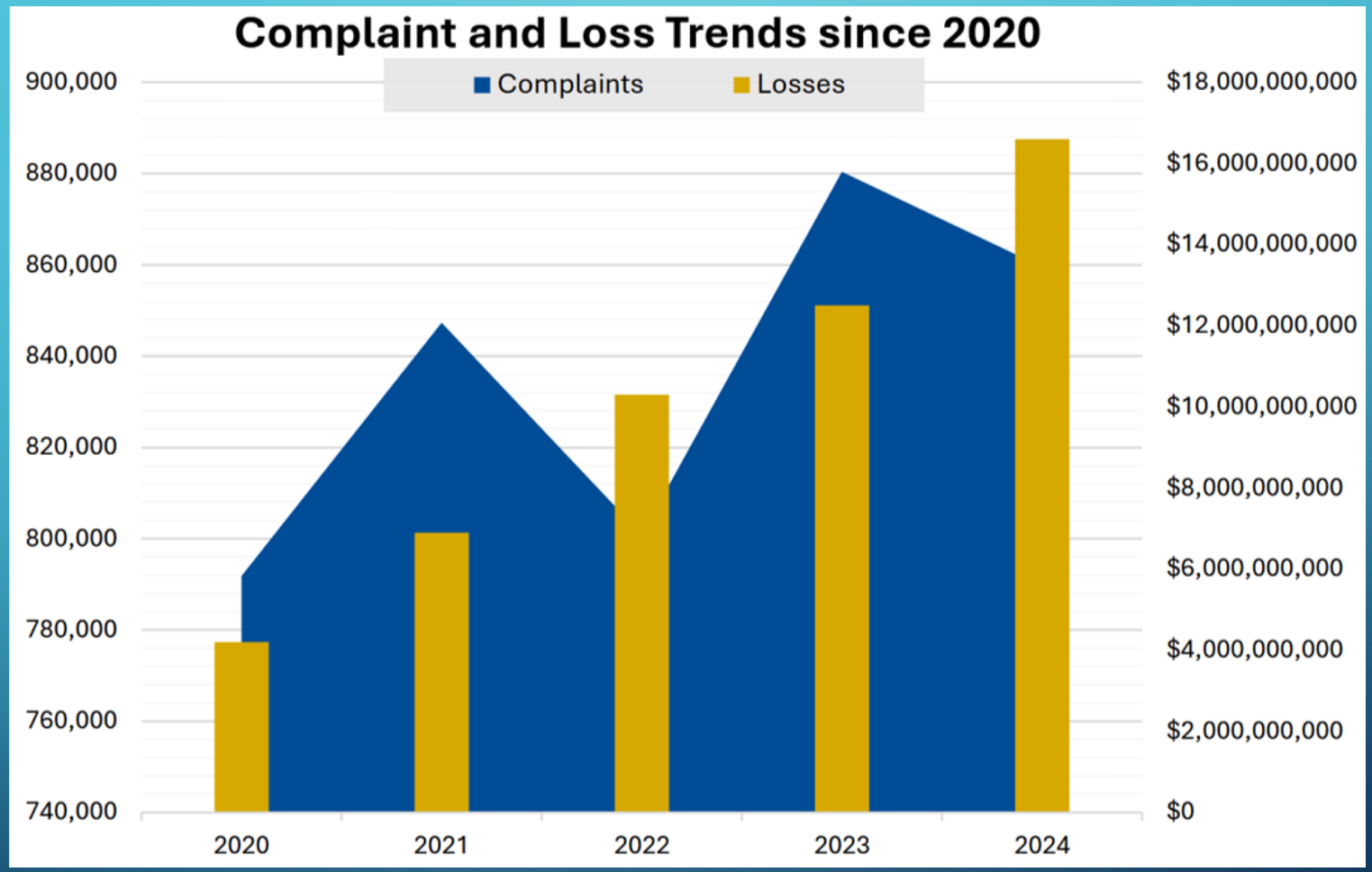
Recognizing and Avoiding Scams

A primer with practical tips

Scammers and thieves are looking to unlock and empty your cash vault!

Why Worry About This Stuff?

