



Defending You Finances

Steps to protect yourself from fraud



PURDUE FEDERAL
CREDIT UNION



B.T. Brown

Fraud Prevention Manager, Purdue Federal Credit Union

Retired Sergeant, Lafayette Police
Department





Agenda

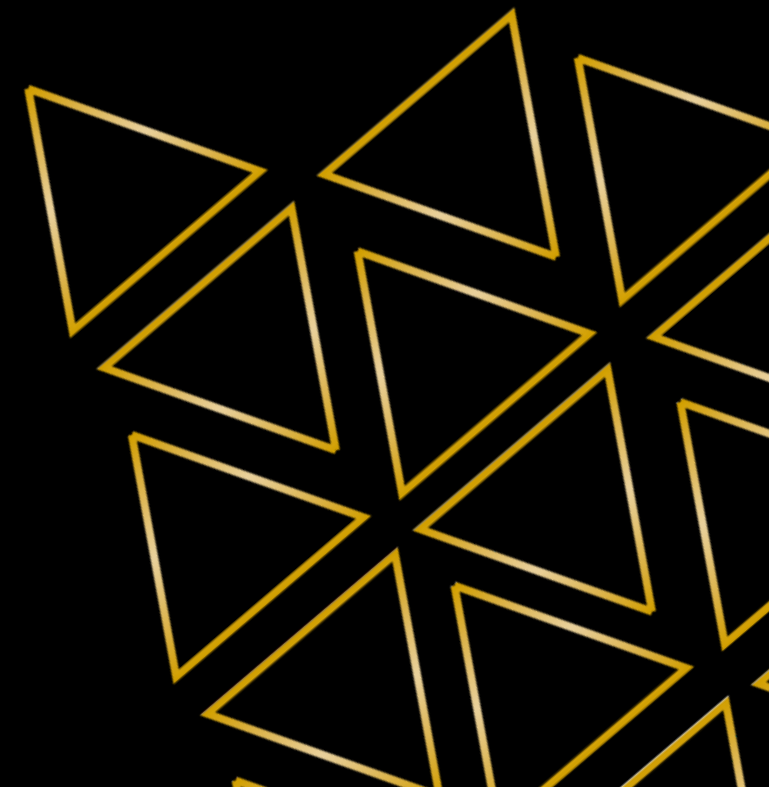
- Purdue Federal Fraud Prevention Dept.
- Scams and Fraud
 - How scams work
 - How fraud works
- Know your vulnerabilities
 - Educate & Understand
- How to protect yourself





Fraud Prevention Department

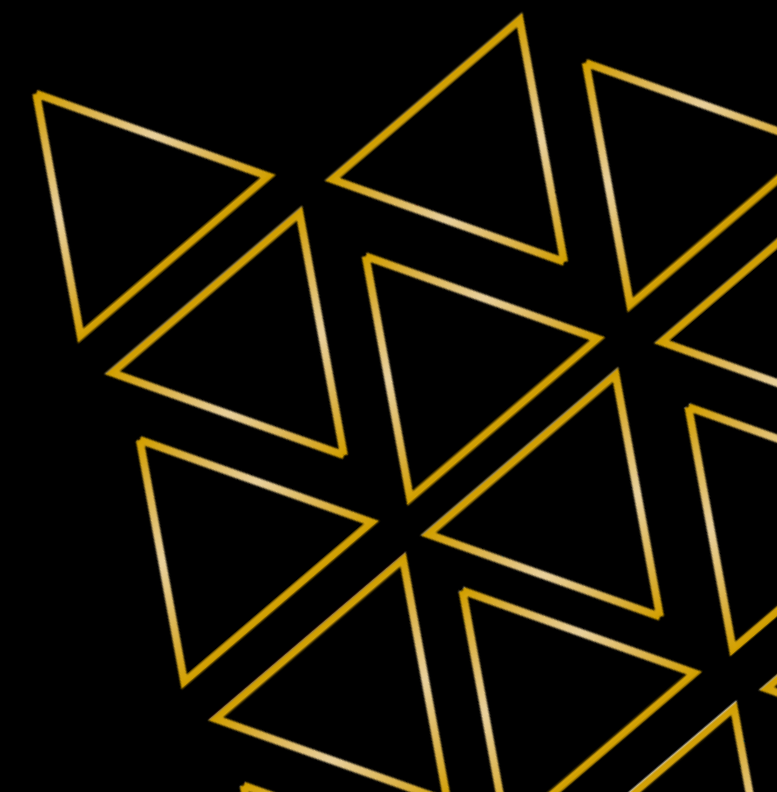
- Established in 2021 to help safeguard our members and their finances
 - Currently a team of 4
- What do we do?
 - Review transactions
 - Educate our staff and members
 - Incorporate prevention strategies
 - Protect our members finances and the credit union against fraudsters





Types of Scams

- Romance Scam: Someone portrays themselves as being romantically interested.
- Work Scam: Offering an easy work process, usually involves receiving a check & a request to purchase products.
- Overpayment Scam: Offers to purchase something & sends payment, usually in the form of a check.





