2022 Internet Scams Targeting Seniors

Presented by Andrew J. Mayers

Objectives

- **To learn and become aware of the latest scams targeting seniors in 2021.**
- **To learn safe strategies and best practices for avoiding scams, and helping to recognize if someone else is a victim of a scam.**
- **To learn about the resources available to you if you have been scammed.**

Alarming Statistics!

- According to the Federal Trade Commission (FTC), each year tens of millions of Americans have their personal information stolen through a scam or data breach.

- The National Council on Aging estimates that **the annual cost of elder financial abuse is close to $35 Billion** and rising.

- According to the National Center on Elder Abuse, approximately **1 in 10 seniors are victimized financially**.

Alarming Statistics!

- These scams are out to drain senior victims of their retirement funds and government benefits.

- The American Journal of Public Health estimates that about **5 percent of the elderly population** (*which equates to around two to three million people*) **suffer from some sort of scam every year**.

- This is likely an underestimate, since it's expected that a *large percentage of Internet scams go unreported.*

Risk Factors for senior-targeted scams

- Isolation — can make seniors susceptible
- Financial circumstances
- Trusting nature
- Insecurities/Anxieties that are triggered by scam may lead to fear-based decisions
- Memory and cognitive changes
- Being too embarrassed to report they were scammed means scammers know there is a lower chance of being caught

Email Phishing

- Email “**Phishing**” (as in fishing for information)
- Scammers send phony emails, claiming to come from reputable companies such as the bank, only to request personal or account information to use for their own benefit.
- Victims often respond by providing their personal and financial information (with good intent) and unfortunately are subjected to identify theft

How to detect a Phishing email

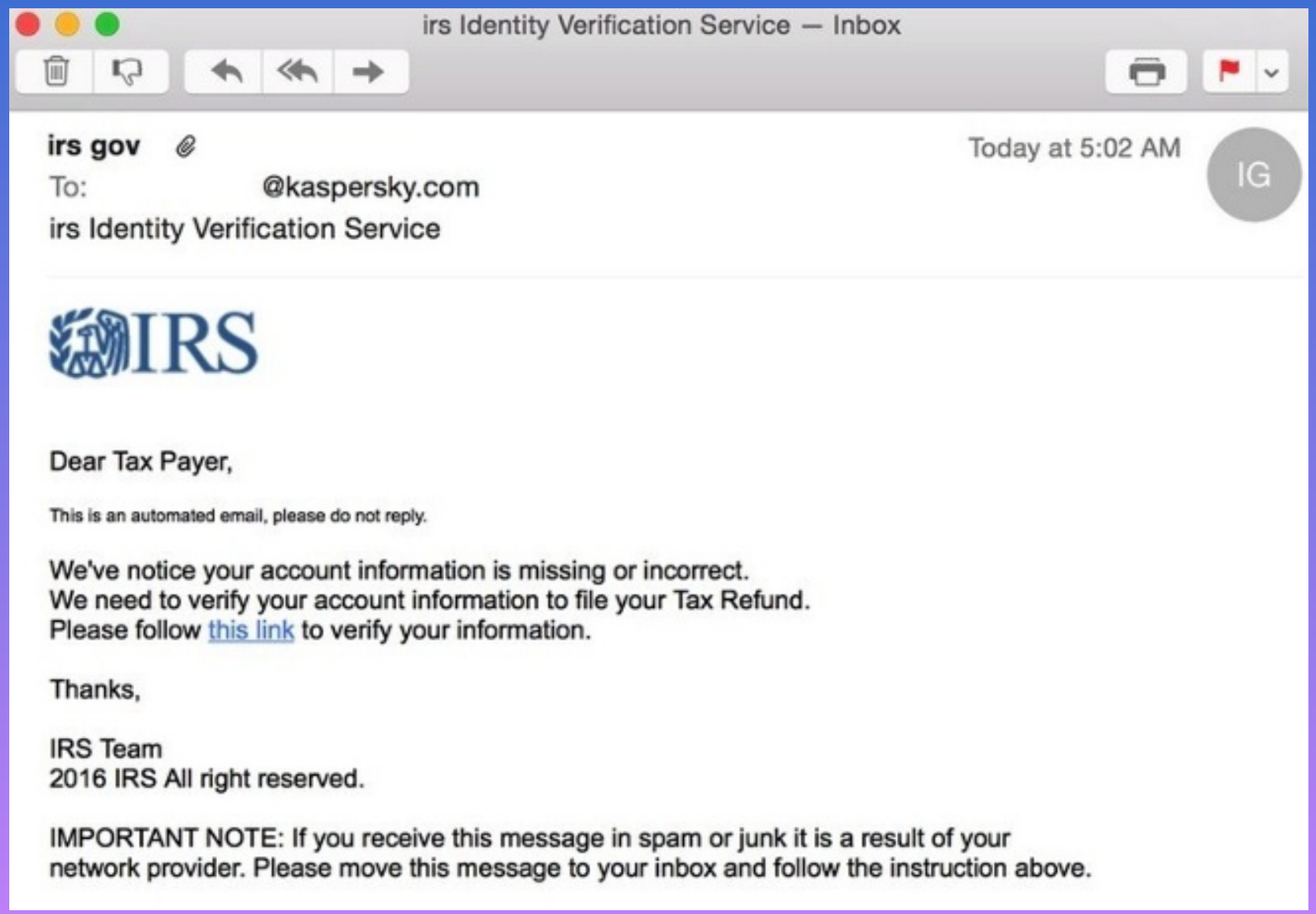
- Don’t trust the display name
- Be aware of grammatical errors and unprofessionalism
- Be aware of scare tactics and other emotional manipulation
- Analyze the email for suspicious links
- Be aware of how they address you
- Reputable companies will never ask for personal information over an email

