layer security
 - Multi-factor authentication
 - Constantly monitoring for fraud
 - Fraud prevention partners
 - Annual system & security audits
 - Awareness via website, social media, newsletter & blog articles
 - Sound employee training
- 

Things to remember....

- No legitimate business or gov't agency will ask for a gift card or crypto currency as payment
 - When sending wires transfer or crypto currency – IT IS GONE
 - Avoid suspicious callers, websites, texts, and links
 - Never give out your personal info to a caller or through email
 - Delete unknown emails & text messages
 - Shred personal documents
 - Limit your exposure
 - Trust your gut or skeptical – if something feels too good to be true....
- 

Final Thoughts....

- Be Cautious of Your Personal Information
 - Be Skeptical of Online Requests
 - Monitor Your Finances
 - Continue to Educate Yourself
 - Never send gift cards as a form of payment
- 
- A decorative graphic in the bottom right corner consisting of several light blue, stylized fish shapes of various sizes and orientations, swimming towards the right.

Questions? Contact us!



communityrelations@soundcu.com



soundcu.com



800.562.8130

**sound
credit
union**