Types of Scams

- Loan Scam : Request of personal information and provides deposits, usually the deposit comes in the form of a check
- Advertisement Scam : Offers money to advertise a product
- Federal Warrant Scam: Threatens a legal proceeding against you for drug trafficking, terrorist activity or tax delinquency





Types of Fraud

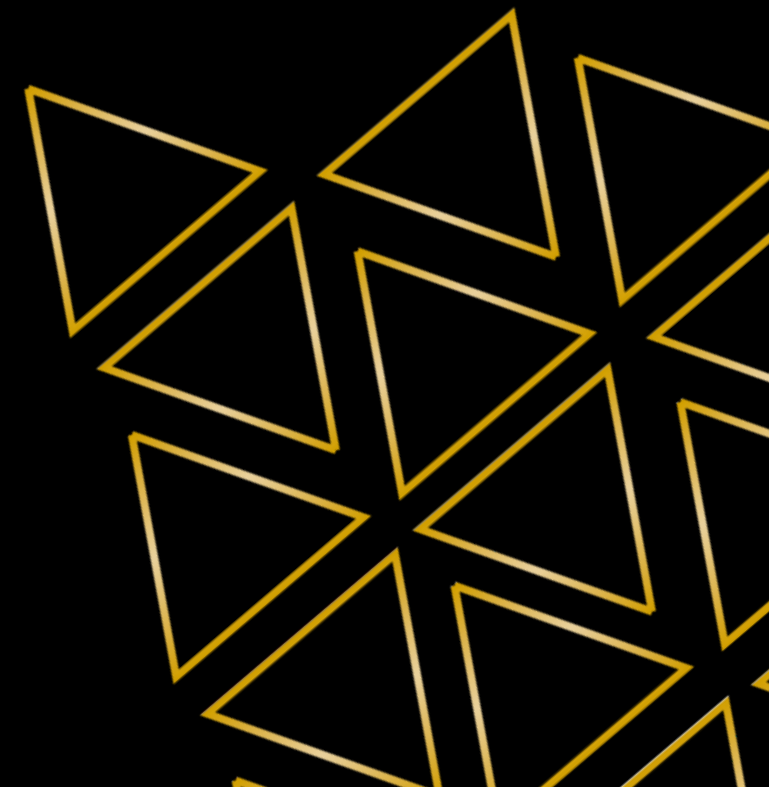
- Account Take-Over: An unauthorized person obtains your banking information and uses the account for their personal gain.
- Person-to-person: An unauthorized person uses your access to a payment system to make unauthorized transactions.
- Counterfeit Checks/Check Fraud: An unauthorized person uses your check information to produce new or written checks.





Know your vulnerabilities

- Knowledge: Know what is real vs. fraud
- Understanding/Education: Educate yourself on technology (phones, computers, software)
- Be vigilant.





Text Scams

Examples of fraud texts

FRM:PURDUE
MSG:Your online access has been locked for security reasons. Confirm your details below or visit the nearest branch
<https://dmln.in/Purdue/>

FRM:PURDUE
MSG:A charge of \$591 require your action. Kindly Press 1 to approve or Visit:<https://qeal.in/Purdue/> to cancel