Collection Fraud—IRS Phishing

- Example: Scammers claim to be the IRS, scaring you into believing you are unable to file your tax refund.

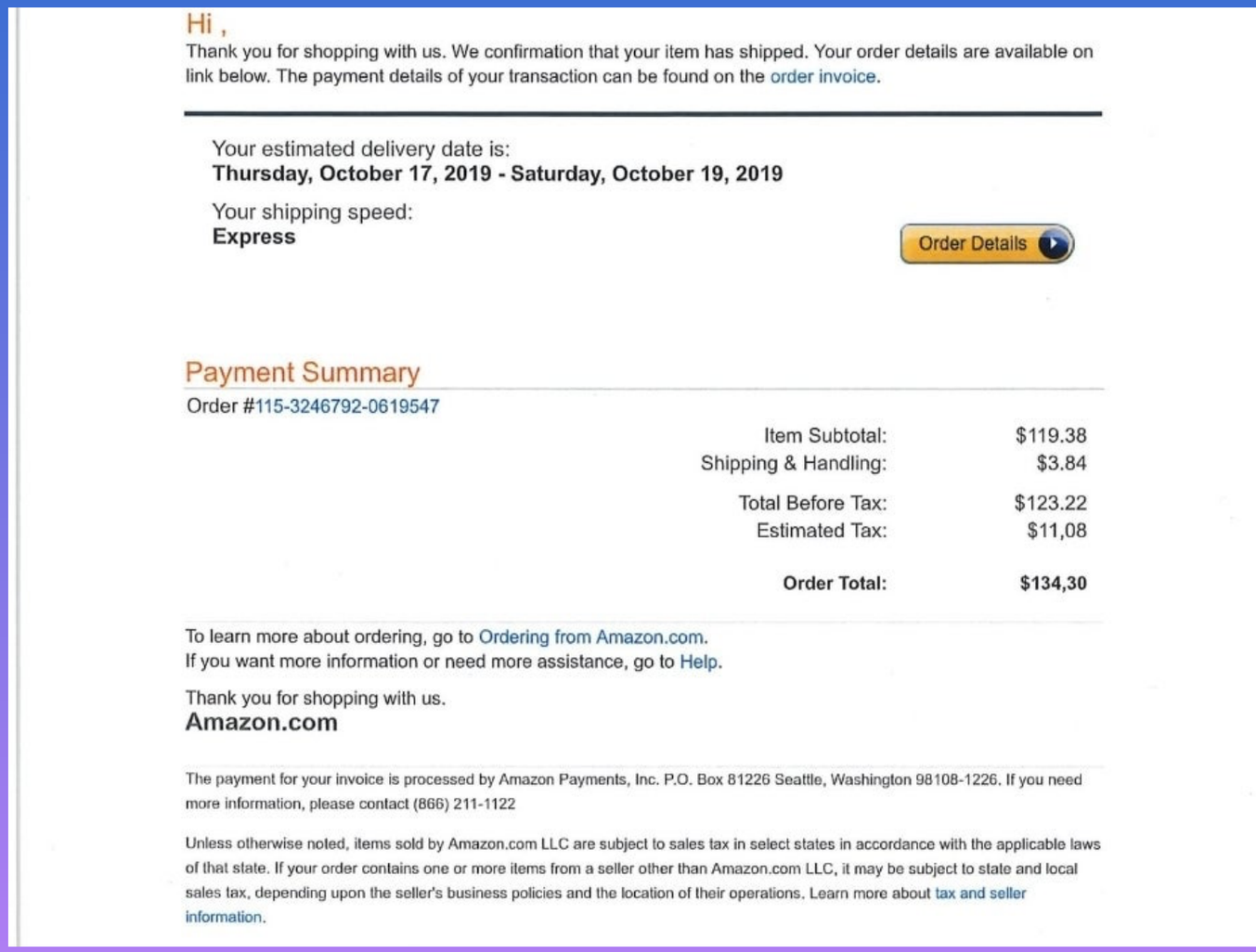
- The email asks you to click a fraudulent link, where you will be asked to enter personal information.

