Financial Crimes: Awareness & Prevention

uw credit union

Agenda

- Understanding Types of Payments
- Types of Scams
- Identity Theft
- Precautions to take
- Steps to take if you become a victim
- Educational and informational resources

Understanding Payments

- Checks
- Wires
- Person to Person Payments (P2P)
  - Zelle
  - Apple Cash
  - Cash App
  - PayPal
- Debit and Credit Cards
- Gift Cards
- Cypto Currency/Bitcoin

Check Scams

Types of scams

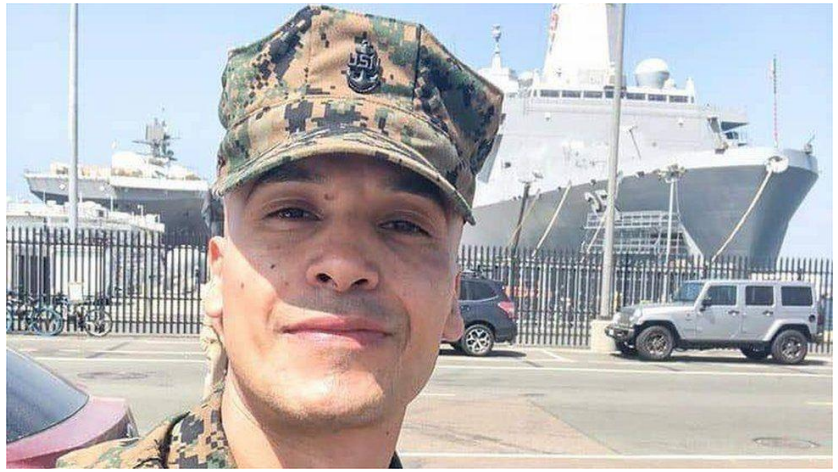
- Employment
- Social Media
- Loan Scams

Things to be on the look out for:

- Receiving a check that was not expected or for a job you have not done
- Receiving a payment for more than what you expected and being asked to return a portion of that check for any reason
- Being asked if your financial offers Mobile Deposit
- If you are hesitant about the validity of the check do not use the funds and contact your financial immediately

Romance Scams

- Victims reported losing more money to romance scams in 2022 than any other fraud reported to the FTC
- Starts on Dating Sites or social media, a “relationship” starts
- Push communication off an app promptly via text, emails, phone calls, skype, etc



- Eventually, the love interest (Scammer) asks for money.
  Most common reasons are: “so I can visit you”, a sick family member, an emergency "health" cost or they're overseas and have no access to funds.

- Common for individuals to be added to fake accounts to write checks or receive funds from a "lawyer" or "assistant" to further transfer to the scammer

- If money is sent (Wire transfer, P2P , cryptocurrency), “scammer” will continue to ask for more money, until victim figures it out or they’re out of money.

- It's a difficult situation to navigate for a financial. We don't want to refuse access to their own money but also don't want to assist them in losing substantial amounts of $$$

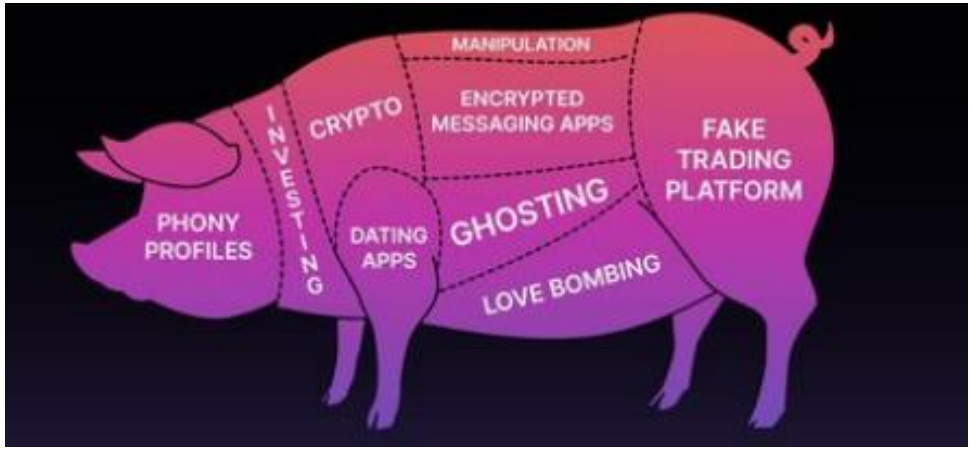
- These scams commonly result in the largest monetary losses due to amount of time individuals could be involved with the scammer

Pig Butchering- what is it?