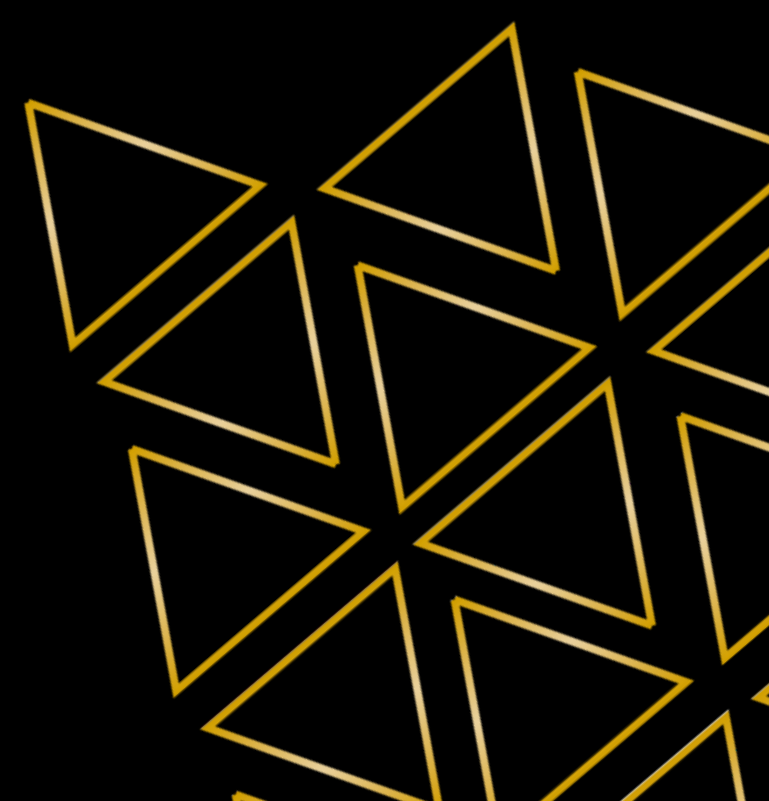
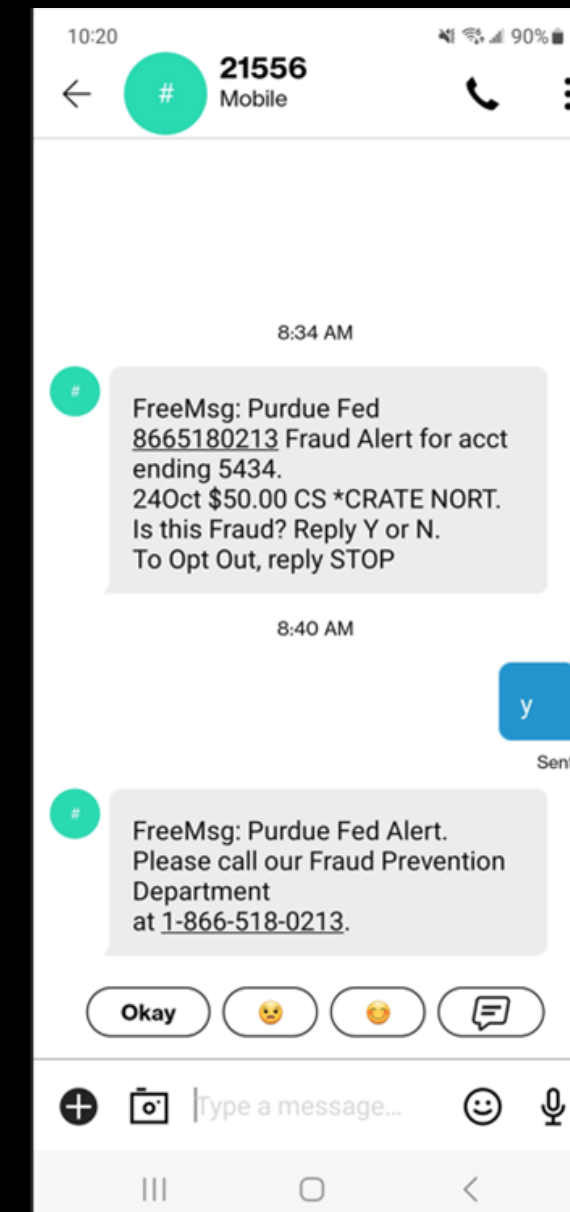
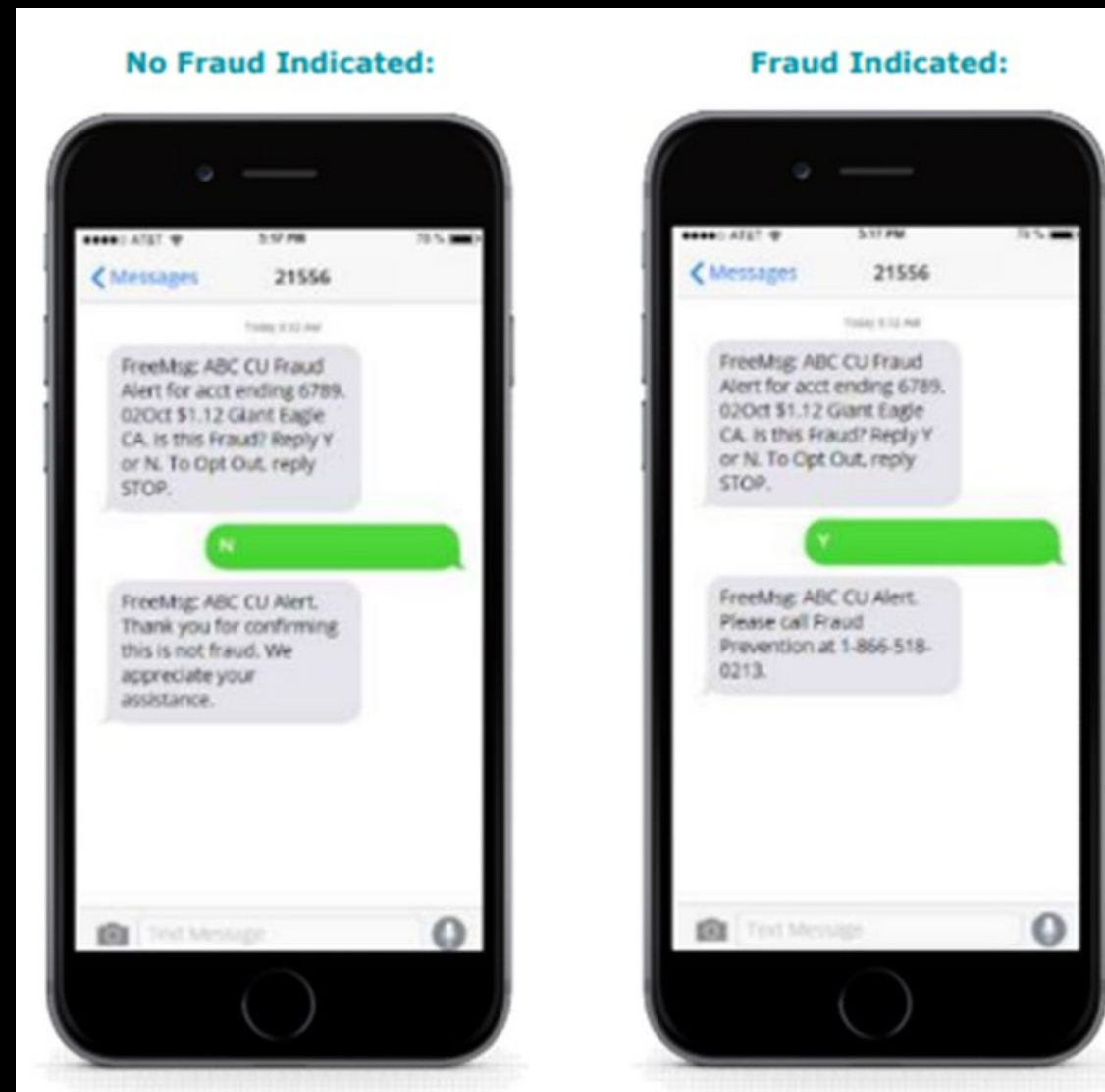
..PURDUE...CU...
ARE YOU TRYING TO CHARGE 623.49 At XMA store IF NOT YOU PLS VISIT wearfascia.com/purr/purduefe TO CANCEL OR REVIEW