Colorado was 7th in complaints per 100K citizens at 249.2/100K



Colorado was 12th in losses per 100K citizens at $4,087,582

In 2024, Colorado ranked 17th for complaints at 14,848 and 17th for losses at $243,517,403 ($16,400/complaint)

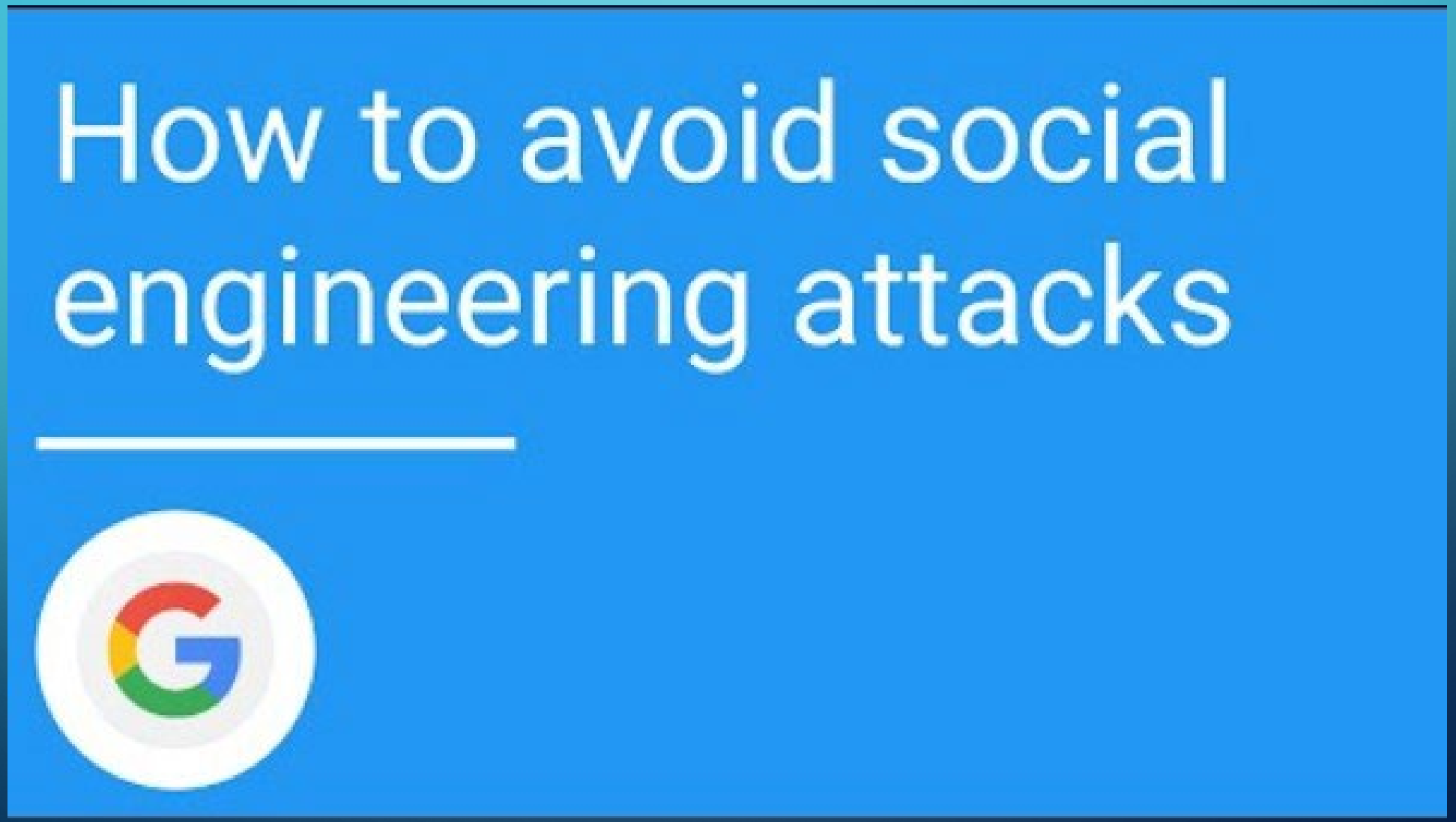
Why Worry About This Stuff?

