



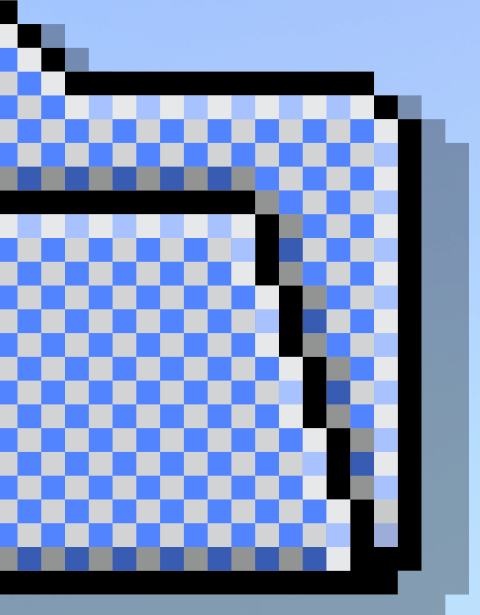
HARRISON TOWNSHIP
PUBLIC LIBRARY



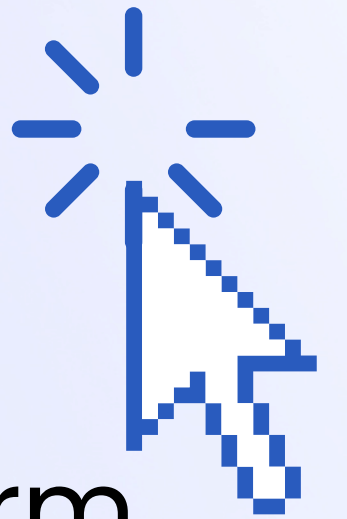
Tech Time at HTPL

Avoiding Cyber Scams





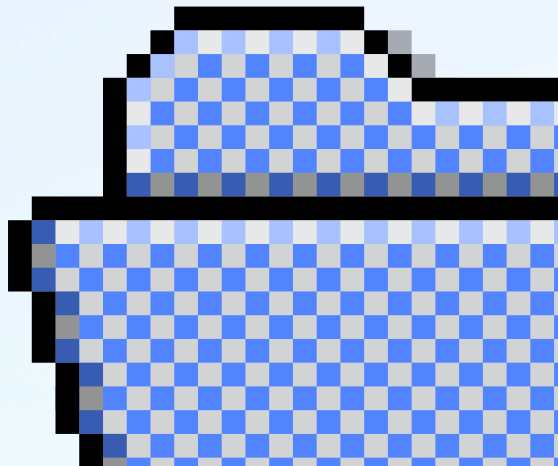
Terms to Know



Cyber Scams: People using the internet as a tool to harm a person by means of deception

Cyber Security: The practice of protecting computer systems, networks, and data from digital attacks, theft, or damage

For more in-depth terms, visit
<https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/common-terms/>



Statistics

The FBI's Internet Crime Complaint Center's annual report, released in April 2025, reported just under one million cyber scam reports filed, with losses exceeding \$16 billion—a 33% increase in losses from 2023. **And this is just from official reports! 142,000 of these reports were from Michigan.**

The top three cyber crimes, by number of complaints reported by victims in 2024, were phishing/spoofing, extortion, and personal data breaches.

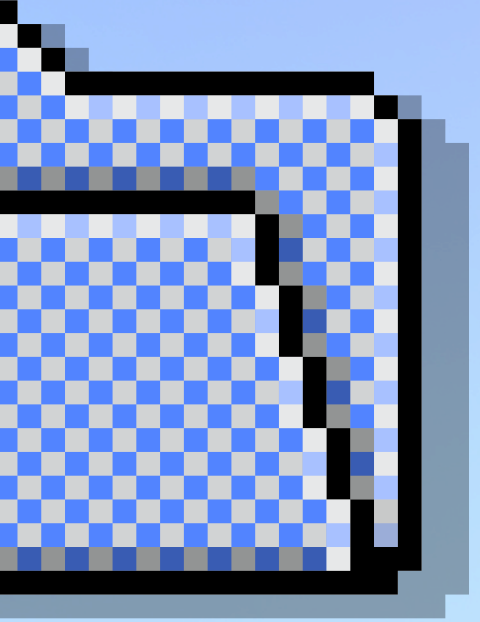
The top cyber crimes **reported from Michigan** were imposter scams and online shopping scams.

The highest age group victimized by cyber crimes was people **in their 60s**, but people **in their 20s** reported an increase in losing money online.

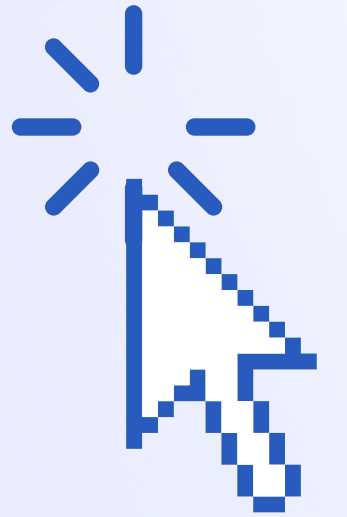
Sources: <https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report>
<https://consumer.ftc.gov/consumer-alerts/2025/03/top-scams-2024>

Basics of Recognizing Scammers

- **Can be persistent or demanding**
 - “Act now!” or putting a time limit on when to respond
 - Fast talking but vague details
- **Can be threatening**
 - Could threaten being arrested or breaking the law if you don’t do (x) action
- **Threats related to money**
 - Urge you to transfer money to “protect” it, or threaten a deadline for paying something back
- **Claims to be helping an agency, usually government**
 - No government worker will ever call you directly unless you contacted an agency first
- **“Too good to be true”**
 - Either they’re rescuing you or you’re rescuing them
- **Payments in strange forms like gift cards or bitcoin**
- **Misuse of terminology**
 - ie: referring to the Michigan Secretary of State as the DMV