Text Scams

Examples of real texts from Purdue Federal





Text Scams

Compare fraud vs. real alerts

..PURDUE...CU...
ARE YOU TRYING TO CHARGE
623.49 At XMA store IF NOT YOU
PLS VISIT [wearfascia.com/purr/
purduefe](http://wearfascia.com/purr/purduefe) TO CANCEL OR REVIEW

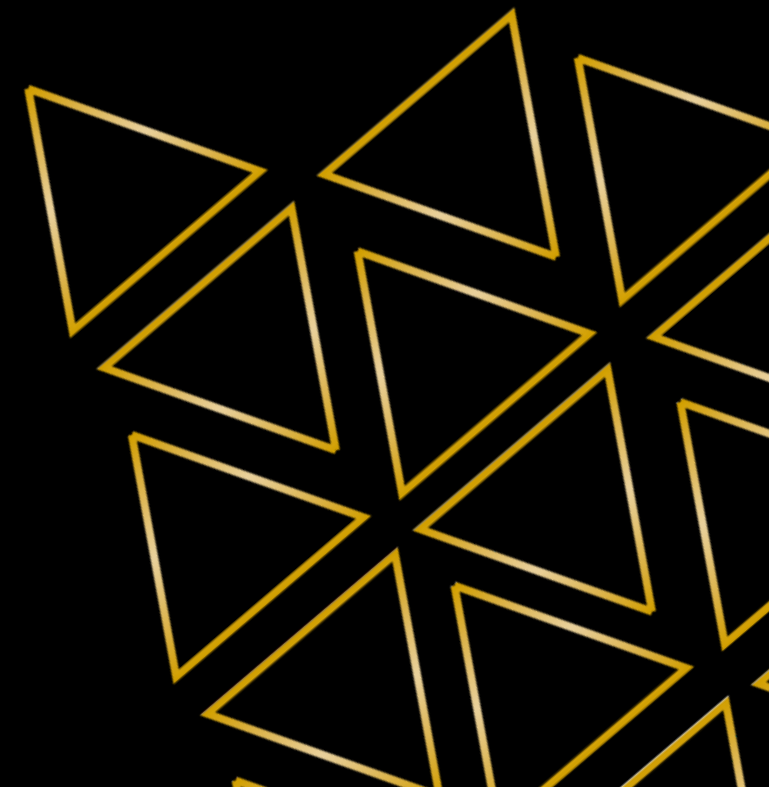
FreeMsg: Purdue Fed
[8665180213](tel:8665180213) Fraud Alert for
acct ending 6428.
13Sep \$1.40 UBR* PENDING D.
Is this Fraud? Reply Y or N.
To Opt Out, reply STOP

- Note the link in the fraud text
- Reply Y or N in the legit text
- The Opt Out of STOP in the legit text