  - Your social security number, address, and banking information could be stolen



Phishing — Amazon Order Confirmation

- These scams are often claiming that you recently made a large purchase on amazon.com and attempt to trick you into believing this is a receipt
- These scams are hoping to confuse and fluster the victim!
  - The goal is for you to <u>click on a fraudulent link</u> that asks you to "*log in*" to your Amazon account, thus giving the scammers your account information.



Hi ,
Thank you for shopping with us. We confirmation that your item has shipped. Your order details are available on link below. The payment details of your transaction can be found on the order invoice.

Your estimated delivery date is:
Thursday, October 17, 2019 - Saturday, October 19, 2019

Your shipping speed:
Express

Order Details

Payment Summary

Order #115-3246792-0619547

Item Subtotal:	$119.38
Shipping & Handling:	$3.84
Total Before Tax:	$123.22
Estimated Tax:	$11,08
Order Total:	**$134,30**

To learn more about ordering, go to Ordering from Amazon.com.
If you want more information or need more assistance, go to Help.

Thank you for shopping with us.
Amazon.com

The payment for your invoice is processed by Amazon Payments, Inc. P.O. Box 81226 Seattle, Washington 98108-1226. If you need more information, please contact (866) 211-1122

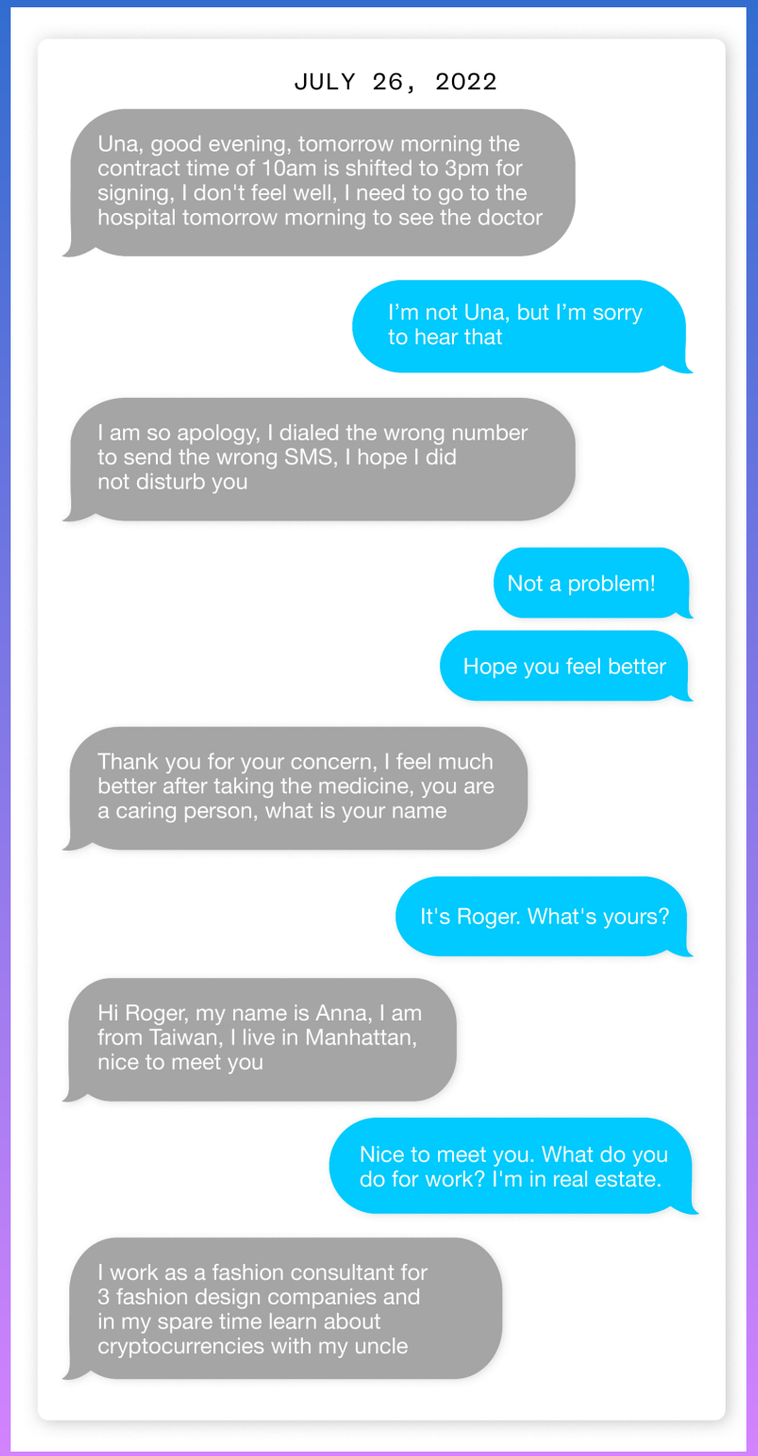
Unless otherwise noted, items sold by Amazon.com LLC are subject to sales tax in select states in accordance with the applicable laws of that state. If your order contains one or more items from a seller other than Amazon.com LLC, it may be subject to state and local sales tax, depending upon the seller's business policies and the location of their operations. Learn more about tax and seller information.

Text Message Scams
Wrong Number

- **Wrong Number Text Scam** — occurs when you receive a text message that seems pretty important to someone, but it was sent to you by accident.

- A You may respond back that the message has been sent to the wrong number. The next thing you know, you're being drawn into a continuing text conversation that could cost you a lot of money.

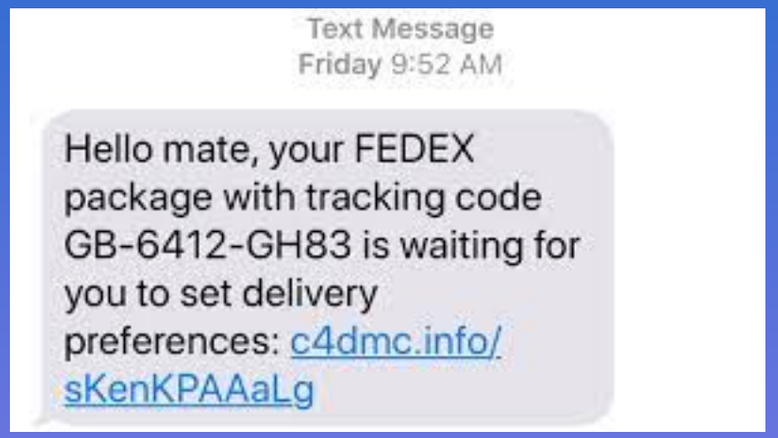
- The correspondence seems to start as an accident, scammers will try to establish relationships with the potential victims and eventually try to persuade them to give away their savings with the belief that they're investing in cryptocurrency.