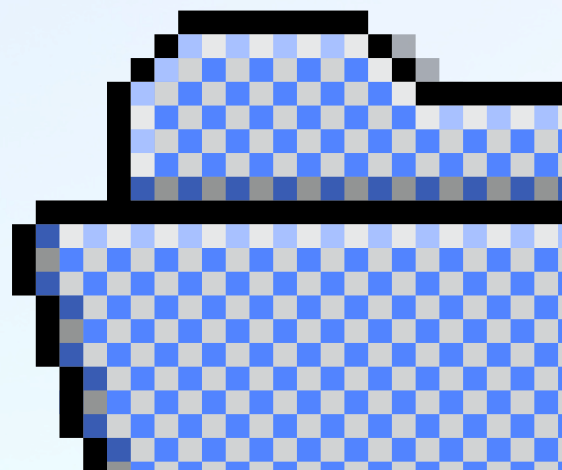
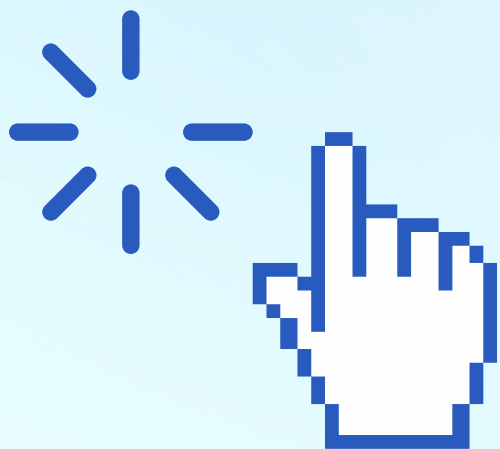


Common Cyber Scams



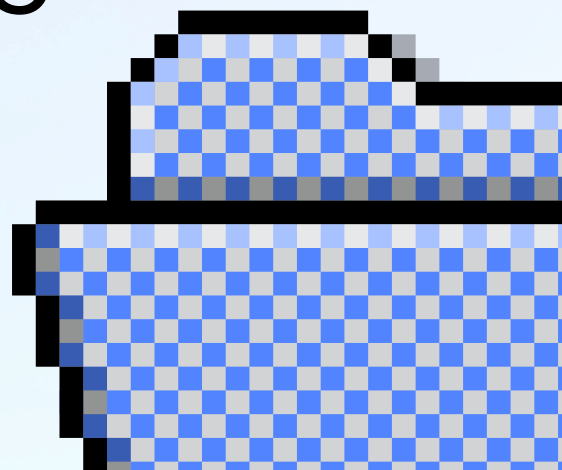
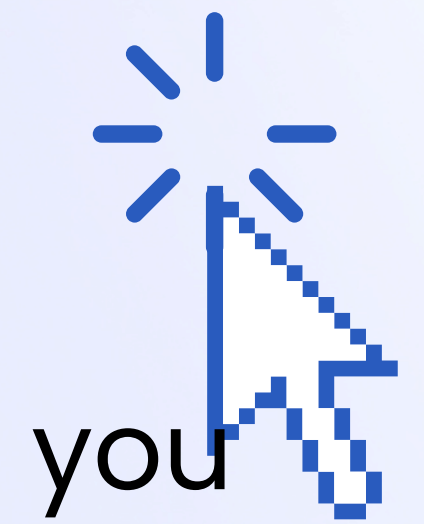
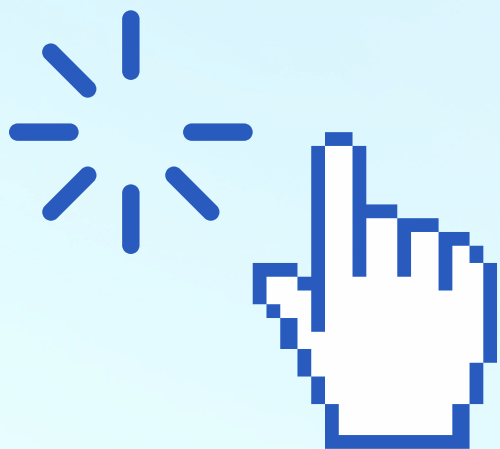
There are dozens and dozens of types of scams. We'll take a look at some common cyber scams you might hear about in 2025 to familiarize you with what to look out for.

Many of these scams could also occur off of the internet, like via phone call.