Phone Calls

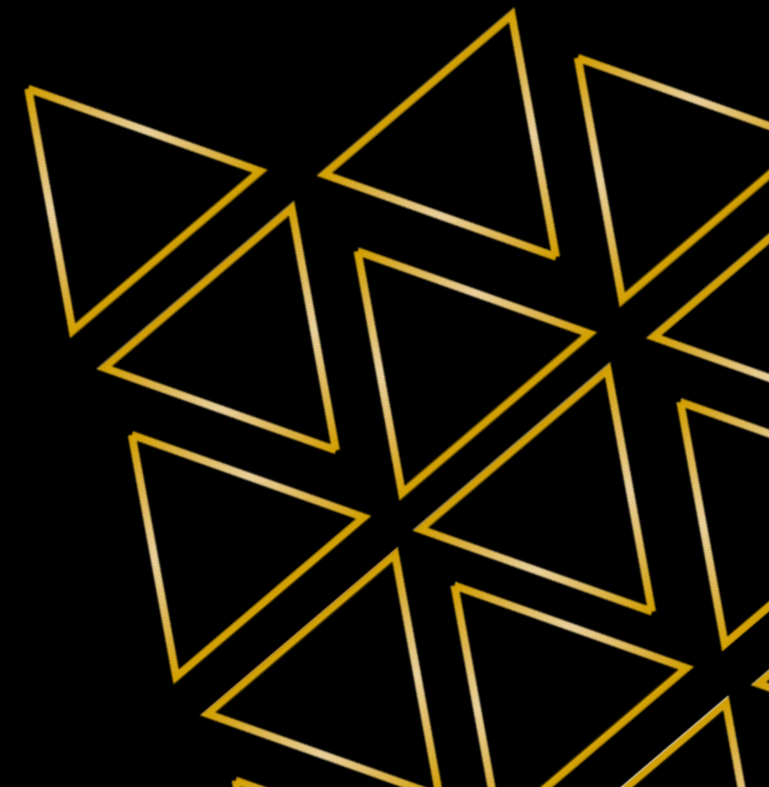
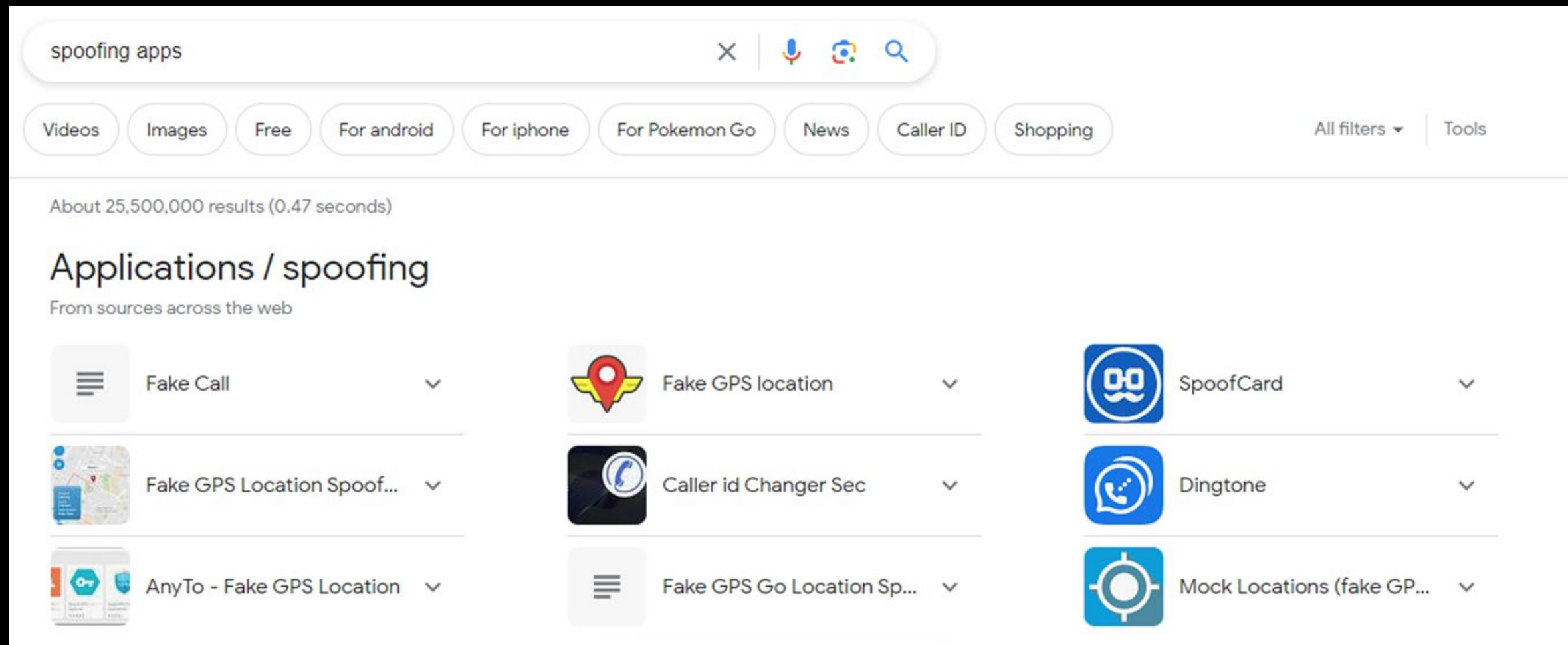
- Were you expecting the call?
- What information are they telling you?
- What information are they asking for?
- They force you into action by causing fear.
 - Calling from a federal agency (IRS, Treasury Dept., Drug Enforcement).