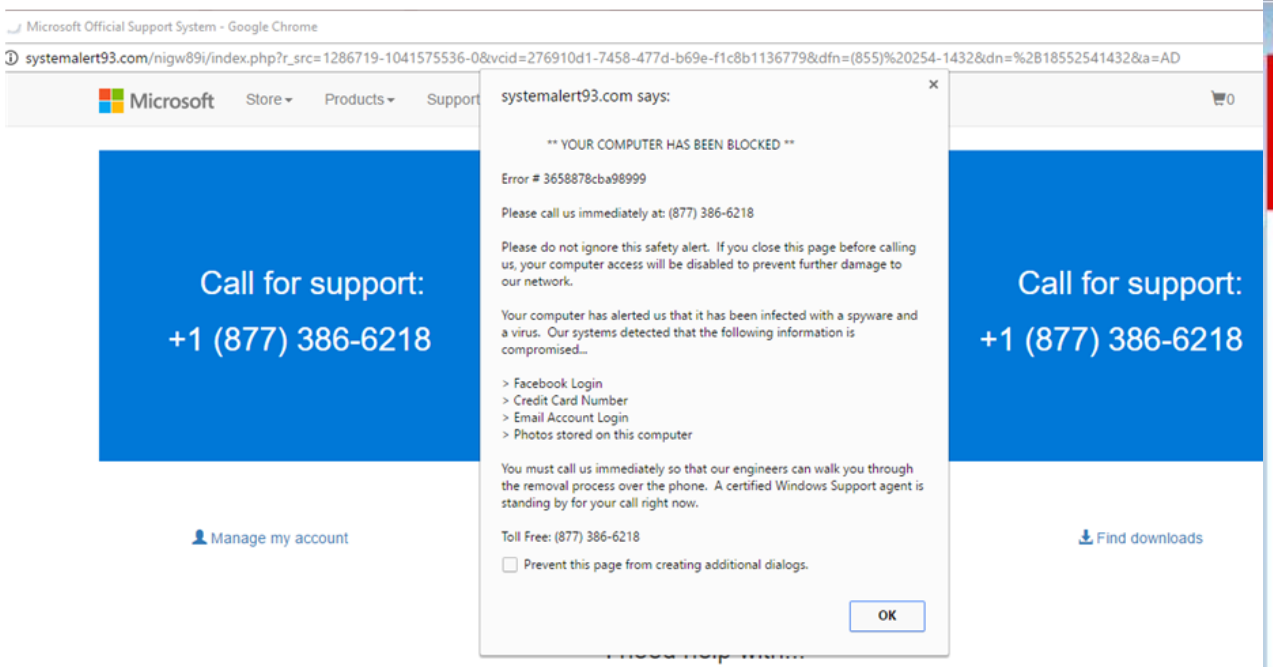
- Form of Investment Scam
- Colorful metaphor -The “Pigs” are the victims. As they are spending more and more money, they’re getting “fattened up”.
- When its time for the Victims to withdraw their funds, they are unable to and may now realize it’s a scam. That’s when the “Pig” has been butchered.