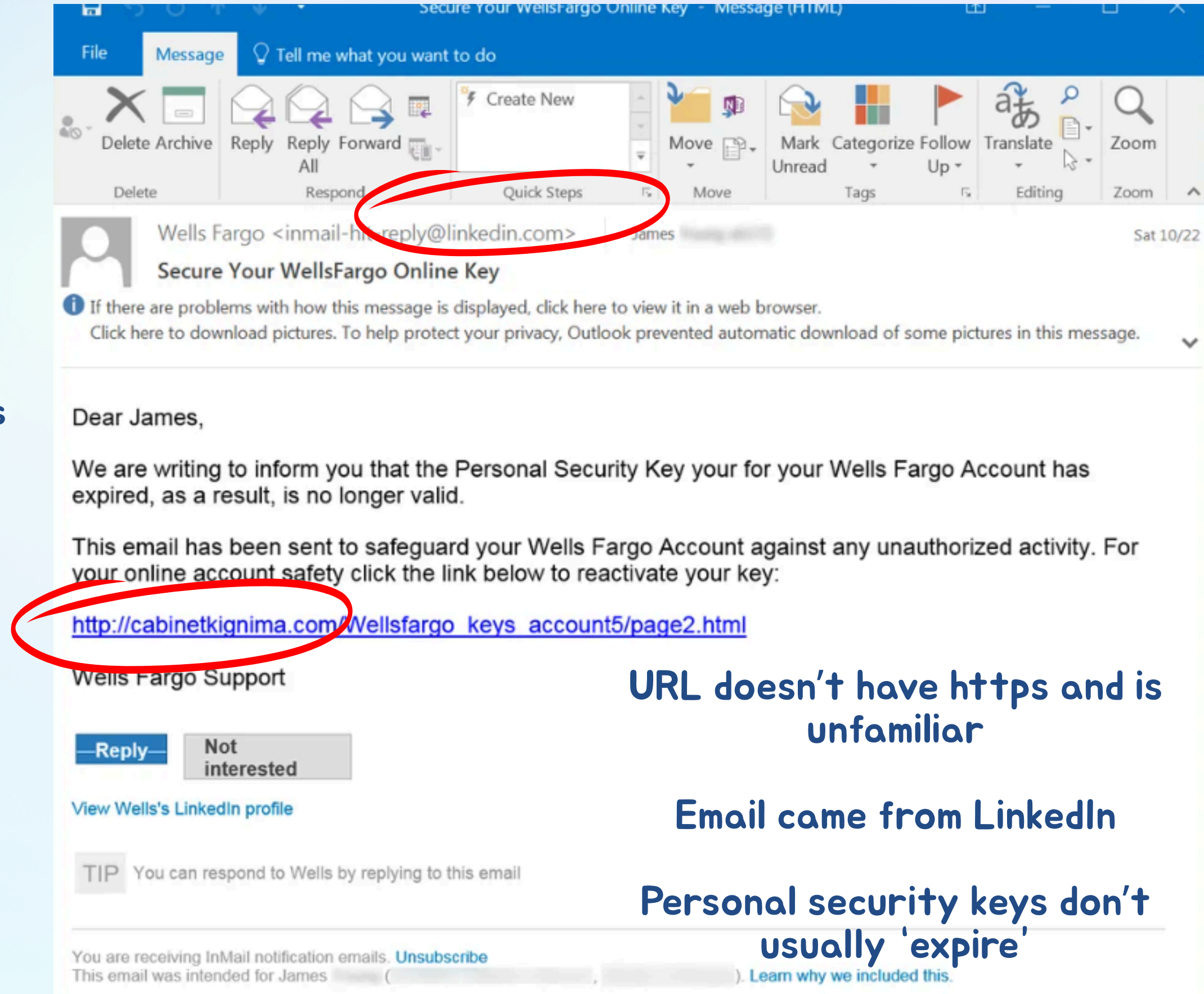
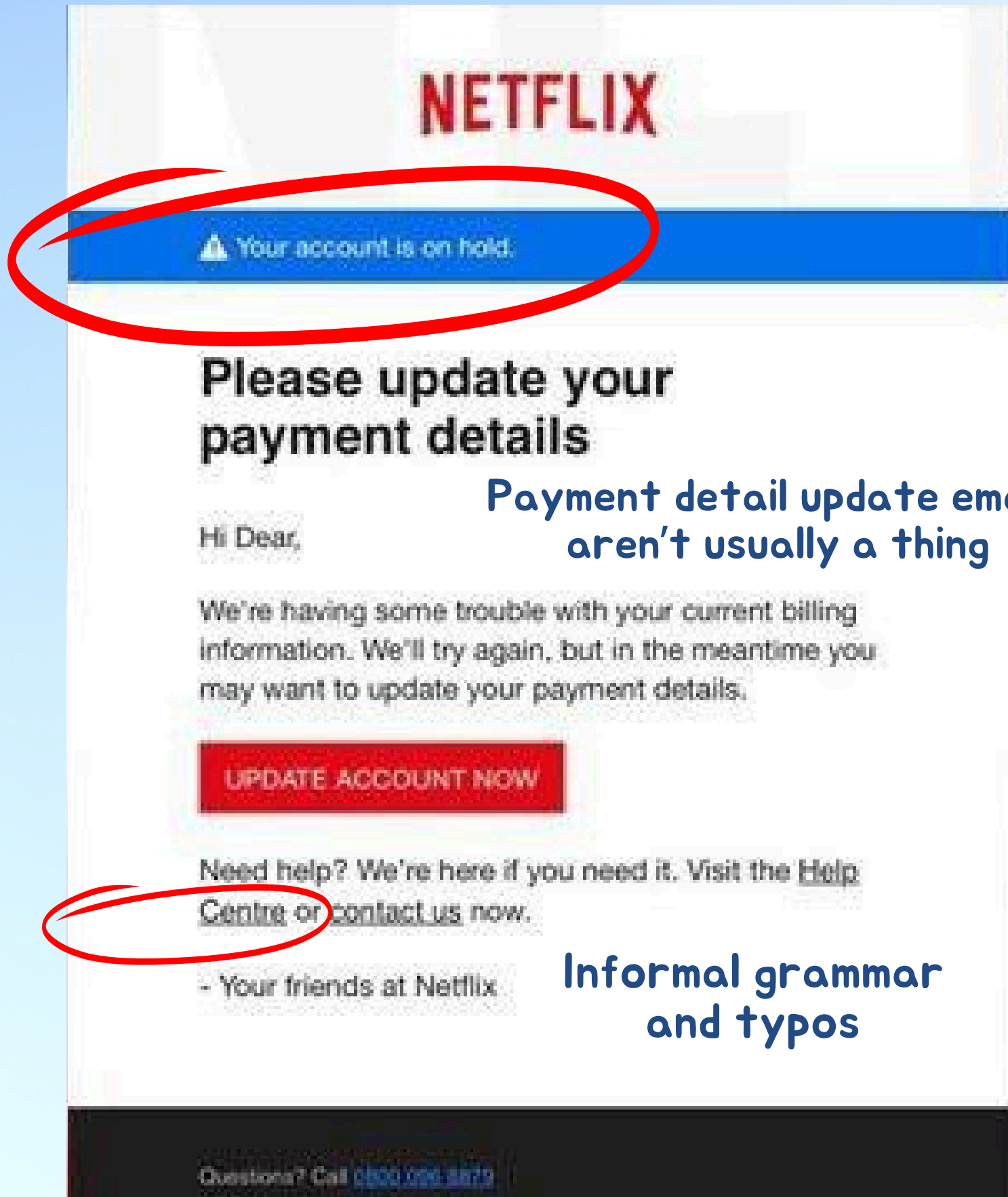


Phishing

- **Phishing** is a classic scamming method that tricks you into giving away personal information via email, text, or sometimes fake websites
- Usually scammers will try to create a sense of fake urgency or trust in established brands to get you to reveal personal information to them
- Revealing your username and password is often the first step
 - Giving the scammer any account information to help them out can lead to later financial damage



Phishing Examples



Phishing

- **Check the sender of the email/text.** Usually, scam emails won't make any sense. They contain random numbers or letters. Scam texts will often have an unfamiliar area code.
- **Check for grammatical errors.**
- If a phone number or website is provided, try Googling it. Can you locate it easily on the internet?
- Have you interacted with the company recently (ie: Amazon, UPS)? If so, visit their official website, log in, or give them a call. If you're worried about the contents of the potential scam, it doesn't hurt to contact the company and ask.

Tech Support Scams

- **Tech Support scams** refer to scammers who pose as representatives for popular tech companies like Microsoft, Best Buy's GeekSquad, Google, etc.
- Usually these scams involve pressuring you into buying unnecessary technical support, downloading malicious software, or updating payment info for a subscription.
- Similar to classic phishing scams, these scams have a sense of urgency - "your subscription will end," "you will lose tech support," etc.

Tech Support Scam Examples



Lack of your
personal information

No official links or
logos

Dear User,

Your Subscription with GEEK SQUAD will Renew Today and \$349.99 is about to be Debited from your account by Today. The Debited Amount will be reflected within the next 24. In case of any further clarifications or block the auto-renewal service please reach out Customer Help Center.