Spoofer Calls

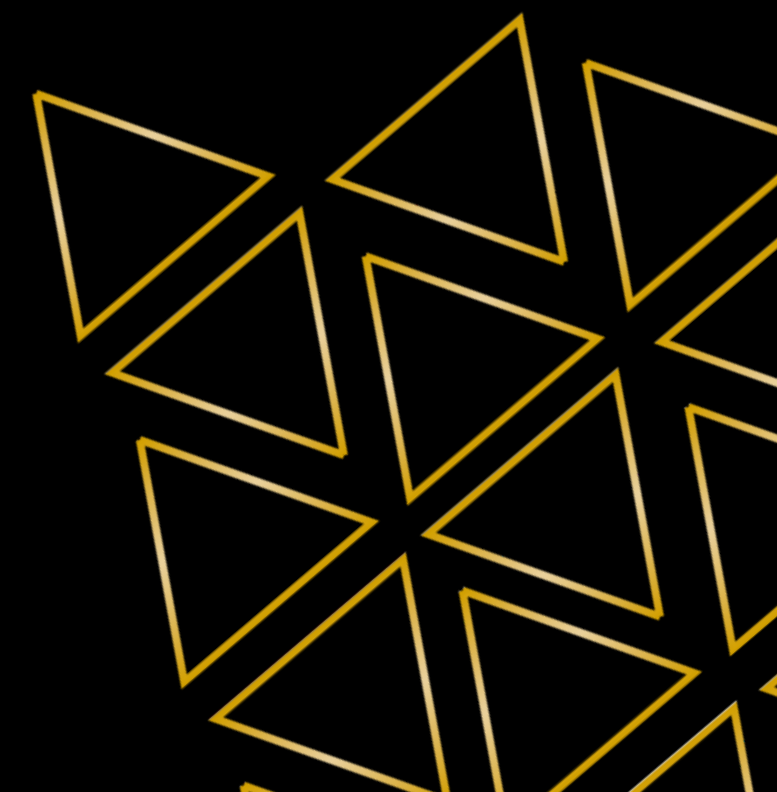
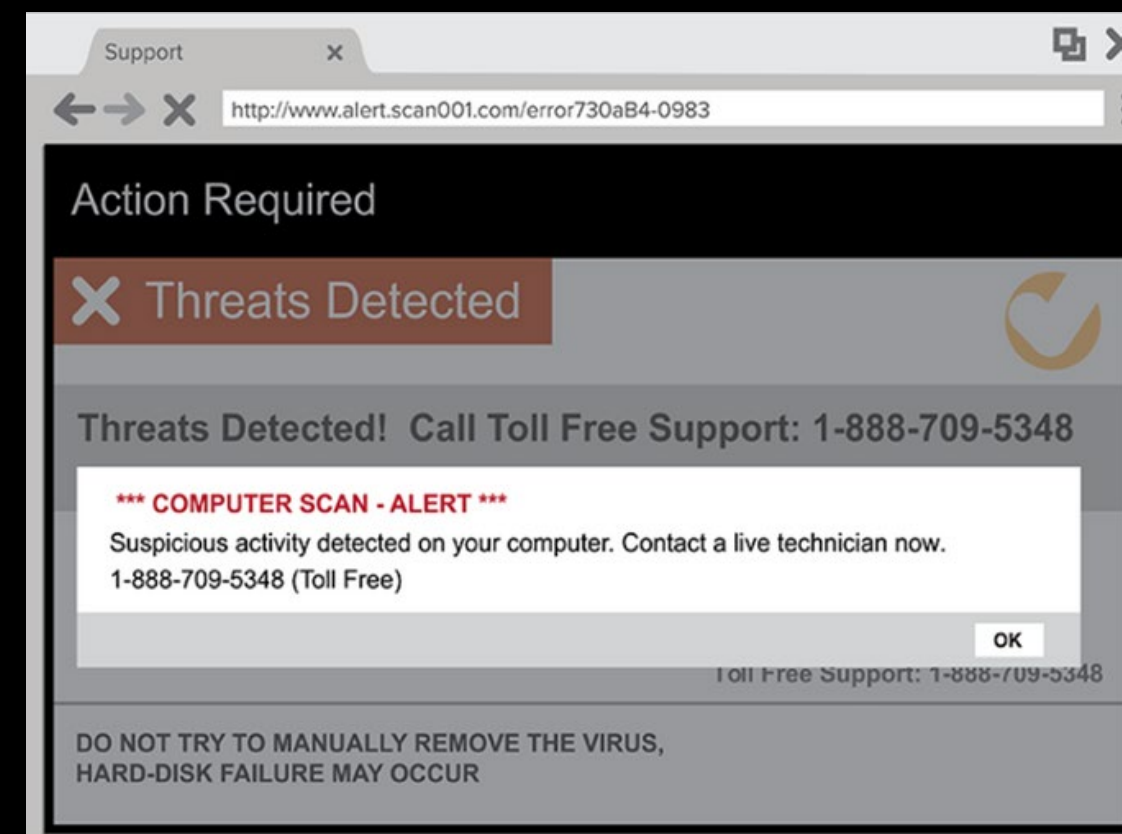
- Spoofer is a service that allows someone to misrepresent their real caller ID.