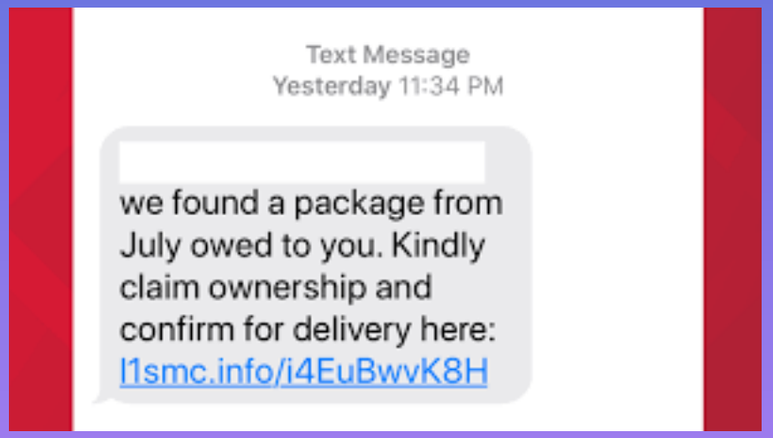
Text Message Scams
Package Delivery

- **Package Delivery Text Scam** — occurs when you receive an unsolicited text message that claims you have a package delivery waiting for you, but you need to click the link to have a successful delivery

- Scammers hope you may respond back to that the message, and enter in personal information on their fake websites

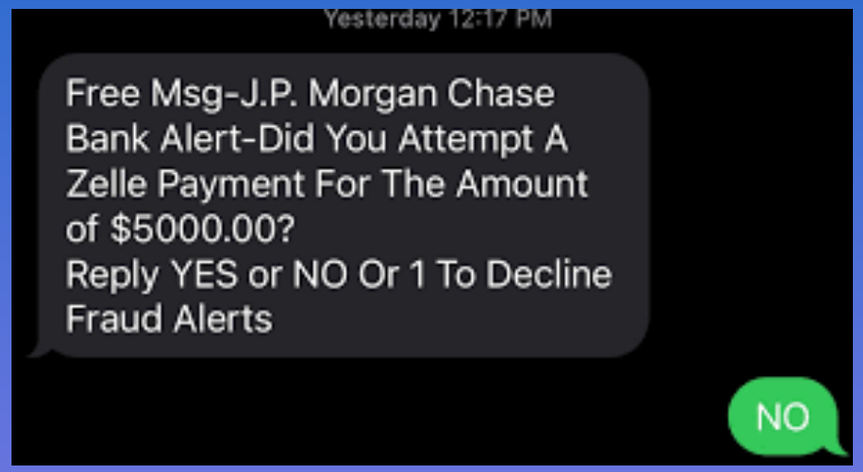


- Examples include:
  - Unexpected requests for money in return for delivery of a package, often with a sense of urgency.
  - Requests for personal and/or financial information.
  - Links to misspelled or slightly altered website addresses, such as "fedx.com" or "fed-ex.com
  - Certificate errors or lack of online security protocols for sensitive activities.



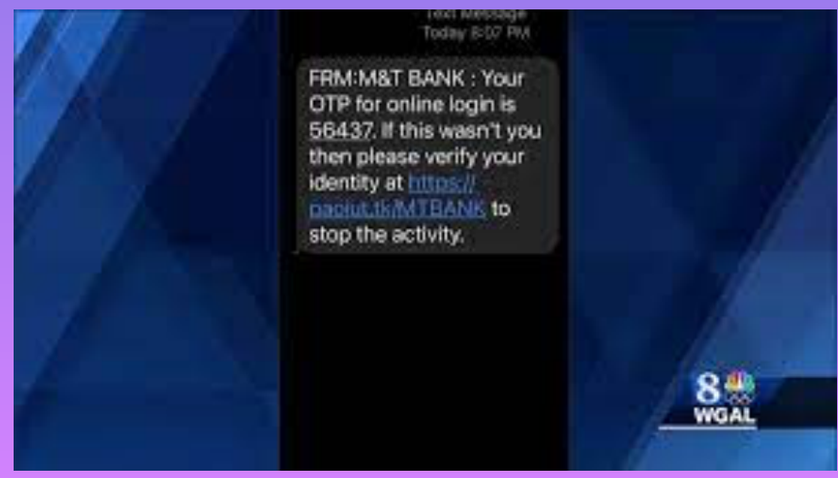
Text Message Scams
Bank Account/Debit Card

- **<u>Bank Account Text Scam</u>** — occurs when you receive an unsolicited text message that claims you have have recent activity on your bank account or debit card that you need to confirm.



- The claimed activity is designed to induce a fear response, prompting you to click the link and enter in private information such as bank passwords or pin numbers

- If you receive this type of text message delete it, and do not respond! Call your bank from a separate number (not the link) to verify if this is true or a scam.



‘Favor for a Friend’ Gift Cards

- You receive an email from a friend asking for a quick favor. She’s having trouble with a credit card or store account and, annoyingly, can’t buy a gift card she needs for a birthday present. Will you buy the card and call her with the numbers on the back?

- .She’ll pay you back. But this favor’s really a fraud, as it’s almost always an impostor sending the request, the Better Business Bureau (BBB) warns. If you do as told, you’ll never see the money again because gift cards don’t have the protections that debit and credit cards have.

- Call or text your friend to confirm the person really needs the favor. Target, Google Play, Apple, eBay and Walmart were the top cards used by scammers in 2021. “Always double check before sending someone money,”.

Catfishing—
Senior Dating Scam

- "**Catfishing**"— a term used to describe the practice of setting up fake online-dating profiles to scam unsuspecting victims

- These individuals only interact with you through messages, email or by telephone; never in person or face-to-face (*an excuse always comes up*)

- They also often ask for 'help' in the form of financial payments, care-taking or other types of gifts

Malware Scam

- This occurs when someone sends you an email containing malware.

- The email will most likely ask you to download something or the malware may even download automatically when you open the email.

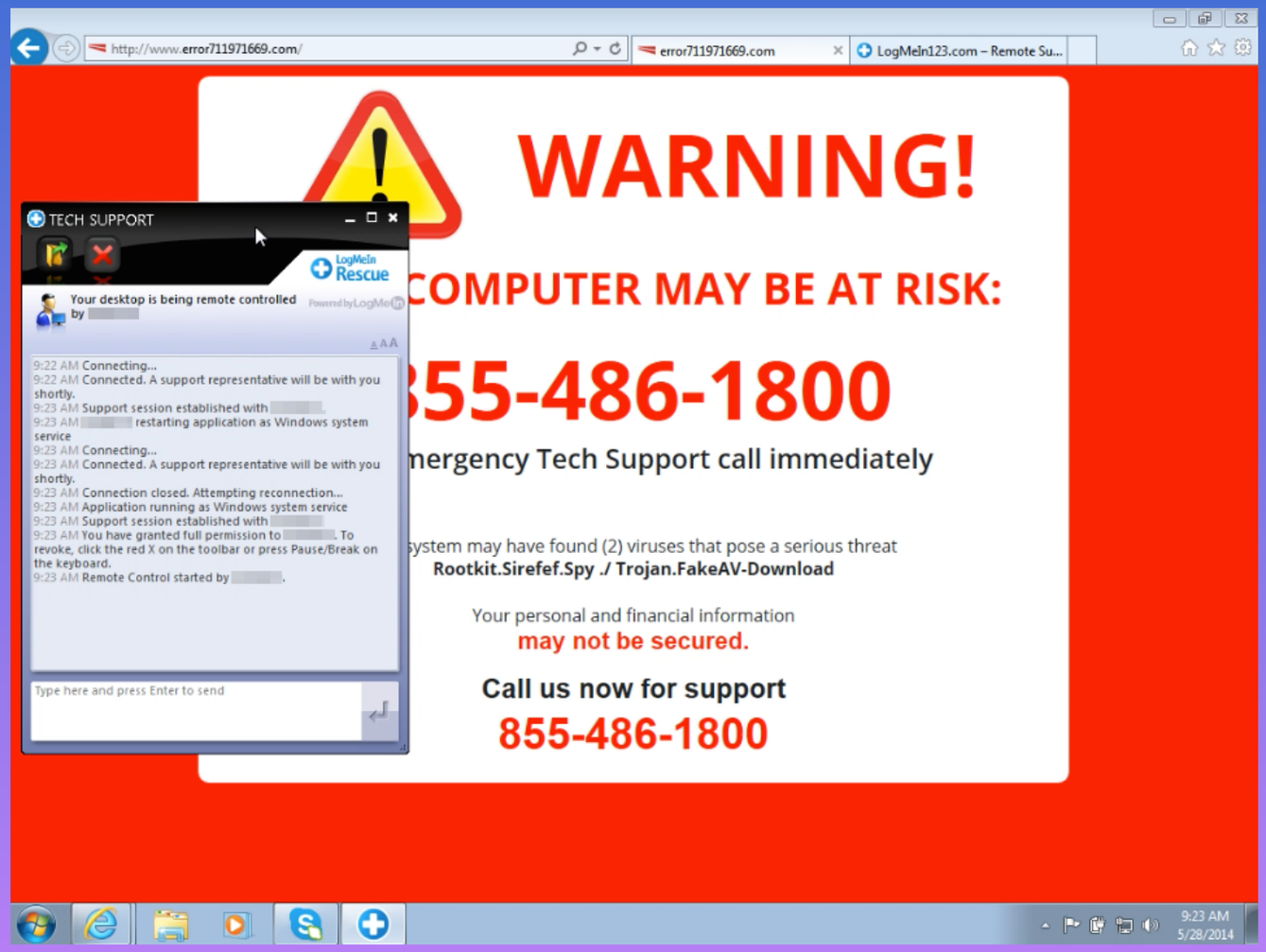
- The download may cause damage to your computer or device, allowing hackers to search through your computer to find personal information such as: tax files, financial accounts and more.

Computer Support Scam

- **Computer Support Scam** —this occurs when you get on the phone with a person who introduces themselves to you as tech support, promising to assist you in wiping your computer of any viruses, only to gain your trust so that they may infiltrate the computer.

- Through installing malware on your device, scammers gain access to personal files and possibly banking information.

- Some scammers even lock victims out of their computers, demanding payment in order for you to regain access.



Inside an International Tech-Support Scam

- Security camera footage from inside a fraud factory office

- https://www.aarp.org/money/scams-fraud/info-2021/international-tech-support-scam-exposed.html

Other Examples of Fear or Threat

- Con artists re known to exploit public fear by using it to hook victims. Examples include messages such as:

- “You will lose all your data and photos, and only our software can help fix it.”

- “Pay your electricity bill now, otherwise you will lose power.”

- “This is a warning from the local tax authority. Complete this action now or face a fine or court action.”

- “Your Netflix service will terminate unless action is taken.”

How Seniors can AVOID Getting Scammed

- Learn how to identify scams
- If you come across a deal that seems too good to be true, it probably is! Do more research on the company offering the deal before making any decisions.
- If someone is trying to sell you something or requests personal information from you, ask them to verify their job role/title and the company they represent. ***Walk away if they refuse***
- Consult with trusted family members and caregivers about potential purchases.
- Avoid answering email ads & messages from unfamiliar sources
- Be advised, the government will not notify you of an owed-payment or urgent matter over an ad on a website and will not request personal information from you in an email

How Seniors can AVOID Getting Scammed — *for Caregivers & Loved ones*

- **Keep loved ones informed on all the ways they could fall victim to an Internet scam**
- **Check-in on your loved one's financial accounts often, observing for odd purchases or withdrawals**
- **Visit them to discuss their monthly bills and prescriptions**
- **If a loved one mentions a deal they're interested in, ask for more information about the details of the deal; check to see if it's valid**
- **Make sure your loved ones know not to shop impulsively on the Internet**

How to Report a Scam

- **Federal Bureau of Investigations (FBI)**
    - The FBI deals with blue and white collar crimes, so they will address crimes like ‘scams over the internet’, especially if money is involved.
- **Federal Trade Commission (FTC)**
    - Deals with telemarketing and phishing cams
- **Securities and Exchange Commission (SEC)**
    - If you’ve ‘invested’ in an opportunity that you later feel might be a scam, report it to the SEC.
- **Social Security Administration**
    - Great for assisting with scams which involve your social security number or social security funds
- **Better Business Bureau**
    - If you feel a business is scamming you online, report it here.
- **Your Bank/Retirement Facility**
    - Scams with senior adults often involve money coming from their bank or retirement accounts. As soon as you find out or realize that you’ve been scammed, you should notify whoever deals with your money. There may still be a chance to get your money back or it may not have even left your account yet!
- Not sure where exactly to report a scam? Contact your local officials. You can even file a police report if you are scammed to help ensure there’s evidence and a timeline of the scam.
    - However, do not report this to 9-1-1. Instead, call your local police department’s non-emergency number.

Get in touch with us!

www.ajmtechsolutions.com

Phone: 267-240-7688

Email: ajmayers@ajmtechsolutions.com

Thank you for attending!

AJM

TECHNOLOGY SOLUTIONS & TRAINING

Presented by Andrew J. Mayers