Customer ID: [REDACTED]

Invoice Number: YDGC9873

Description	Quantity	Unit Price	Total
Geek Squad Best Buy Service (One Year Subscription)			

Subtotal \$349.99

Sales Tax \$0.00

Total \$349.99

If you didn't authorize this Charge, you have 24 Hrs. To cancel & get an instant refund of your annual subscription, please contact our customer care: [REDACTED]

'24 hours to cancel'

Grammatical errors
(weird capitalization)

IMPORTANT: You may have spyware/adware

Your personal data could be at risk. It is not advised to continue using this computer without making sure you are protected.

Possible threats:



Possible Threat: spyware/adware
Your OS: Windows
Version: Windows 8.1
Date: March 17, 2015

Message from webpage



WARNING: Time Warner Cable Customer - Your Internet Explorer browser and computer may be compromised by security threats. Call 844-335-2291 now for IMMEDIATE assistance.

OK

The following information could be at risk:

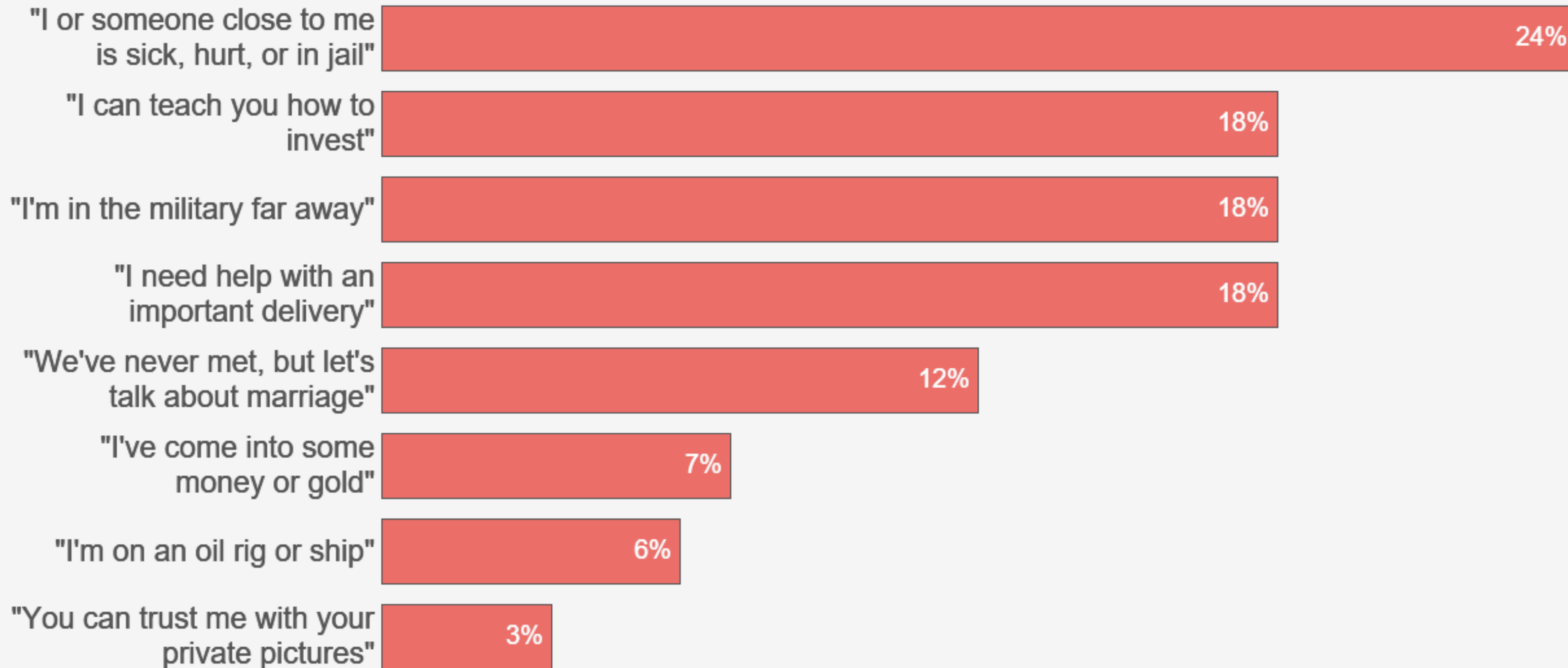
- Your credit card and bank account Information
- Your account passwords
- Your Facebook chat conversation logs
- Chat logs of Instant Messengers like AIM, Skype etc
- Your private photos and other sensitive files
- Webcam Privacy (your webcam can be turned on remotely at any time without you knowing)

Vague description of 'spyware/adware'
Pretending to be Windows but no logo or
official website given
Phone number isn't official
'IMMEDIATE' assistance + weird grammar

Dating/Romance Scams

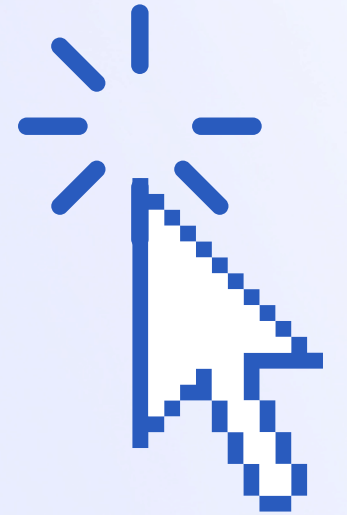
- **Dating and Romance Scams** occur online, usually on social media or dating apps
- Scammers build fake online personas to lure victims into relationships
- Scammers utilize “love bombing” tactics (showering victim with intense affection in a short period of time)
- After gaining your trust, the scammers will often try to convince the victim to send money, gifts, or help with some other kind of grandiose action
- Usually scammers will deny in-person action and push for secretive behavior