Computer Take Over

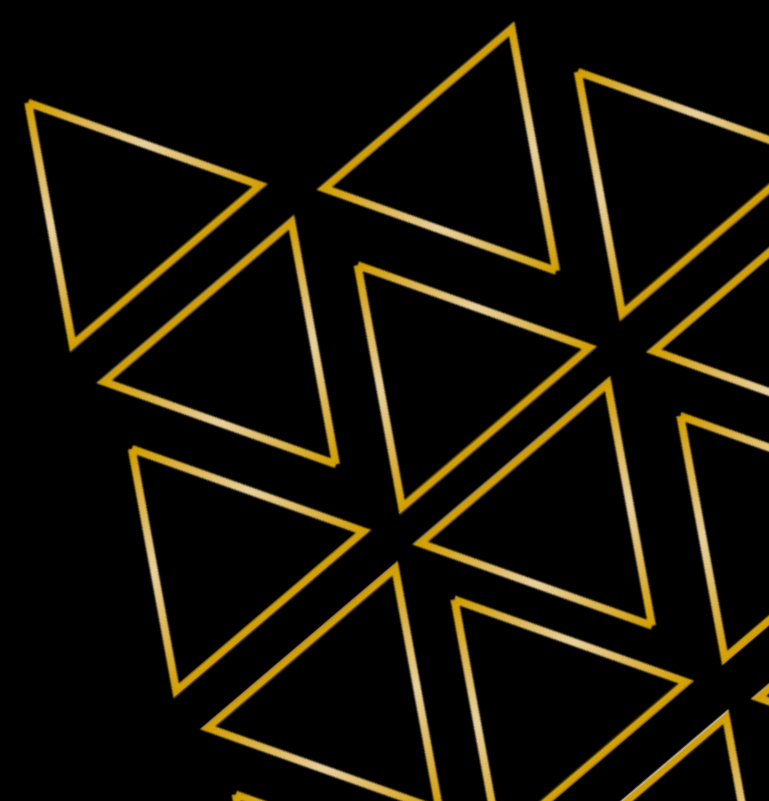
- Typically happens after you have unknowingly clicked on a fraudulent page
- They will say they are Microsoft, Google or another big name brand or government agency
- They will threaten to turn over evidence from your computer to a government agency





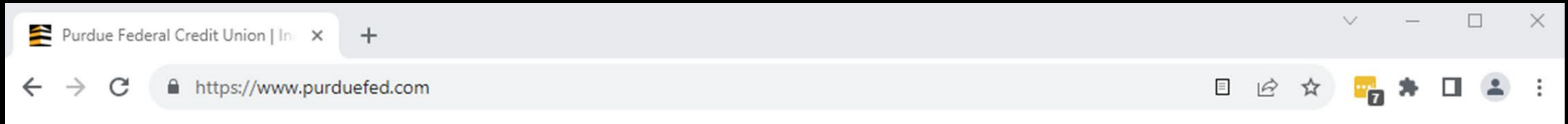
Understanding URLs



- Paying attention to and understanding the URL address line will help you identify potential fraud websites.





Understanding URLs



- Look for the padlock 
- Look for “https:” 
- Make sure it is an address you’re familiar with
 - <https://www.purduefed.com>
 - <https://www.ssa.gov>
 - <https://www.ftc.gov>
- Familiarize yourself with your common websites
- Do not give permission to “remote into” your computer





How to protect yourself

- Know who you are in communication with
- NEVER give out any information until you are certain of who you are dealing with
- Use trusted websites
- Use trusted methods of payment
- Be vigilant!





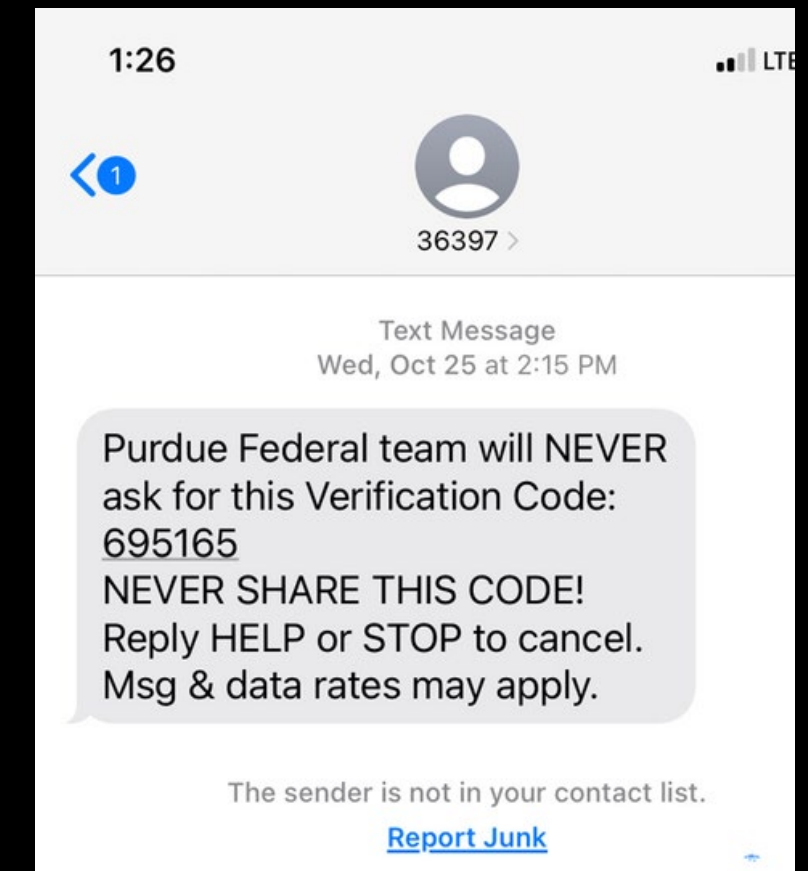
How to protect yourself

- Do not answer calls or texts you are unsure of.
 - If you believe the call or text is legit, call a number you are familiar with before giving out any information