Pig Butchering Warning Signs

- Unexpected Contact
- Request for Crypto wallet information via screen shots
- Exaggerated claims and elevated emotions
- Unknown or confusing investment opportunity (CYRPTO)
- Sense of urgency about upcoming financial news
- Unfamiliar trading platforms
- Wallet that someone else help you set up

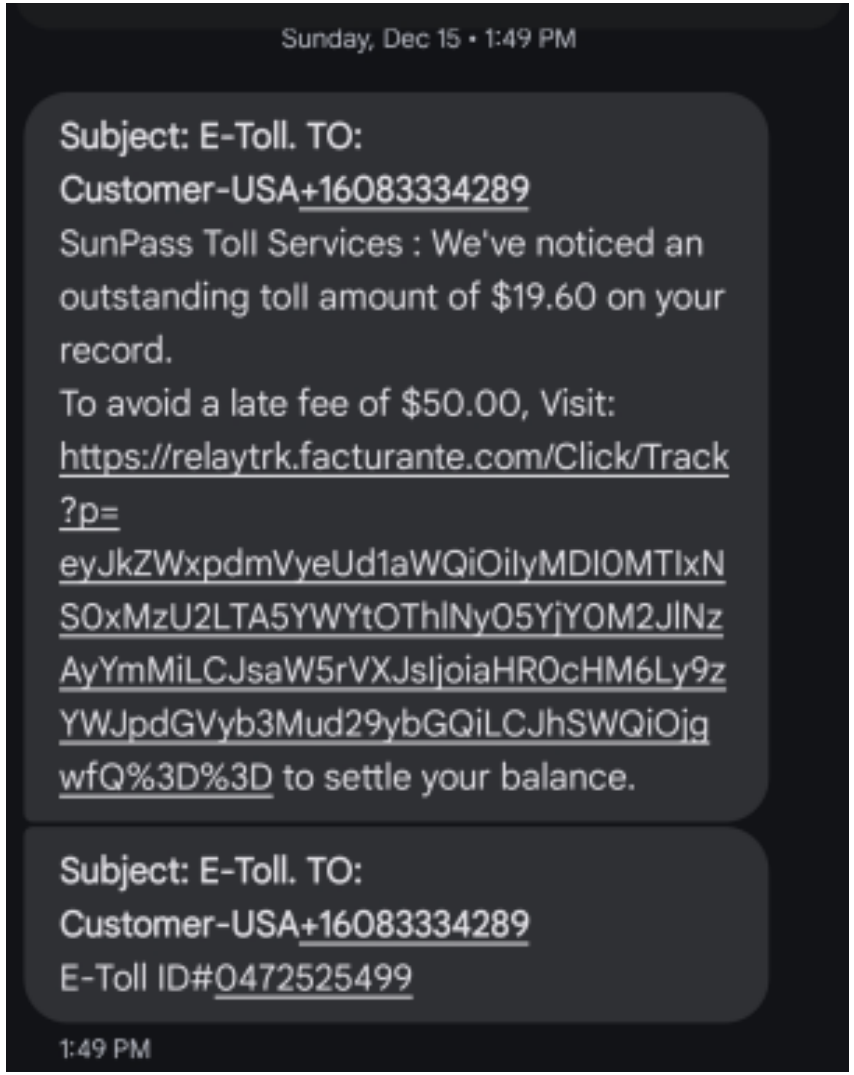


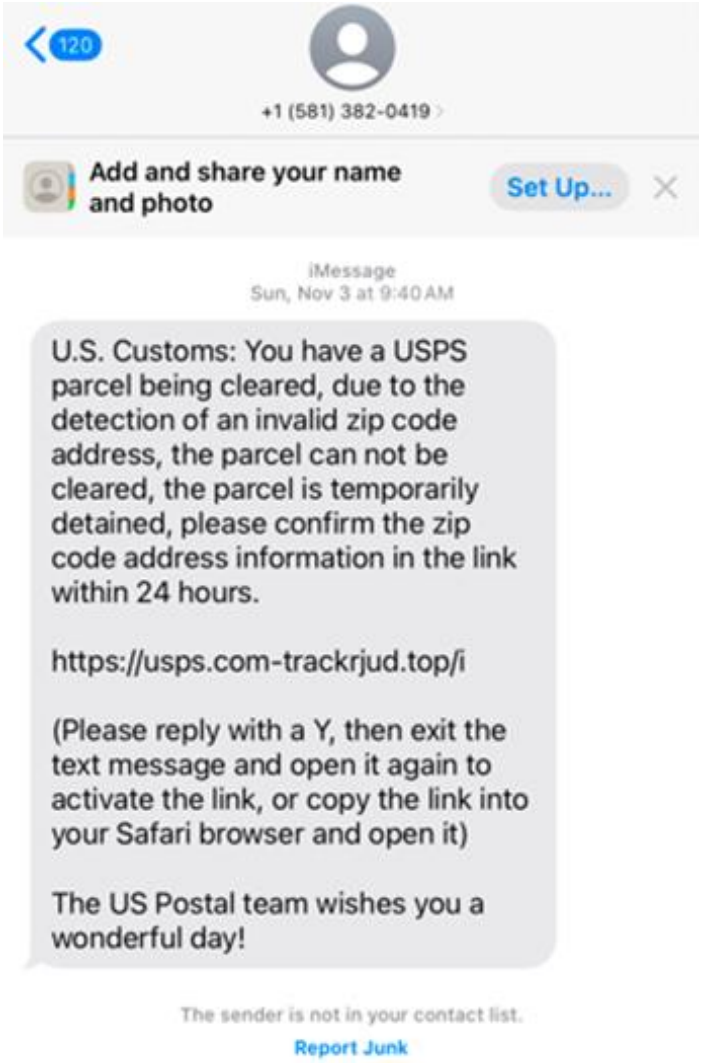