Romance Scammers: Their Favorite Lies by the Numbers

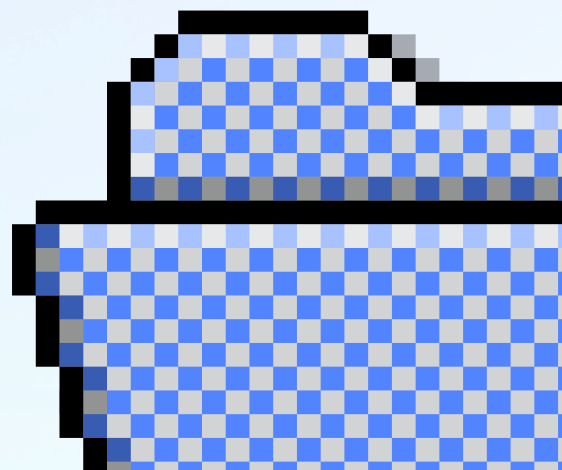
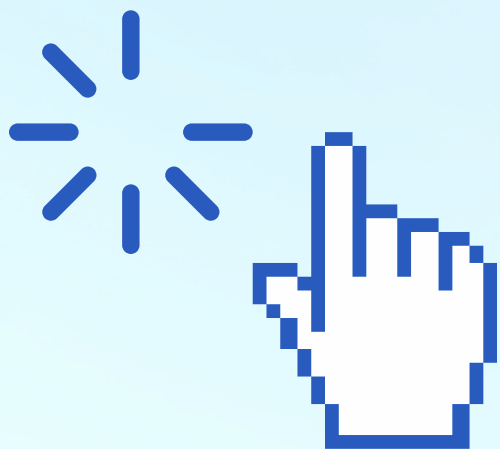


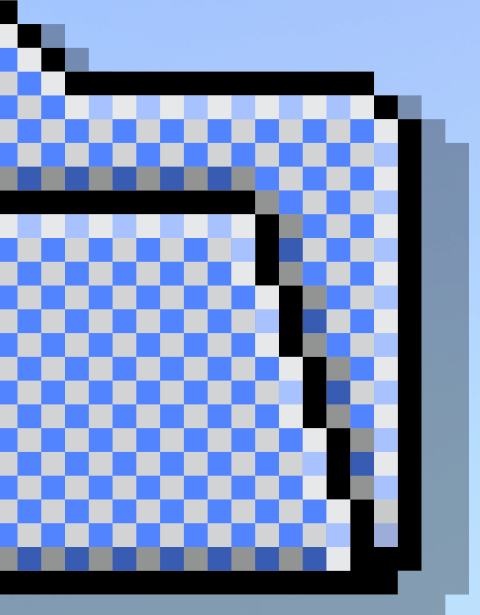
Figures are based on 8,070 2022 romance scam reports that indicated a dollar loss and included a narrative of at least 2,000 characters in length. Lies were identified using keyword analysis of the narratives.

Dating/Romance Scams

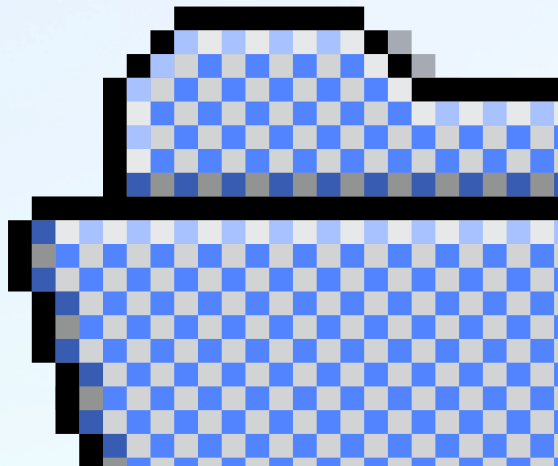


- **Google the person's supposed name, or reverse-image search their photos.**
- Never send anyone who isn't a close friend or family money or pay by gift card, bitcoin, etc.
- Talk to friends and family about the person. Dating/Romance scammers often try to isolate the victim from their support system.
- Be wary of people who move too quickly, but refuse to meet up.





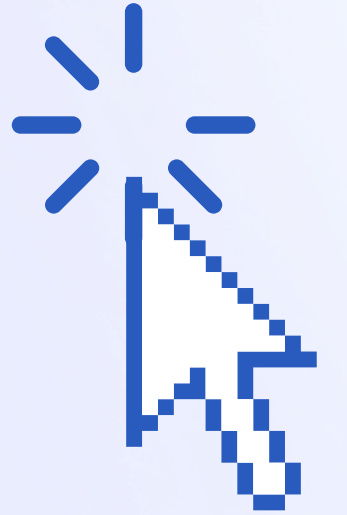
Online Shopping Scams

- **Online Shopping scams** can happen in a variety of ways
 - Usually scammers will try to lure you with deals that seem too good to be true if they are trying to scam you on a buying/selling app, or they will claim that your account is “in danger” of something if scamming via email or text
 - Scammers typically have little to no reviews on a selling app or a generic profile photo/username
- 

Online Shopping Scams

- **Popular websites to buy or sell on:** Facebook Marketplace, Craigslist, Ebay, Etsy, Poshmark, Mercari, Nextdoor, Depop
- **Ways scammers might manifest on these platforms:**
 - Fake payment receipts – you think you were paid, so you sell the goods
 - Overpayment – the scammer sent you a fake payment page, then asks you to send payment back
 - Bootleg or broken items were received by you
 - Shipping scams – the buyer creates a fake page so you think the item sent
 - Conversations move out of the app to a different platform

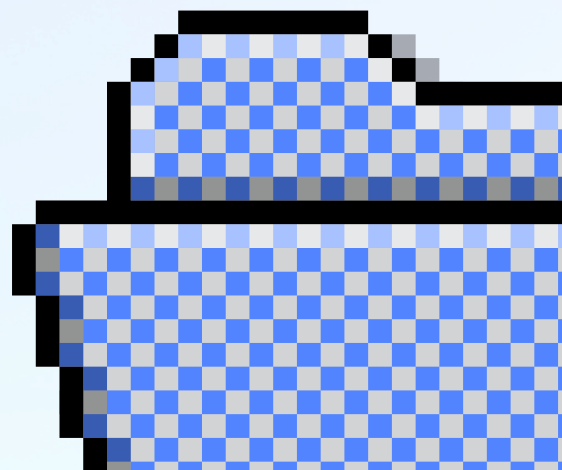
Online Shopping Scams

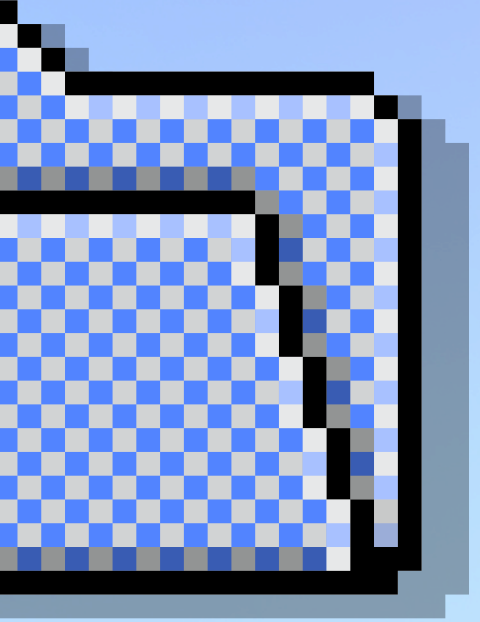


- **Look out for fake websites or apps**
 - Does the service have any reviews? Is it a household name?
- **Ensure that you only open emails from official websites and beware of strange phone numbers**
- **Look for websites beginning with https://, not http:**
 - You can also look for a padlock icon near the URL, which ensures that the website is secure