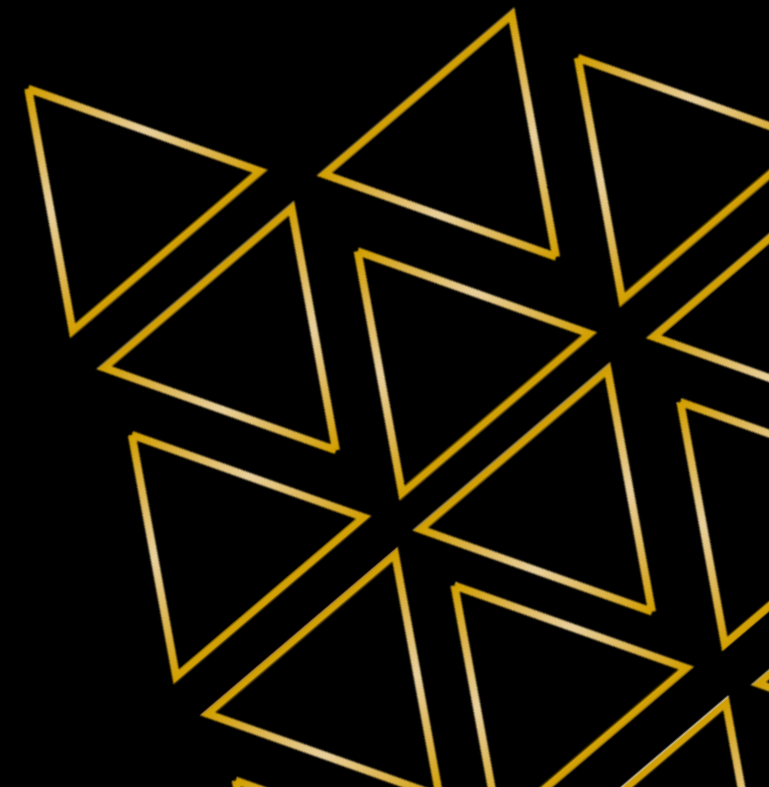
Purdue Federal Verification Methods

- We will NEVER ask for the following:
 - Your username or password to digital banking
 - Your entire date of birth or SSN
 - Your entire debit or credit card number
 - Your one-time passcode



Purdue Federal Verification Methods

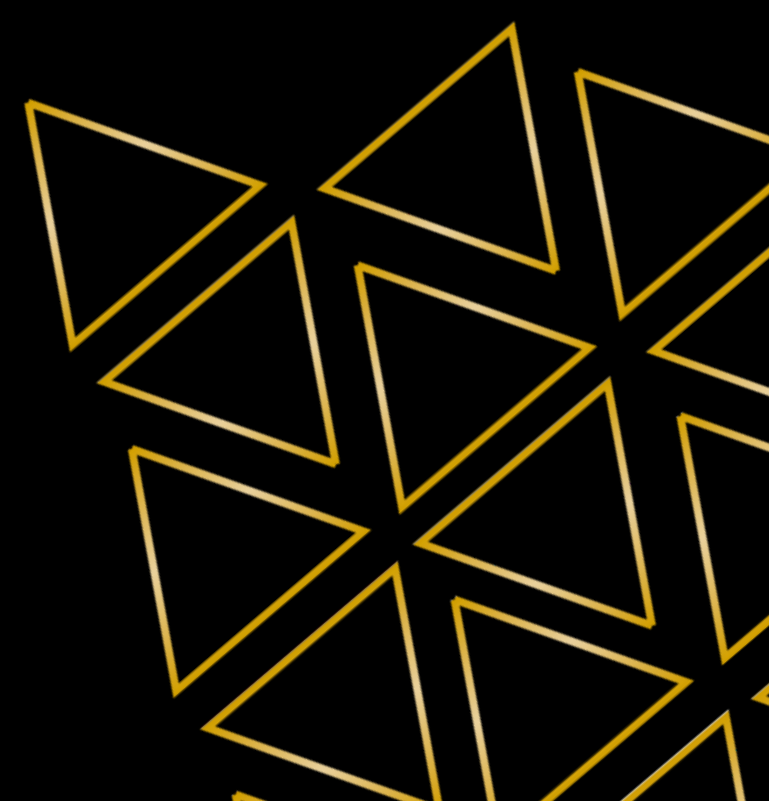
- We COULD ask for the following:
 - The last four digits of your SSN
 - The last four digits of your debit or credit card number
 - A current or previous address
 - A current or previous phone number
 - A passport or driver's license number





Helpful Resources

- www.ftc.gov
- www.occ.treas.gov
- www.purduefed.com
- www.justice.gov
- www.usps.gov



Questions?



PURDUEFED.COM/FRAUD



fraud@purduefed.com



1.800.627.3328