The full 47-page report is available online…just search, “2024 IC3 report”

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	Harassment/Stalking	11,672
Extortion	86,415	Real Estate	9,359
Personal Data Breach	64,882	Advanced Fee	7,097
Non-Payment/ Non-Delivery	49,572	Crimes Against Children	4,472
Investment	47,919	Lottery/Sweepstakes/ Inheritance	3,690
Tech Support	36,002	Data Breach	3,204
Business Email Compromise	21,442	Ransomware	3,156
Identity Theft	21,403	Overpayment	2,705
Employment	20,044	IPR*/Copyright and Counterfeit	1,583
Confidence/Romance	17,910	Threats of Violence	1,360
Government Impersonation	17,367	SIM Swap	982
Credit Card/Check Fraud	12,876	Botnet	587
Other	12,318	Malware	441
*Descriptor***			
Cryptocurrency	149,686		

The 2024 IC3 report defines these crimes in an appendix

How to Avoid Social Engineering Attacks

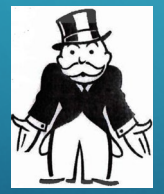


Tips on How to Avoid a Scam

The four typical signs of a scam:

1. **Scammers PRETEND to be from an organization you know**
2. **Scammers say there's a PROBLEM or a PRIZE**
3. **Scammers PRESSURE you to act immediately**
4. **Scammers tell you to PAY in a specific way (*e.g.*, cryptocurrencies such as Bitcoin)**

Other potential signs of a scam:



1. **Encouraging you to move conversations from email or phone to messaging apps like WhatsApp or Signal**
2. **Overly flattering messages or ones that share sympathetic stories about a sick child or a similar tragedy**
3. **Refusing to join live video conferences or meet offline – you should never meet an unknown person in real life**
4. **Popups and/or requesting remote operation of a device**

Tips on How to Avoid a Scam

Avoid becoming a victim of a scam by:

1. **Block unwanted calls and text messages**
2. **Don’t give your personal or financial information in response to a request that you didn’t expect – or more safely – ever**

3. **Resist the pressure to act immediately**

4. **Know how scammers tell you to pay**
5. **Assume strangers are NOT telling the truth about their identity**
6. **Instead of "trust and verify," use "don't trust and also verify."**
7. **Never purchase crypto assets from someone you've only met online**
8. **Never download files or click on links sent to you by strangers and unknown numbers…also be suspicious of QR codes**
9. **Stop and talk to someone you trust – urgency is by design**

Three Tips for Spotting Malware

Start With The Equipment You Use

Always secure your device(s) – biometric or passcode

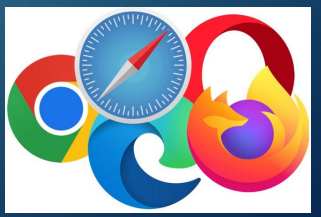
- **Make sure all of the security features are enabled.**
- **This includes your phone, tablet, computer, and router**
- **Keep the operating system, firmware, and user software up-to-date**

Always use and keep your antivirus software up-to-date

- **Free antivirus such as Windows Defender and those offered by your ISP are fine**
- **Don't use freeware or shareware offered via a website**

Adjust your browser – privacy review in settings

- **Enable private browsing and don't track or sell data**
- **Enable clearing of the of all site data, cookies, history, etc.**
- **Don't store any passwords**
- **Block cross-site cookies, cryptominers, fingerprinting, popups, and installing add-ons; and possibly page caching (limitations)**
- **Disable popups…if you see a popup chances are it is malware**



Passwords, Managers, 2FA, and Passkeys

Passwords, Managers, 2FA, and Passkeys

Passwords ≤ password managers < two factor authentication < passkeys

Never store your passwords in your browser or an open document on your electronic device