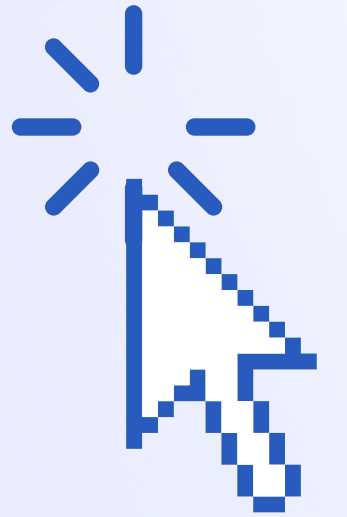
Further examples:

<https://www.getcybersafe.gc.ca/en/resources/real-examples-fake-online-stores>





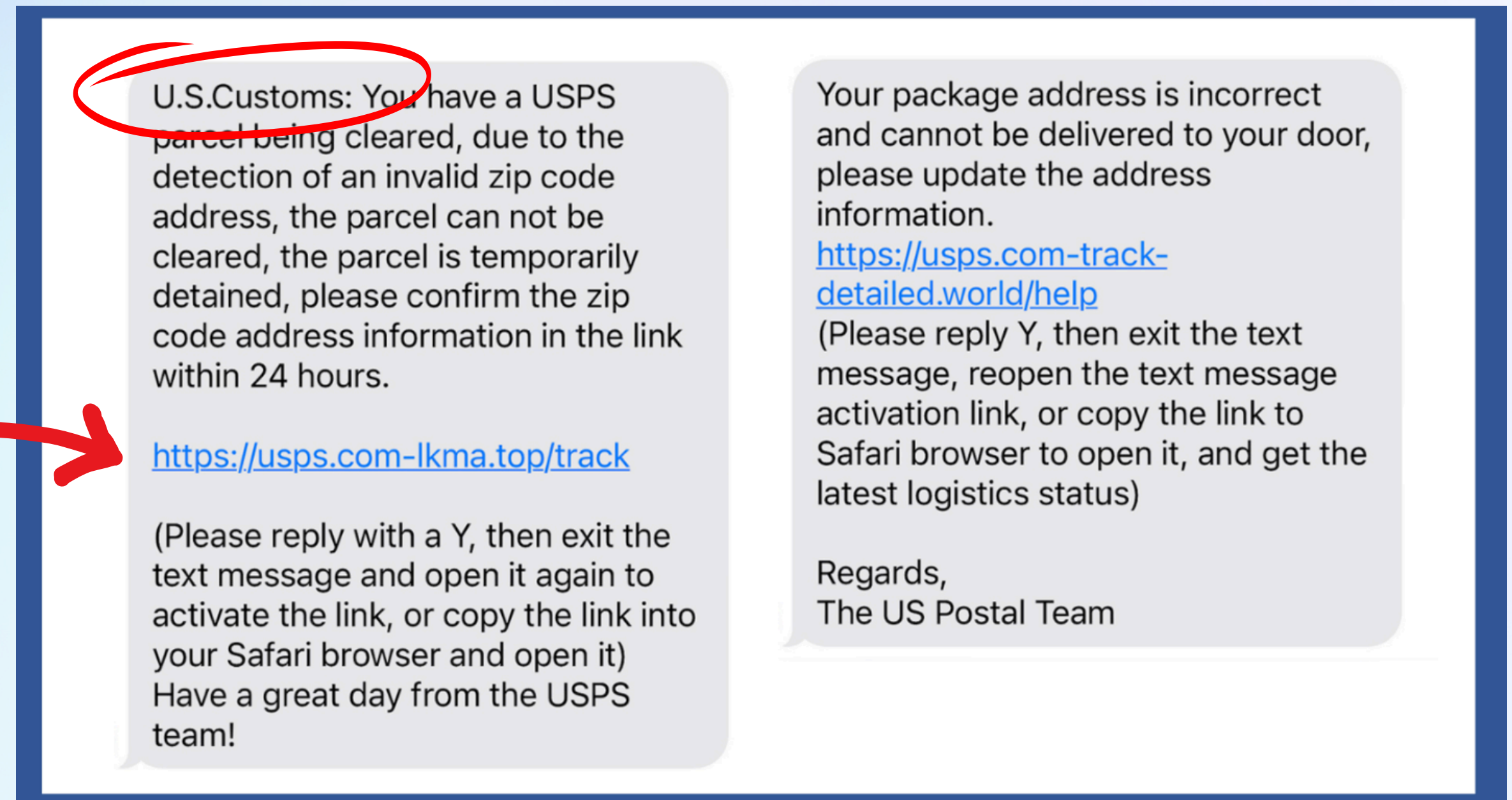
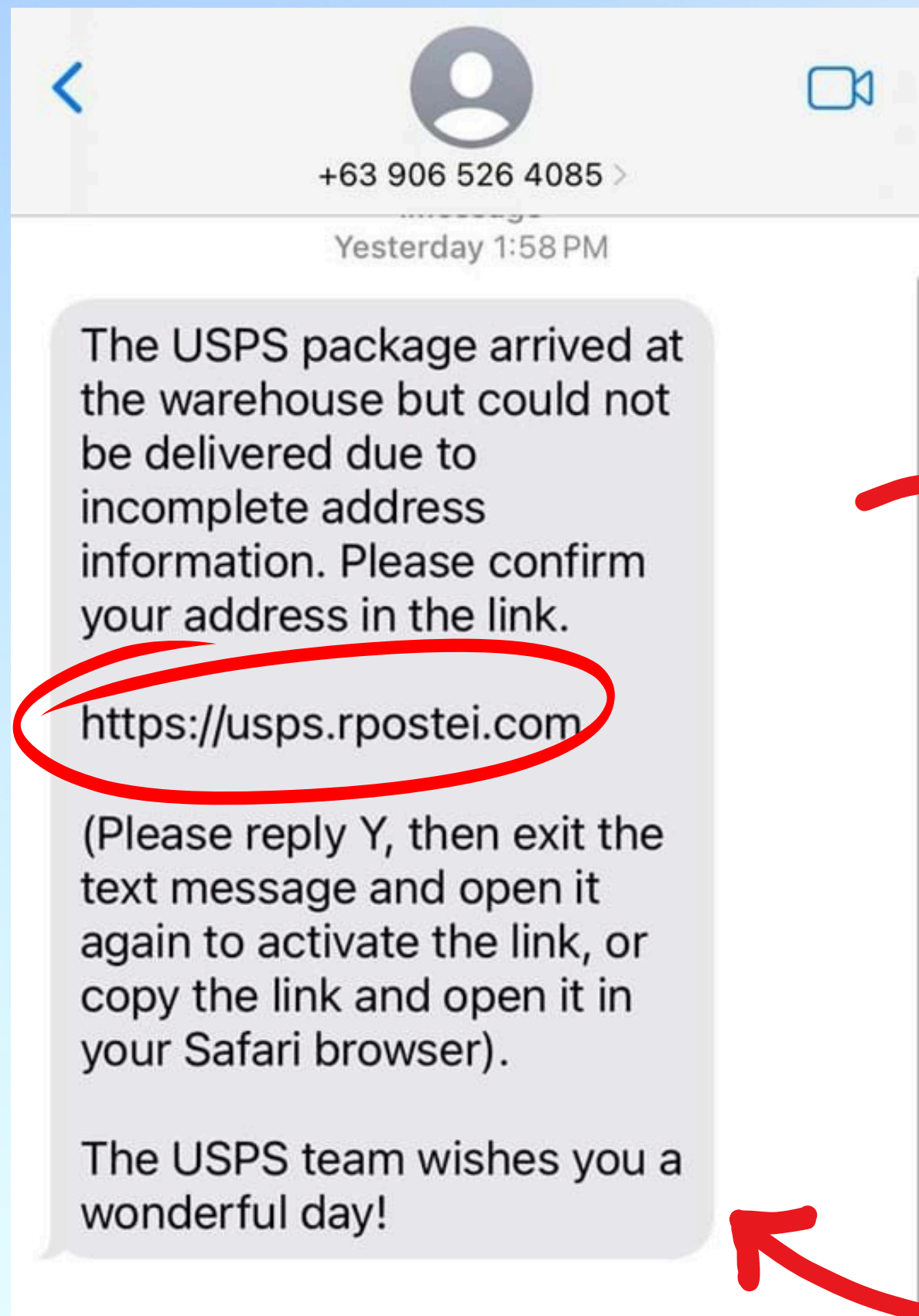
Package Delivery Scams