Tech Support Pop Up Scam

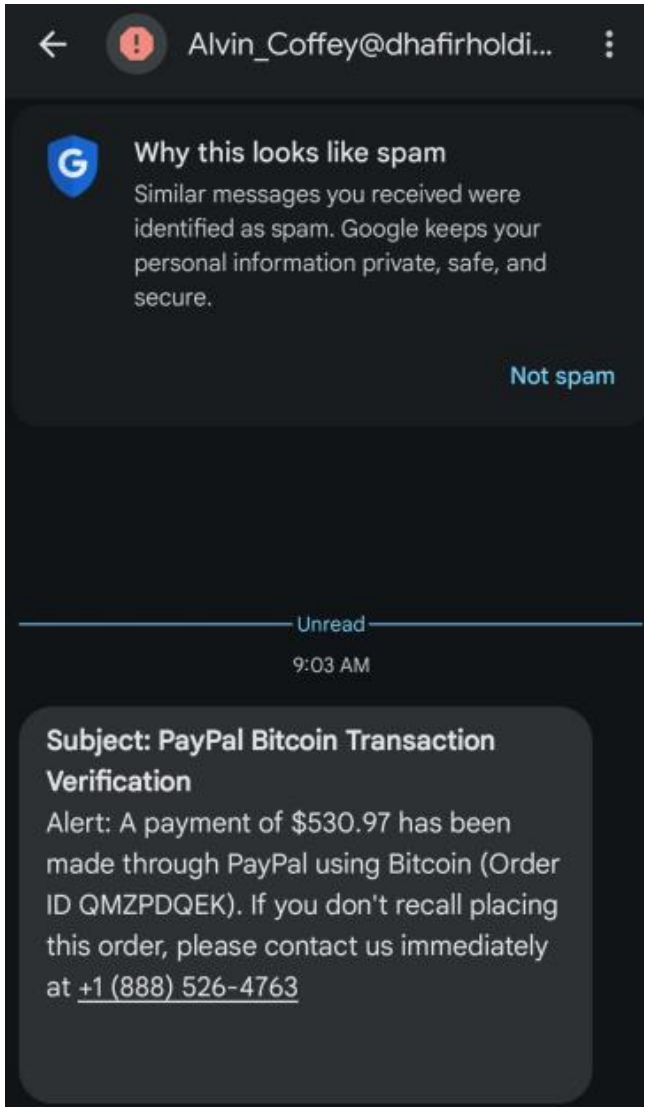


Tech Support Pop Up Warning Signs

- If you receive a pop up urging to call a number - Do NOT click on pop up or call number displayed – instead shut the device off and disconnect from the internet immediately.
- Do not allow anyone remote access to your device
- If you are instructed to lie to your family, friends or financial it is a scam!


Sunday, Dec 15 • 1:49 PM
Subject: E-Toll. TO: Customer-USA+16083334289
SunPass Toll Services : We've noticed an outstanding toll amount of $19.60 on your record.
To avoid a late fee of $50.00, Visit: https://relaytrk.facturante.com/Click/Track?p=eyJkZWxpdmVyeUd1aWQiOiIyMDI0MTIxNS0xMzU2LTA5YWYtOThlNy05YjY0M2JlNzAyYmMiLCJsaW5rVXJsIjoiaHR0cHM6Ly9zYWJpdGVyb3Mud29ybGQiLCJhSWQiOjgwfQ%3D%3D to settle your balance.
Subject: E-Toll. TO: Customer-USA+16083334289
E-Toll ID#0472525499
1:49 PM


120
+1 (581) 382-0419
Add and share your name and photo
Set Up...
iMessage
Sun, Nov 3 at 9:40 AM
U.S. Customs: You have a USPS parcel being cleared, due to the detection of an invalid zip code address, the parcel can not be cleared, the parcel is temporarily detained, please confirm the zip code address information in the link within 24 hours.
https://usps.com-trackrjud.top/i
(Please reply with a Y, then exit the text message and open it again to activate the link, or copy the link into your Safari browser and open it)
The US Postal team wishes you a wonderful day!
The sender is not in your contact list.
Report Junk


Alvin_Coffey@dhafirholdi...
Why this looks like spam
Similar messages you received were identified as spam. Google keeps your personal information private, safe, and secure.
Not spam
Unread
9:03 AM
Subject: PayPal Bitcoin Transaction Verification
Alert: A payment of $530.97 has been made through PayPal using Bitcoin (Order ID QMZPDQEK). If you don't recall placing this order, please contact us immediately at +1 (888) 526-4763

Phishing and Smishing

- Smishing/Phishing is the fraudulent practice of sending text/emails pretending to be reputable companies
  - Usually they are stating an urgent payment is needed and a link is embeded
- Purpose is to trick individuals to reveal personal information such as card numbers, passwords and SSN
- Do not let your guard down even if you believe you are talking to the company!
- Look for spelling mistakes, grammar and the web link address.

Fraud with credit and debit cards

- **Benefits of Cards**
  - Safer and more convenient than cash
  - The benefits offered by Visa protect cardholders
  - No liability on the cardholder for charges that they do not authorize
    - Dispute vs Fraud

- **Cardholder Responsibilities**
  - Never share your card, card number or pin with anyone
  - Report lost or stolen cards immediately
    - Most financials offer the ability to lock your card if you are not sure if it is fully missing
  - Notify you bank if there are unauthorized charges

Identity Theft

Every 3 seconds someone's identity is stolen…

Who is most at risk?

1. Children are targeted 35x more than adults
2. People with social media profiles
3. College students
4. Deceased individuals

*Identity theft victims spend **165 hours** repairing the damage done by the creation of fraudulent accounts.*

Identity Theft Prevention

- Do not carry your SSN card with you
- Freeze your credit with the three credit bureaus – It's FREE!
  - Experian
  - Equifax
  - TransUnion
- Review your credit report annually
- If you have been a victim visit identitytheft.gov

Fraud Prevention

What is one common thing with all the scams we reviewed today?

That you must act and most of the time it must be done urgently

- Beware of phishing and spoofing
- Don’t click on links in emails, text message or social media messages from people you don’t know
- Monitor your account for accuracy
- Choose passwords wisely and keep them confidential
- Do NOT lie to you financial
- Last and certainly not least, please keep you contact information in your account up to date

Other Tips/Advice

- Don't leave your purse in a locked or unlocked car – especially at work out gyms and hiking trails/parks! If you put it into a locker, make sure it's locked!
- If you google a support number for Amazon, Apple or Cash App, don't assume that number is correct. A lot of those platforms don't have support numbers to call. Log into your account to find a way to contact them. If the support person starts asking for payments through gift cards or cash app or advises you to download an app to get onto their device hang up! Do not allow someone on your device.
- Listen to your gut, if something doesn’t feel right take a step back!
- Have a healthy level of paranoia!

Resources

- IdentityTheft.gov
- www.uwcu.org
  - Banzai
  - Green Path
  - Savvy Money
- Annualcreditreport.com

Questions?

uw credit union