Never reuse passwords

Don't use guessable passwords

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters and Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	1 Second
9	Instantly	Instantly	4 Seconds	21 Seconds	1 Minute
10	Instantly	Instantly	4 Minutes	22 Minutes	1 Hour
11	Instantly	6 Seconds	3 Hours	22 Hours	4 Days
12	Instantly	2 Minutes	7 Days	2 Months	8 Months
13	Instantly	1 Hour	1 year	10 Years	47 Years
14	Instantly	1 Day	52 years	608 Years	3K Years
15	2 Seconds	4 Weeks	2K Years	37K Years	232K Years
16	15 Seconds	2 Years	140K Years	2M Years	16M Years
17	3 Minutes	56 Years	7M Years	144M Years	1Bn Years
18	26 Minutes	1K Years	378M Years	8Bn Years	79Bn Years

Don't base passwords on personal information

Random vs passphrase or unrelated words

Use strong passwords…table based on ChatGPT enabled cracking

Passwords, Managers, 2FA, and Passkeys

Password managers generate strong passwords and store them in an encrypted form, generally in the cloud…only have to recall one password

Bitwarden is an open-source free or paid password manager

1Password is a paid password manager with Travel Mode which temporarily removes sensitive vault items while in a new location

Apple and Google have free password managers

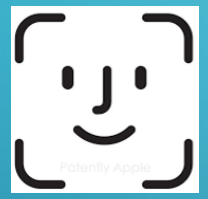
Two-factor authentication should always be used when possible

- **Text to your phone (okay)**
- **Use an authenticator app (better) such as the Google or Microsoft Authenticator (does passkeys too)**

Passwords, Managers, 2FA, and Passkeys

Passkeys are here now and will be the way of the future

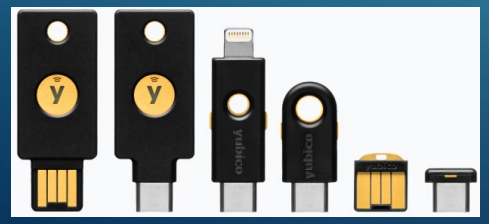
Passkeys are cryptographic credentials tied to a user's account on a website or application…no need to enter usernames or passwords



Passkeys allow a user to approve a login via the same process they unlock their device…biometrics, PIN, or pattern

Need to register a passkey online for each service or app…some websites require an existing authentication method (*e.g.*, password and 2FA)

The passkey is stored in the user's password manager (default is the operating system manager), or a physical security key (hardware device)



If using a physical security key purchase two and register both of them…place one in a safe location as a backup to a lost primary key

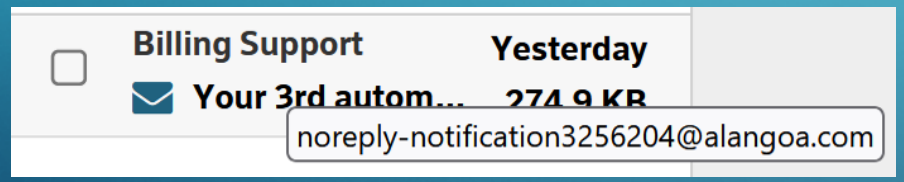
Email…The Modern Postal Scam?

You absolutely should have multiple email accounts…at a minimum create one just for billing purposes, one for social media, and one for other (junk) purposes

Secure each account with strong, unique passwords and 2FA, or a passkey

Review all security and privacy settings for the email provider

Some services and password managers allow email alias and forwarding options



Always hover over an email to verify the sender…some look legitime, but if in doubt send to the spam folder and delete

To unsubscribe or not…if you know it's an email you signed up for (*e.g.*, Kohl's, etc.) then its likely okay, otherwise send to junk or block

Email…The Modern Postal Scam?

Never click on a link in an email…go to the actual website

Bookmark your frequently used websites and financial websites, and verify both the bookmark and secured status

AI makes it possible to create very real and misleading emails, texts, etc.