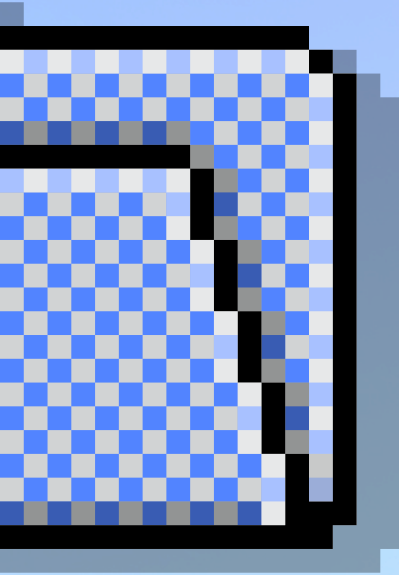
- **Similar to Online Shopping scams, a popular method of scamming nowadays is the Fake Package Delivery scam.**
- Via text or email, you'll receive a message claiming a missed delivery attempt or some kind of issue with Fedex, USPS, etc.
- Usually these contain a link that will download malware or request personal information
- **To avoid these scams,** consider blocking or reporting the number or email they came from, and delete them immediately. If you're worried about a potential package issue, visit the website you ordered from and track your shipment from there.



Package Delivery Scams



- **Unknown numbers**
- **Website is unofficial - despite using https, there are breaks in the '.com' website URL - look carefully!**
- **Complicated 'reply' options**
- **Informal ending to text ('regards', wishes you a wonderful day)**



Robocall Scams



- **Robocall Scams** are automated calls that have a hidden agenda
- Scammers will often impersonate government agencies (ie: IRS) or offer non-existent services in order to steal your personal info
- With the rise of AI, it has become common for scammers to impersonate the voices of people or organizations that you trust

Example of AI scams: <https://www.youtube.com/watch?v=gMXuQ4MusPk>



The best ways to dodge Robocall scams are to **not answer unknown numbers** and **verify weird calls with trusted family members or friends, or even government agencies.**

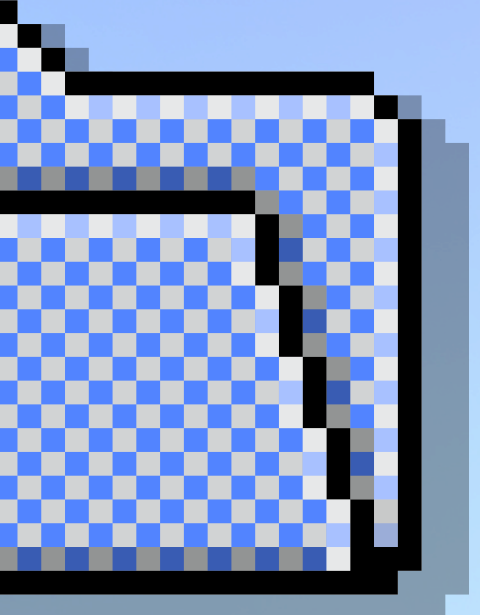
Robocall Scams

- **Examples of common Robocall scams**

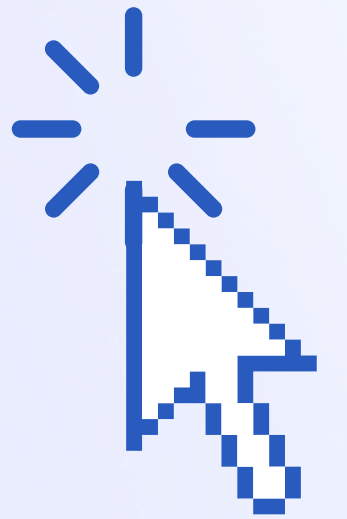
- A call that sounds like your boss asks for your bank account number to update your payroll information
- A call that sounds like a family member asking for dire help in an emergency with vague details, using a phone number that is a “new number” or a “friend’s number”
- A call that sounds like a representative from the IRS urges you to act fast as your tax information didn’t go through correctly