Do not reply, open, or download any item from a suspect email

The spammer will likely know the email was delivered, but if it goes straight to junk email and is deleted, they will likely think it is an abandoned email address

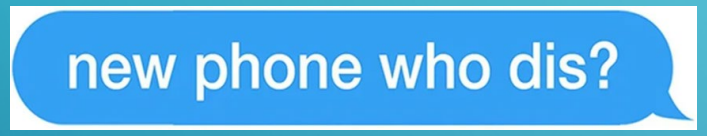
Remember, a bad actor wants you to respond quickly (urgently) to override caution

Universal tip: Pay for items on websites you don't normally use, or via social media using a tokenized pay method (*e.g.*, PayPal)

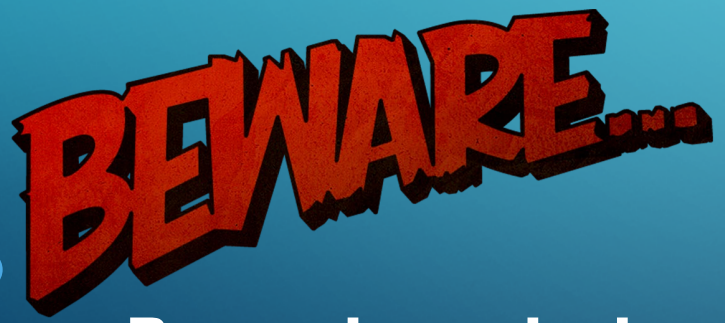
Text Messages…Email by Another Name?

Treat text messages just as you would your email

Don’t open unknown or suspect texts, open or download attachments, or follow links in the text



This includes the old “new phone who dis?”, tolls, fines, can’t deliver package, etc.

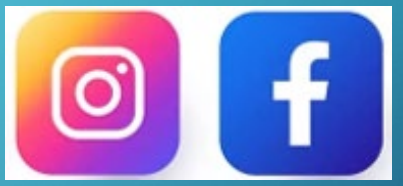


You can also block the phone number, but it’s easier and safer to just report as junk and delete

Remember, a bad actor wants you to respond quickly (urgently) to override caution

Social Media – Open-Source Wonderland

Change the settings on each social media site to limit your information from being used – online guides and guided walkthroughs on the site for privacy and security settings

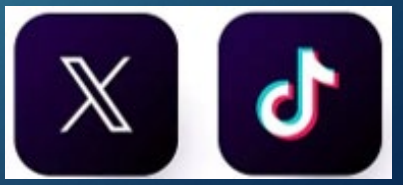


Regardless you will be tracked (*e.g.*, Facebook pixel)

Don't post sensitive information such as birthdate, birthplace, location, photos of your home and valuables, etc.

Even when you limit information via private only posts, that does not mean other "friends" will do the same

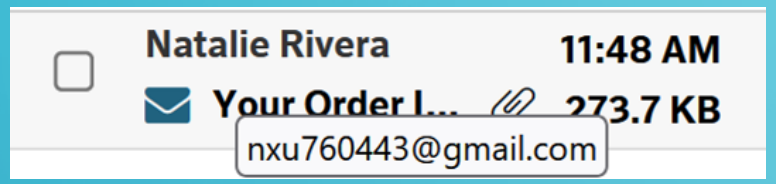
Good old OSINT work, or the use of AI makes it possible to find out who you know and what you are doing via friends and through multiple social media sites you use

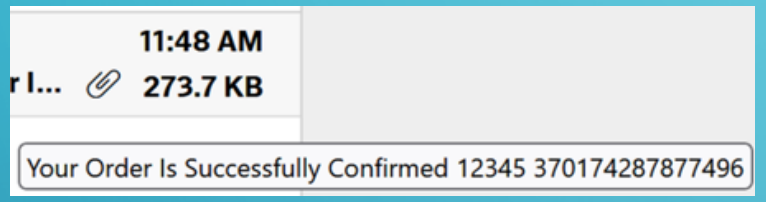


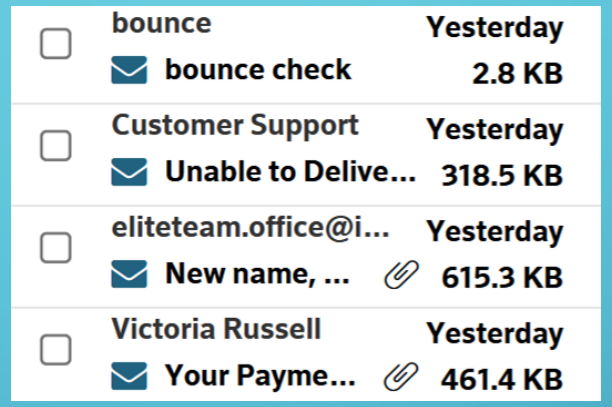
AI makes it possible to create very real and misleading calls using your loved one's voice from TikTok and other media sites

Let's Review

Email...open or junk?





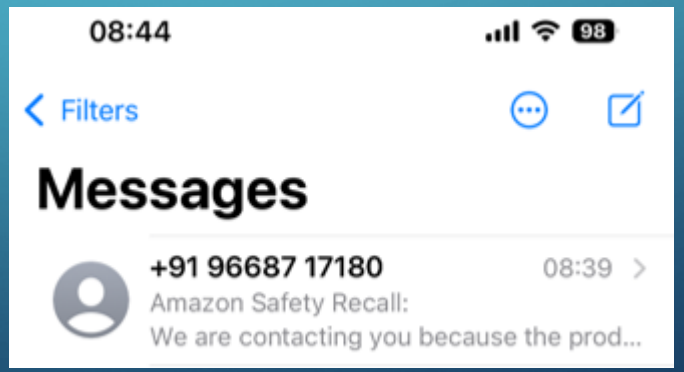


Pop-up request ...

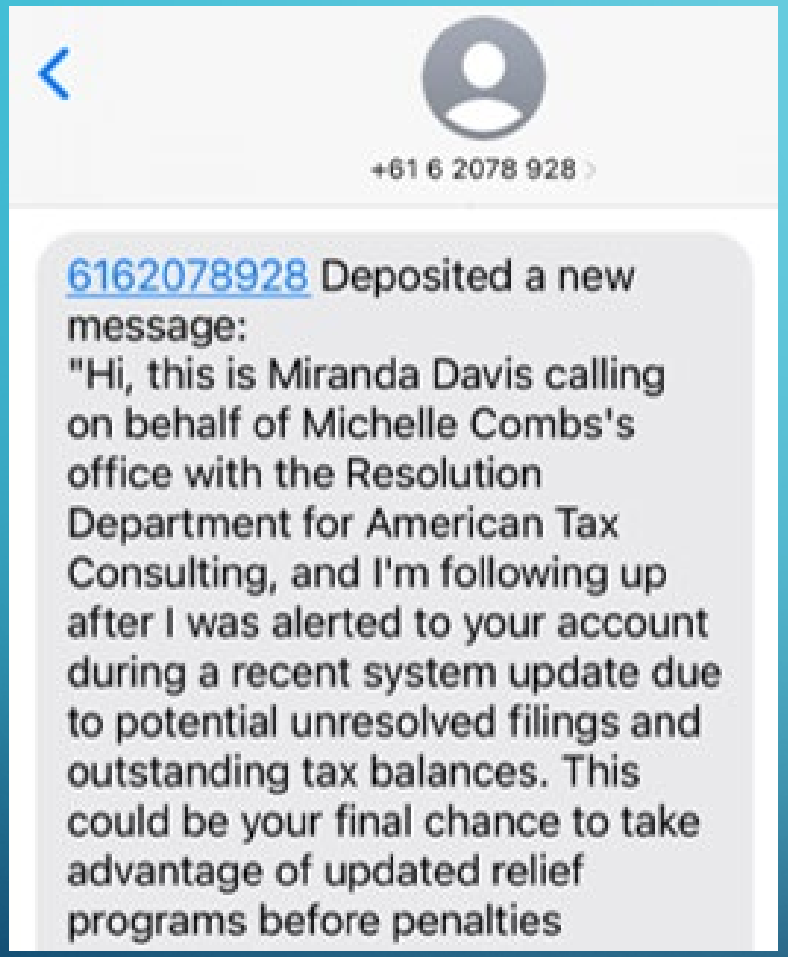
+ R

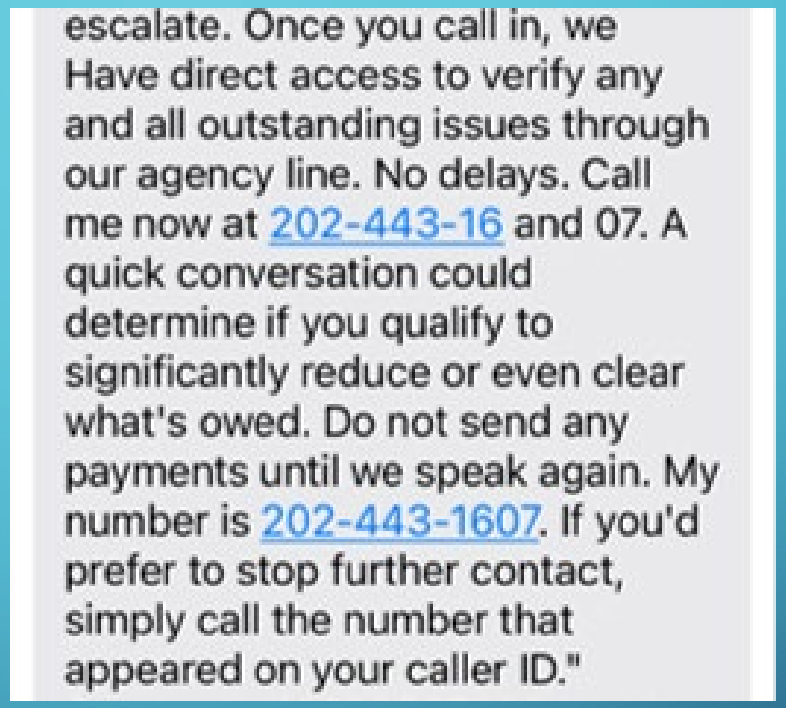
with a cut-paste request

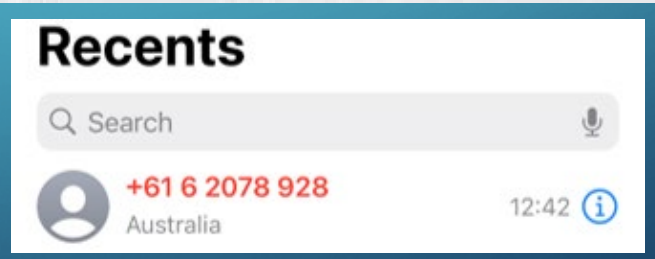
Text...open or delete and report as junk?



Let's Review







616 is Grand Rapids, MI…a spoofed phone number…the 202 number?
The "NZ company" has a barebones website circa 2021
The 616 number was allegedly linked to a fake fundraiser in 2021

Other Critical Topics – FTC Website

Online Security

Are Public Wi-Fi Networks Safe? What You Need To Know

Here's what you need to know about your safety when you connect to a public Wi-Fi network.

How To Protect Your Phone From Hackers

Four steps to protect your phone from hackers.

How To Recover Your Hacked Email or Social Media Account

What to do if you think your email or social networking account has been hacked.

How To Remove Your Personal Information Before You Get Rid of Your Computer

How to remove your personal information from your computer so it doesn't end up in the hands of an identity thief.

How To Remove Your Personal Information Before You Get Rid of Your Phone

Before you trade in, sell, give away, or recycle your phone, remove your personal information.

How To Secure Your Home Security Cameras

There are steps you can take to secure your home security camera. Read on to learn more.

How To Secure Your Home Wi-Fi Network

How to protect your home wireless network.

Malware: How To Protect Against, Detect, and Remove It

Learn how to protect yourself from malware.

Mobile Payment Apps: How To Avoid a Scam When You Use One

Learn how mobile payment apps work and how to avoid sending money to a scammer.

Questions and Additional Resources

AARP– https://www.aarp.org

FBI – https://www.fbi.gov/investigate/cyber

Federal Trade Commission – https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security

Homeland Security – https://www.cisa.gov/resources-tools/resources/cisa-cybersecurity-awareness-program-older-american-resources

And many other organizations (*e.g.*, Apple, Google, Microsoft, etc.)

You are always the first and last line of defense