More examples:

<https://consumer.ftc.gov/features/robocall-scam-examples>



Fake Job Scams



- **A new form of cyber scam includes the Fake Employment scams.** These rose by 45% in 2024!
- These scams can be difficult to spot, as scammers usually create listings on official job posting websites such as Indeed or LinkedIn
- Usually the objective of scammers here is to gain personal information via your job application, sometimes even offering you the job, obtaining your financial information for “payroll,” and then vanishing



Info: <https://www.indeed.com/career-advice/finding-a-job/job-scams>



Fake Job Scams

- **Examples of Fake Job scams:**

- Fake job listings are posted on the internet. Usually the employer is not verified on the website they posted on (LinkedIn, Indeed, ZipRecruiter, etc.) or they ask for a fee to start the application. This is common with work from home jobs!
- Imposters pose as job recruiters and ask applicants for payment
- Email offers – a “recruiter” reaches out via email with an offer
- Interviews are conducted via an online messaging service
- The “recruiter” asks for a credit report to be run before employment
- A “career consultant” reaches out with praise for your resume and offers to “improve it” for a fee
- The offer is often too good to be true (ie: \$2000 every week)

Fake Job Scams

Yes I am interested

GREAT! FOR THE NEXT STEP I
NEED FOR YOU TO SEND A COPY
OF YOUR MISSOURI ISSUED I.D.
ALONG WITH YOUR SOCIAL
SECURITY # & DATE OF BIRTH FOR
YOUR 24 HOUR BACK GROUND
CHECK. DOCUMENTS MAY ALSO
BE SENT TO:

PHASE3366@GMAIL.COM

WE HOPE TO HEAR FROM YOU
SOON!!

**Incorrect grammar and
spacing**

**'We found your profile
on job-seeker website'
(unspecific, incorrect
grammar)**

Wage is unrealistic

**Responsibilities are
basic**

Spelling errors

**Awkward phrasing
('user of office related
things')**

We have found your profile on job-seeker website and we think you would be a perfect match for our currently open position. We are providing good wage rates, workers spending full time are given extra benefits and the relaxation of doing their job from home at any set time. If you don't want to avail this opportunity, please ignore this email. If you wish to apply for this vacancy, please reply to this email and our manager will be contacting you soon.

Title: Quality control manager

Assistances: Eligible

Employment type: Part-time

Wage: \$3200 per month

Responsibilities:

- Review correspondence for flaws
- Managing mail carries with care USPS, UPS, FedEx, DHL
- Accurately record large amount of shipping information

Qualifications:

- Should have a minimum age of 18 years
- United States Resident
- Have basic computer skills
- User of office related things scanner, printer, copier etc.
- Should be able to handle packages up to 30 lbs.

**All caps, poor grammar
Email account is odd name/unofficial
Asks for Soc. and ID before even filling
out application**

Fake Job Scams

- **Avoiding Fake Job scams**
 - Research the company before applying, and read reviews
 - Do not partake in any discussion via instant messaging
 - Make sure the company is verified, has its own website, has reviews, has physical photos, etc.
 - Never provide payment for a job application
 - Talk to friends, family, or previous employers for opinions and advice before applying
 - Contact the company directly if you have doubts
 - Never give out personal information via email without conducting an in-person or official Zoom interview first (driver's license, SSN, etc.)

How to Stay Safe

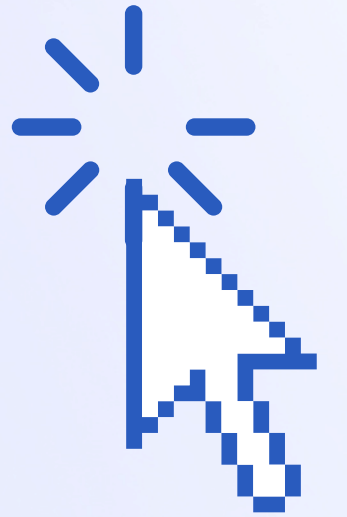
- **DON'T answer texts, phone calls, or emails you don't recognize.** Don't click any links involved with the messages either. If the supposed organization *really* wants to contact you, they will multiple times. You can also contact them directly and ask! It's not worth the risk.
- **Check the spelling and grammar of the suspicious message.** Google the associated website or phone number to see if any results pop up.
 - ie: Government websites usually end in .gov. Websites that aren't suspicious just end with .com, no hyphens or weird dots in between
- **Use strong passwords** (use numbers and symbols in them) and have different passwords for different websites. Store them somewhere safe like a physical password journal.
- If someone calls or texts claiming to be your loved one and asking for personal information or money, but you don't recognize the number, call or text their known number and ask if they sent you something.

What to Do If You Suspect You Were Scammed

- Take screenshots for evidence or save all potential evidence
- Report that you're a victim of a scam to your bank or financial institution, your local police department, and/or <https://www.ic3.gov/> (Internet Crime Center) and take recommended next steps from them
 - If you used a credit card or bank account, contact that institution to close the card or protect your account
- Contact loved ones or anyone who may need to know

More resources: <https://consumer.ftc.gov/articles/what-do-if-you-were-scammed>

Who to Contact Regarding Cyber Scams

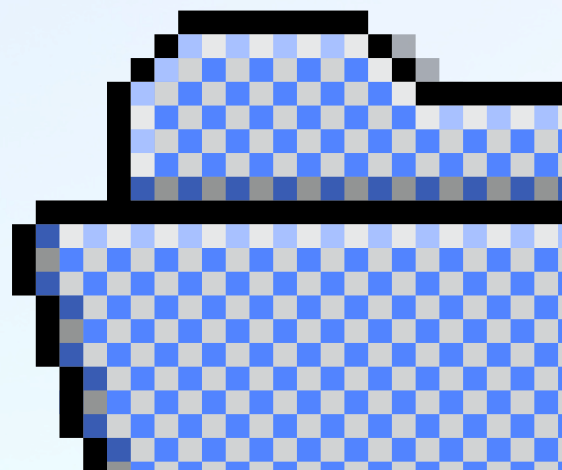


Macomb County Prosecutor's Office – Cyber Crimes Unit
(586) 469-5100

ReportFraud.ftc.gov – shares info with over 2,000 law enforcement officers nationwide

Local Police Department

Additional resources for contacting others at
michigan.gov/dtmb/services/cybersecurity



Resources

- <https://www.fdic.gov/consumer-resource-center/2021-10/avoiding-scams-and-scammers>
- <https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>
- <https://www.phishing.org/phishing-examples>
- <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams>