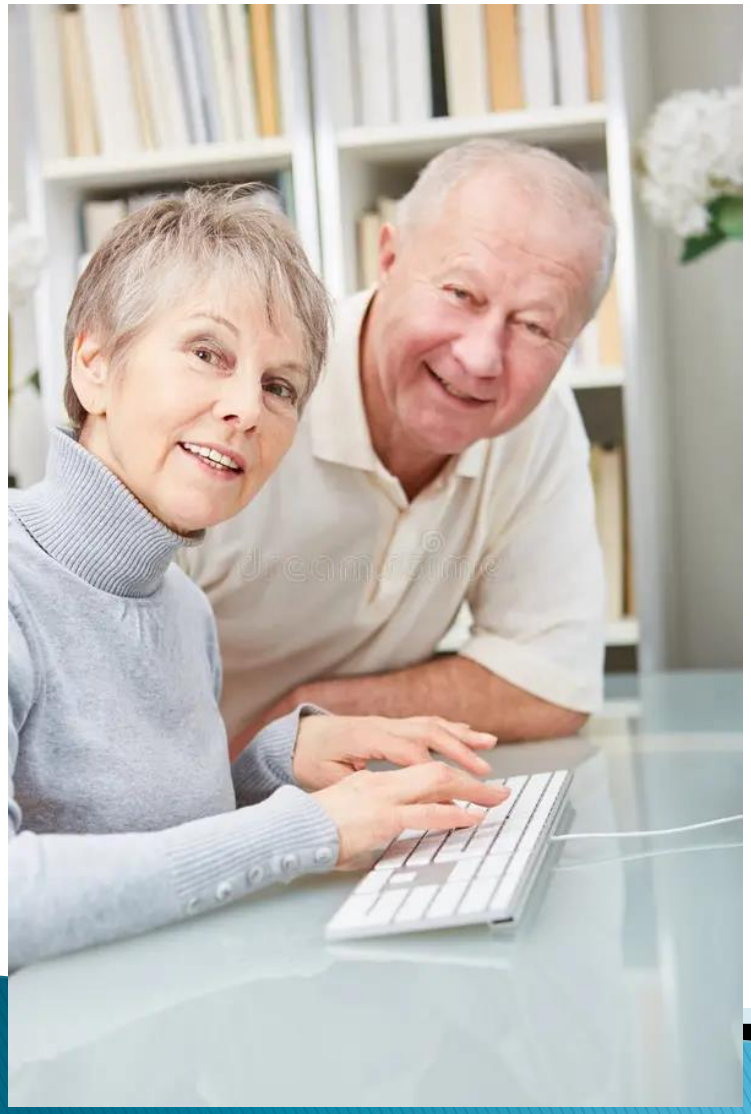


Using Your Computer Safely

Anne Matheus, Instructor
Time: 11:00 AM – 12:15 PM
Wednesdays, Sept. 4, 11,18 & 25

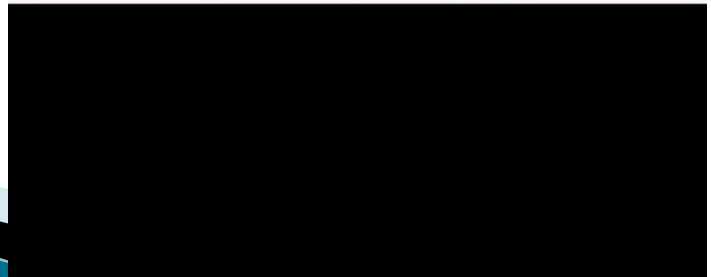
Basic Safety Tips

- Use strong, unique passwords.
  - Use a password manager
  - Long passwords
  - Never reuse passwords
  - Never use personal information
  - Store passwords securely
  - Use different password for different sites

- Keep your software up to date.
- Install antivirus software.

a scammer called my grandma and said he had all her passwords

she got a pen and paper and said 'thank god for that, what are they' 😂



Example of Password File

Allegiant	anne.matheus@marist.edu	$jEc#S8HE&2M4XR		
Adams	annebmatheus@gmail.com	g4reYisewb2!t		
Amazon	anne.matheus	RE+&D-*t7V_^F		
American Airlines	DC393N4	miG9R%32		
AppleID	Henry	In2rmAID	Teddy	
BestBuy	anne.matheus@marist.edu	nfrKif%76		
Best Western	henrymatheus@gmail.com	BEpwfEM70#		
Botti at Sea	abmatheus	3Af8VzWX7GFb		
Celebrity	annebmatheus@gmail.com	nkg6#4KH		
chatGPT	annebmatheus@gmail.com	9F4:!ijBKEPz		
Corporate Parking EWR	annebmatheus@gmail.com	s#8@EF4Kzf5D		
Disney+	annebmatheus@gmail.com	tg6#4KH65		
Dutchess Co Online	annebmatheus@gmail.com	nJ4C$@ejhZGA	7796	
ELAN	annebmatheus@gmail.com	QMjgyi7!kjSAc		

Antivirus Software

- **Norton**
  - Easily compare antivirus plans
  - 100% Virus Protection Promise
  - Password manager
- **TotalAV**
  - Ransomeware Protection
  - Phishing Scam Protection
- **Bitdefender**
  - All-in one plans
  - Unlimited VPN
- **McAfee**
  - Easily compare plans
  - Secure VPN Included
- **Surfshark**
  - Scan files while you download them
  - Enjoy robust webcam protection
  - Protection from Ransomware
  - e protected from the newest viruses
- **Aura**
  - Up to 250X Faster Fraud Alerts
  - $1M Identity Theft Insurance

https://www.forbes.com/advisor/1/best-antivirus-software/?utm_content=163246747678&utm_term=kwd-2138366346&utm_campaign=21298233013&utm_content=163246747678&utm_term=kwd-2138366346&utm_campaign=21298233013&gad_source=1&gclid=CjwKCAjwqre1BhAqEiwA7g9QhpAg06OAdYUYf3QDOveAusQFNwTjkWAkUADQqgIcPSvYkXUARqfXkBoCIv

What Security Threats Can Antivirus Protect Against?

- **Viruses:**
  - Viruses are the most common type of malware and can cause a lot of damage to your computer if they're not removed quickly. They can spread from one computer to another and are often used to steal personal information or destroy data.
- **Worms:**
  - Worms are similar to viruses but can spread without any user interaction. They're often used to create botnets, which are networks of infected computers that can be used to launch attacks or send spam.
- **Trojans:**
  - Trojans are malware that masquerade as legitimate programs to trick users into installing them. Once installed, they can allow attackers to take control of your computer and steal your personal information.
- **Ransomware:**
  - Ransomware is a type of malware that encrypts your files and holds them for ransom. The attackers will usually demand a payment to decrypt your files, but there's no guarantee they will actually do so even if you pay.

What Security Threats Can Antivirus Protect Against? (cont.)

- **Spyware:**
  - Spyware is malware that's used to collect your personal information, such as your passwords, credit card numbers and browsing history. It can also be used to track your movements and activities.
- **Adware:**
  - Adware is a type of malware that displays unwanted ads on your computer. It's often used to generate revenue for its creators but can also be used to collect your personal information.
- **Rootkits:**
  - Rootkits are a type of malware that's designed to hide itself from detection. They can be used to gain access to your computer and steal your personal information or launch attacks against other computers.
- **Keyloggers:**
  - Keyloggers are a type of malware that records everything you type on your keyboard. This can include sensitive information such as passwords and credit card numbers. They can also be used to track your activities and movements.

Recognizing Phishing Scams

- What is phishing?
  - **Phishing** is a type of cybercrime where attackers attempt to trick individuals into providing sensitive information, such as usernames, passwords, credit card numbers, or other personal details.

- How to recognize phishing emails.
  - **Suspicious Sender Address**
  - **Generic Greetings**
  - **Urgent or Threatening Language**
  - **Requests for Personal Information**
  - **Suspicious Links or Attachments**
  - **Poor Grammar and Spelling**
  - **Unusual Requests or Offers**
  - **Mismatch in Email Content**

Department of Treasury
Internal Revenue Service
Atlanta, GA 39901-0025

Your 2023 Form 1040 overpayment was applied to tax you owe.

Refund: $650.00

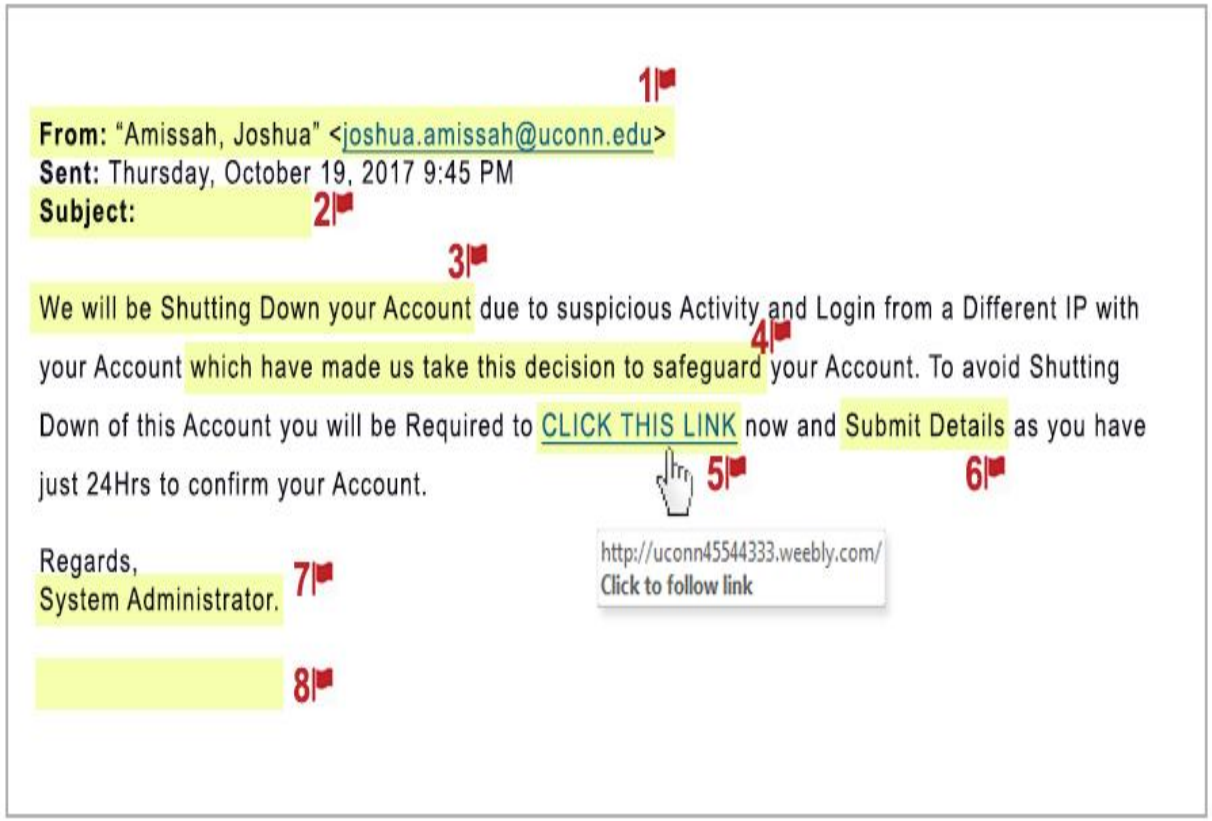
We applied for all or part of your $1000.00 overpayment from your 2023 tax return to the amount you owe for other tax years. As a result, you are due a refund of $650.00.

What you need to do	fill your document in this link
	Check Your Refund
Next steps	We'll send you a refund for $650.00 (the remainder of overpayment if you don't owe other tax or debts we're required to collect or elected to have it applied to your next year's estimated tax. You may receive another notice from us in the next few weeks.
Additional information	Keep this notice for your records. If you need assistance, please don't hesitate to contact us.

The IRS is Never going to send you an email!

NEVER CLICK ON A LINK!
Go to the website for the IRS website:
Irs.gov and create an account to research or by phone contact the IRS.

Below is a phishing message that targeted the UConn community.
It triggers many red flags that identify it as a phishing message.

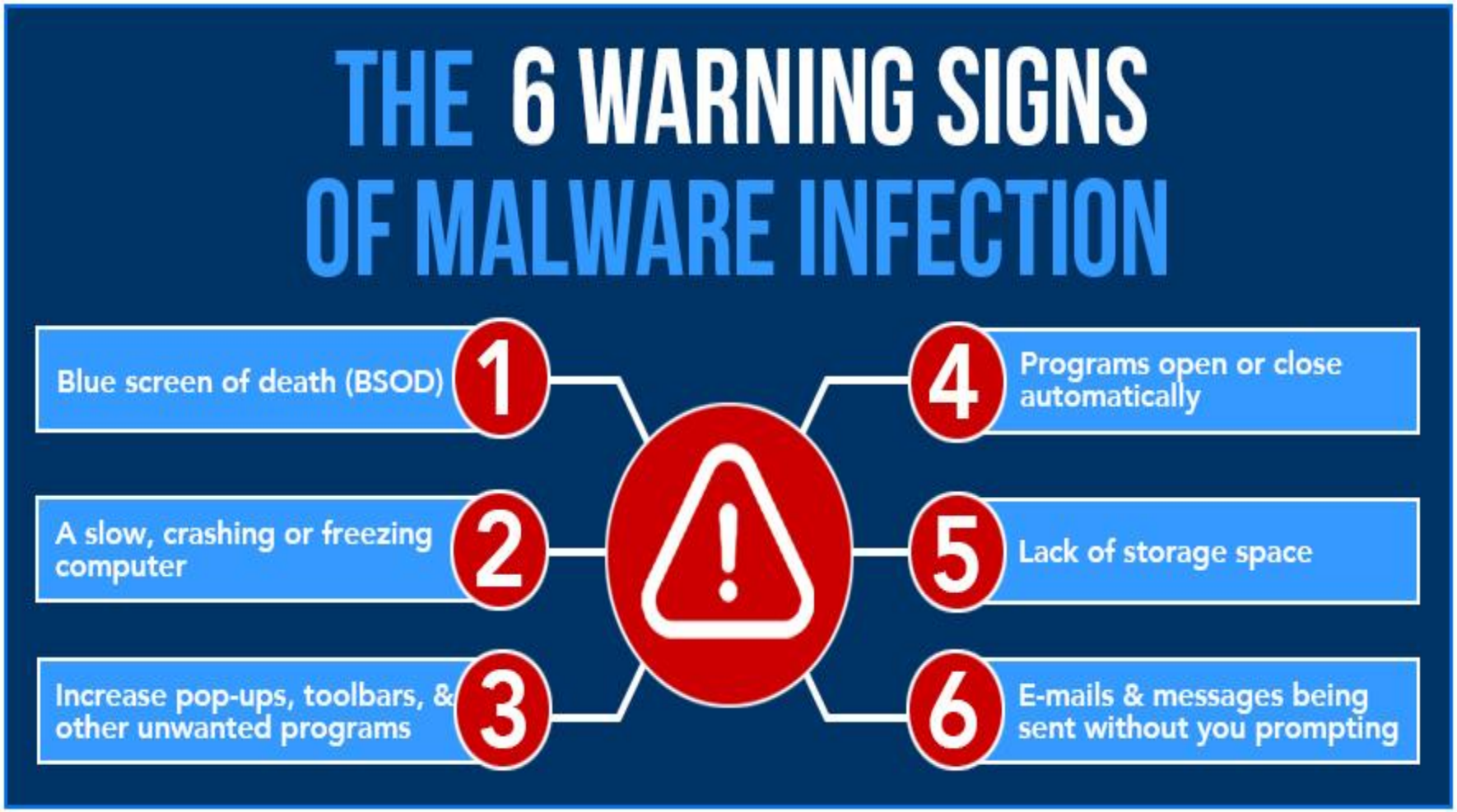


1. Even though this message comes from a UConn address, be wary. These can be easily spoofed or sent from a compromised account.
2. An official message from a University unit will have a subject.
3. The message uses urgent language to prompt a quick response.
4. This sentence is awkward and grammatically incorrect.
5. When you hover over this link, it displays a non-UConn address.
6. This message was an unsolicited request for personal information.
7. The signature line is generic. An official message would be signed by a person whose position and name you could verify.
8. There is no contact information. An official message would list UConn-specific contact information.

Avoiding Malware

- Social engineering is a manipulation technique used by cybercriminals to trick people into giving up confidential information or performing certain actions that may compromise security. Instead of hacking systems or using software vulnerabilities, attackers exploit human psychology to gain access to sensitive data such as passwords, bank details, or personal information.

- **Phishing**:
  - Sending emails or messages that appear to be from a legitimate source
- **Pretexting**:
  - Pretending to be a company representative or authority figure to gain trust.
- **Baiting**:
  - Luring victims with promises of something enticing to get them to click on malicious links or hand over personal details.
- **Tailgating**:
  - Physically following someone into a secure area
- **Impersonation**:
  - Pretending to be someone else


THE 6 WARNING SIGNS
OF MALWARE INFECTION
1
Blue screen of death (BSOD)
2
A slow, crashing or freezing computer
3
Increase pop-ups, toolbars, & other unwanted programs
4
Programs open or close automatically
5
Lack of storage space
6
E-mails & messages being sent without you prompting

If your site is delivering the red screen

If your browser says that your website doesn't exist

Your website has slowed to a crawl

Your website is redirected to a different website

You see random code - letters and numbers

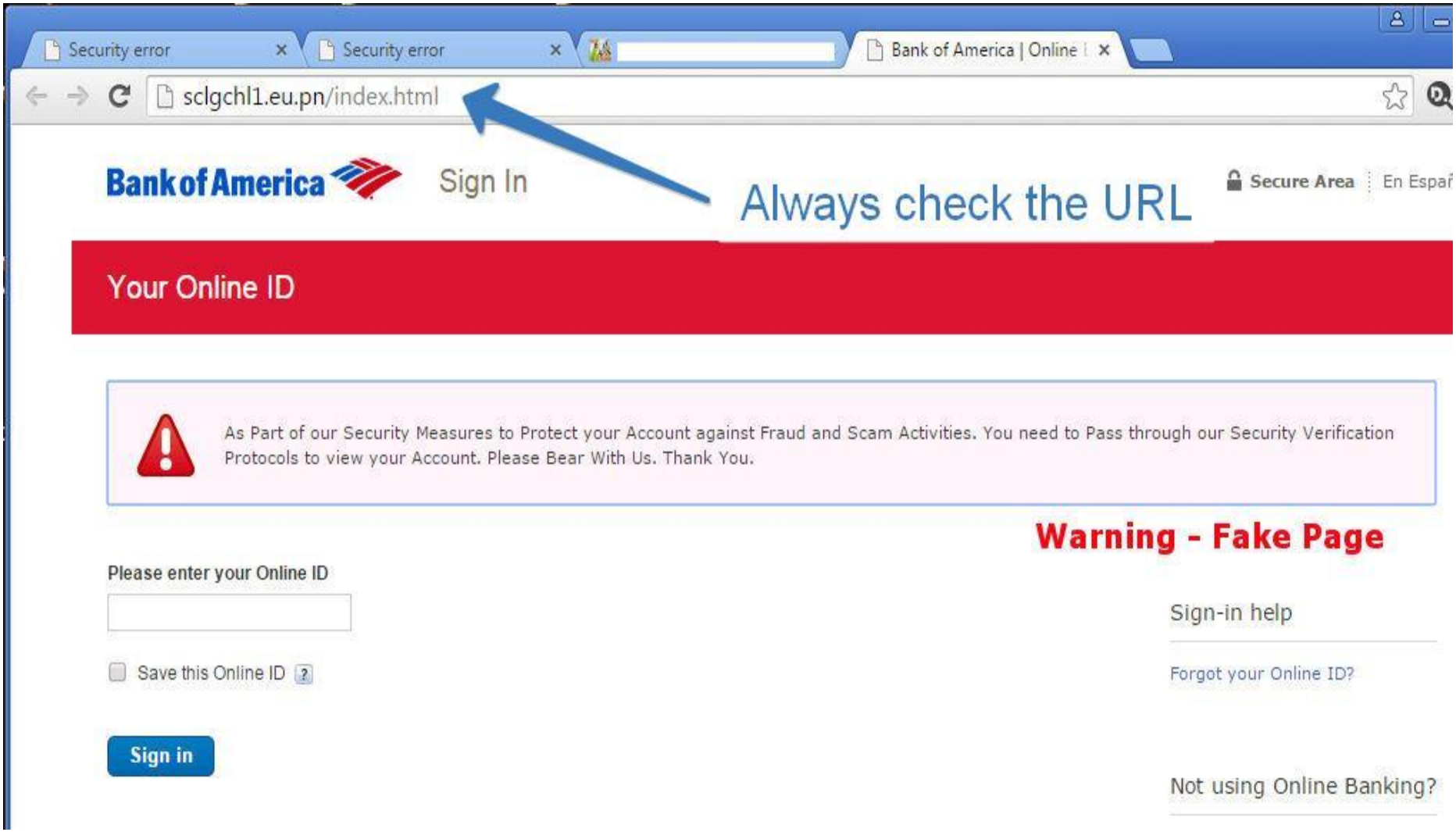
Your domain is marked as unsafe

How to Avoid Downloading Malware

- Download Software from Reputable Sources
- Be Wary of Email Attachments
- Keep Your Software Updated
- Use Antivirus and Anti-Malware Software
- Avoid Clicking on Pop-Ups and Ads
- Be Cautious with Free Software and Filesharing
- Backup Your Data Regularly

Safe Online Banking

- Use strong passwords and change them regularly.
- Avoid accessing accounts on public Wi-Fi.
- Check your accounts frequently for any suspicious activity.
- Look for HTTPS in the URL when banking online.


Security error
Security error
Bank of America | Online
sclgchl1.eu.pn/index.html
Bank of America
Sign In
Always check the URL
Secure Area
En Espa
Your Online ID
As Part of our Security Measures to Protect your Account against Fraud and Scam Activities. You need to Pass through our Security Verification Protocols to view your Account. Please Bear With Us. Thank You.
Warning - Fake Page
Please enter your Online ID
Save this Online ID
Sign in
Sign-in help
Forgot your Online ID?
Not using Online Banking?

What to Do If You're Scammed

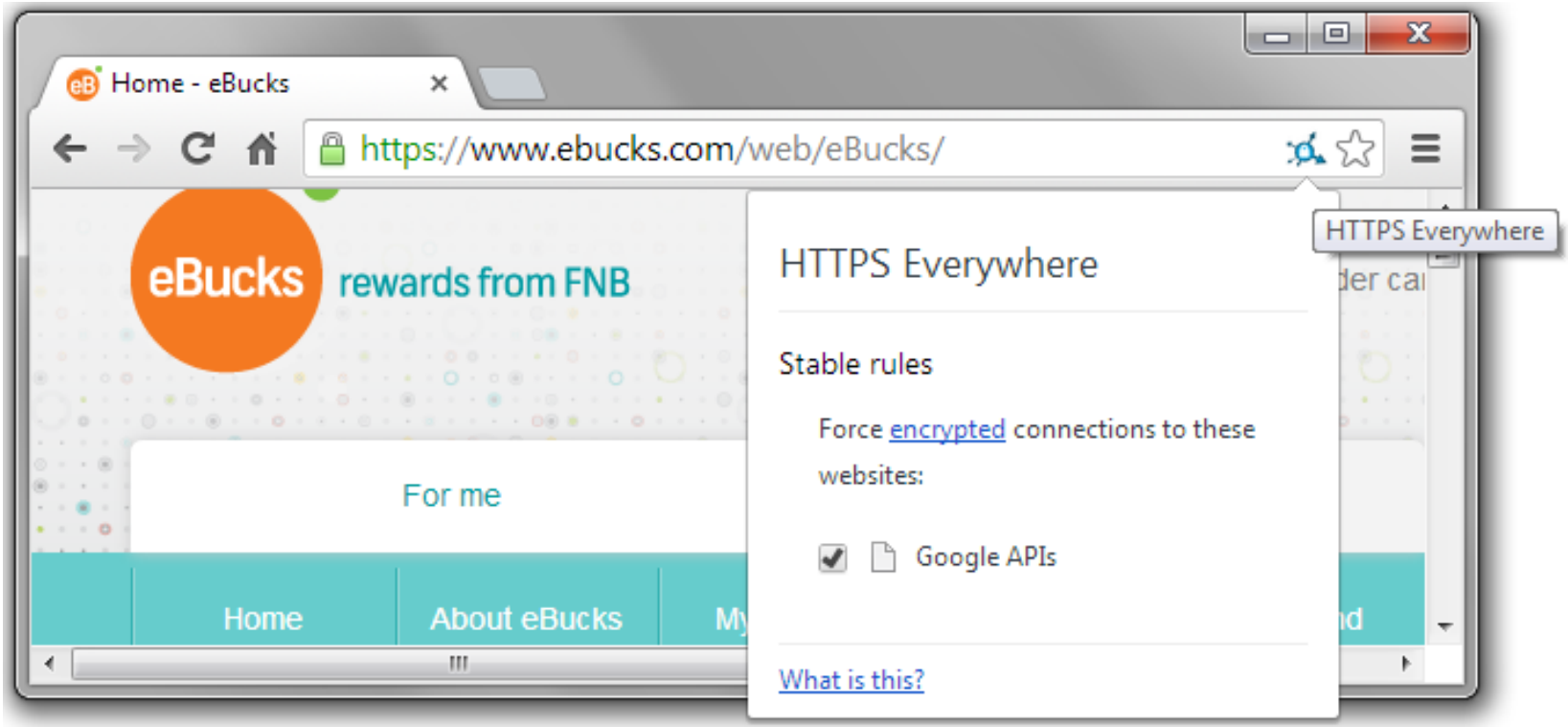
- Steps to take if you think you've been scammed.
- Reporting scams.
- Protecting your information.

- **Federal Trade Commission (FTC) Report:**
- **URL:** https://www.ftc.gov/
- **Fraud Reporting (Fraud.ftc.gov):**
- **URL:** https://reportfraud.ftc.gov/
- **National Elder Fraud Hotline:**
- **URL:** No URL provided, but the hotline number should be available on government websites related to elder care and fraud prevention.
- **Consumer Financial Protection Bureau (CFPB):**
- **URL:** https://www.consumerfinance.gov/
- **Internet Crime Complaint Center (IC3):**
- **URL:** https://www.ic3.gov/

Online Shopping Safety

- Use reputable websites.
- Look for HTTPS in the URL.
- Avoid deals that seem too good to be true.

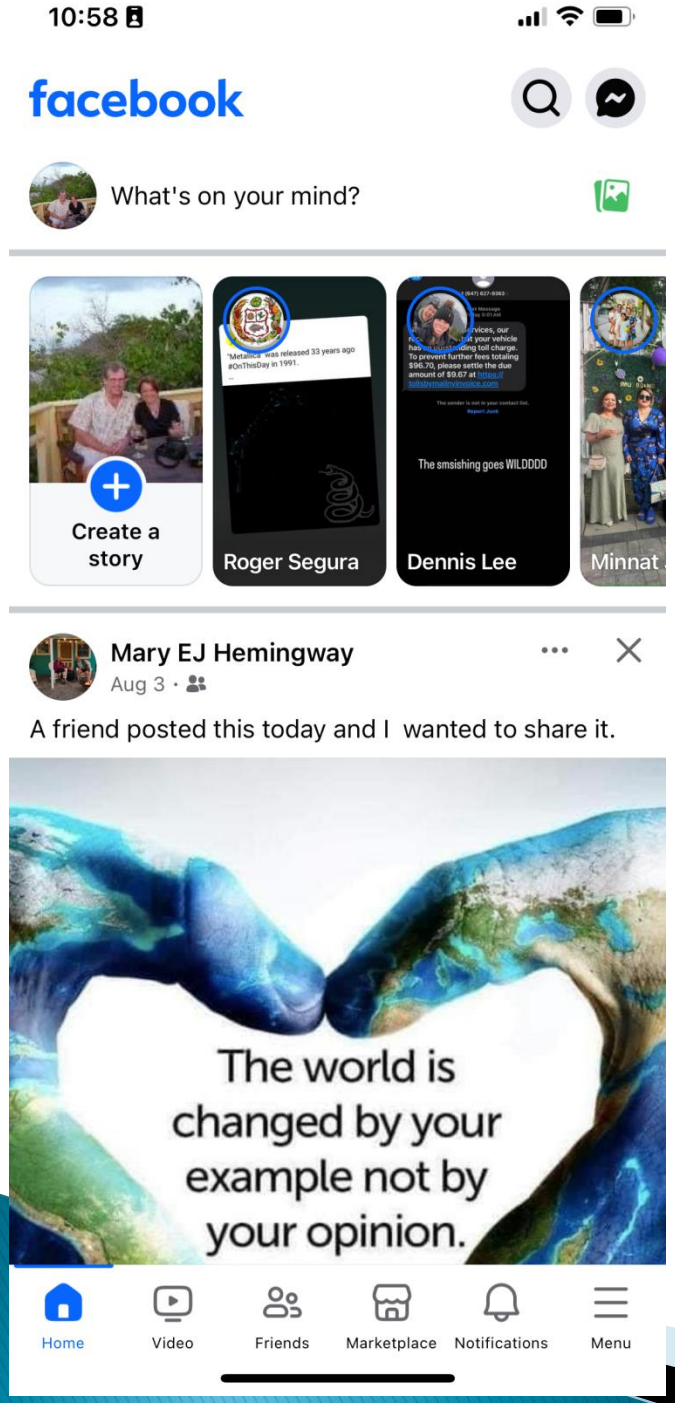
- You should see: “https://” at the beginning of the URL. The “s” at the end of the http means “secure.” A lock icon on the far left side of the address bar.
- Clicking on the Lock icon will give you detailed information on the security status of this website

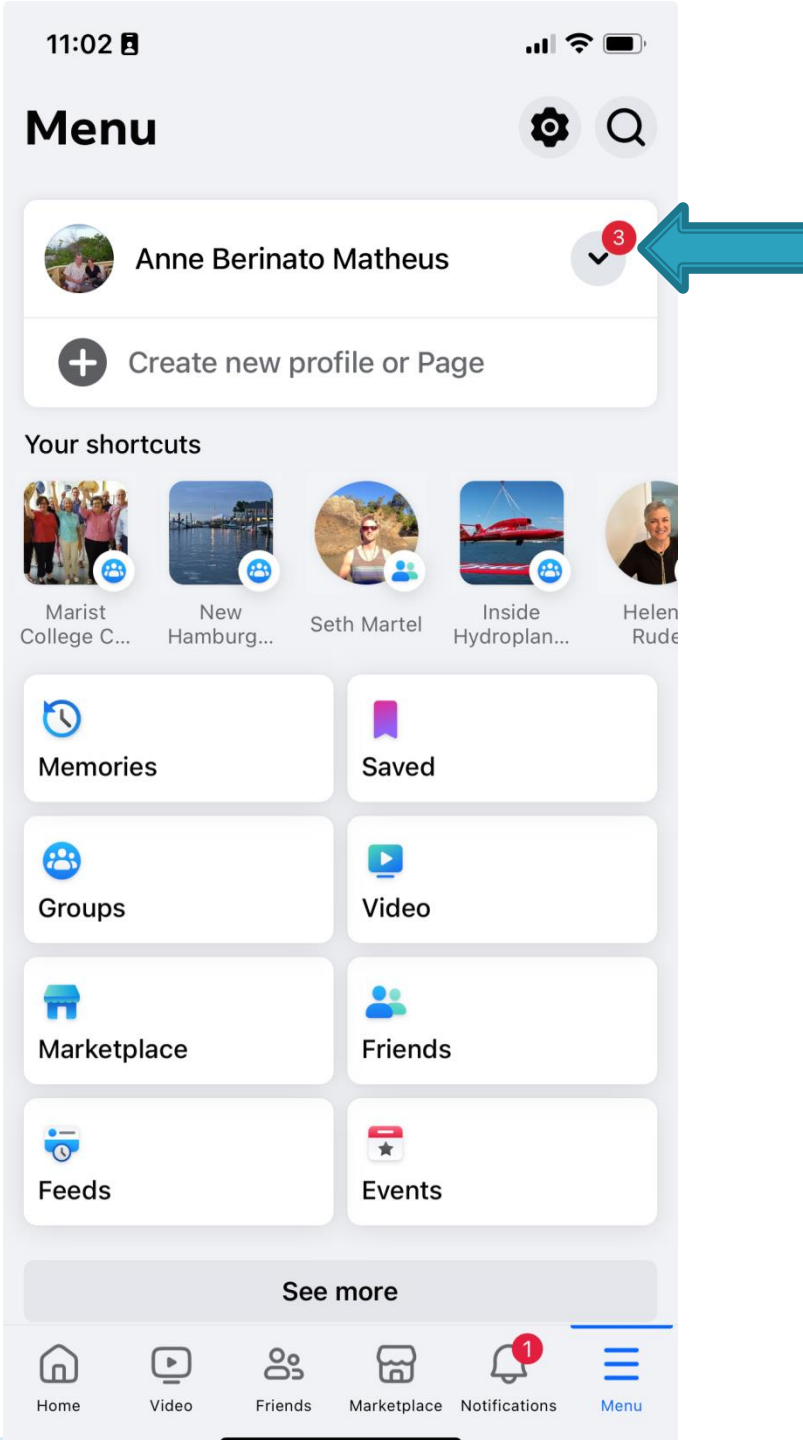

Home - eBucks
https://www.ebucks.com/web/eBucks/
eBucks
rewards from FNB
For me
Home
About eBucks
HTTPS Everywhere
HTTPS Everywhere
Stable rules
Force encrypted connections to these websites:
Google APIs
What is this?

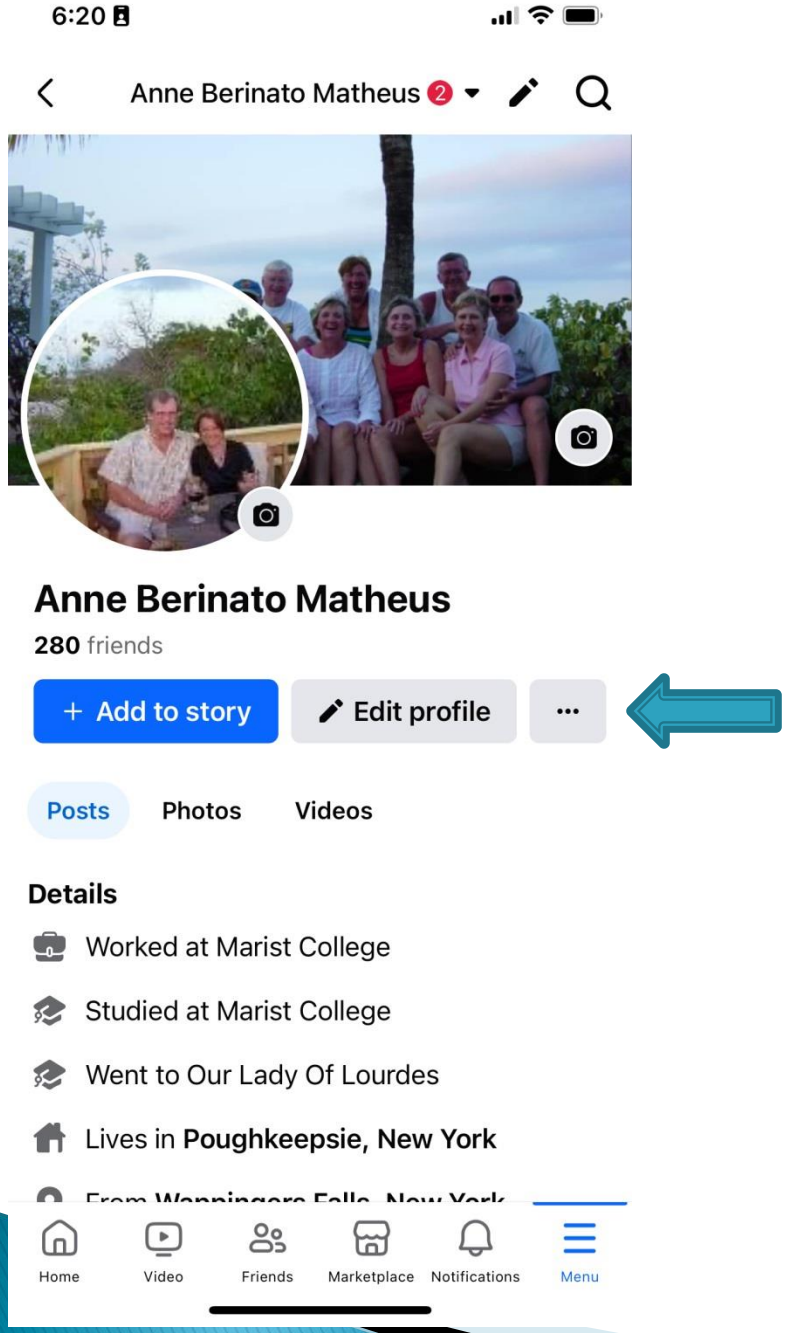
Social Media Safety

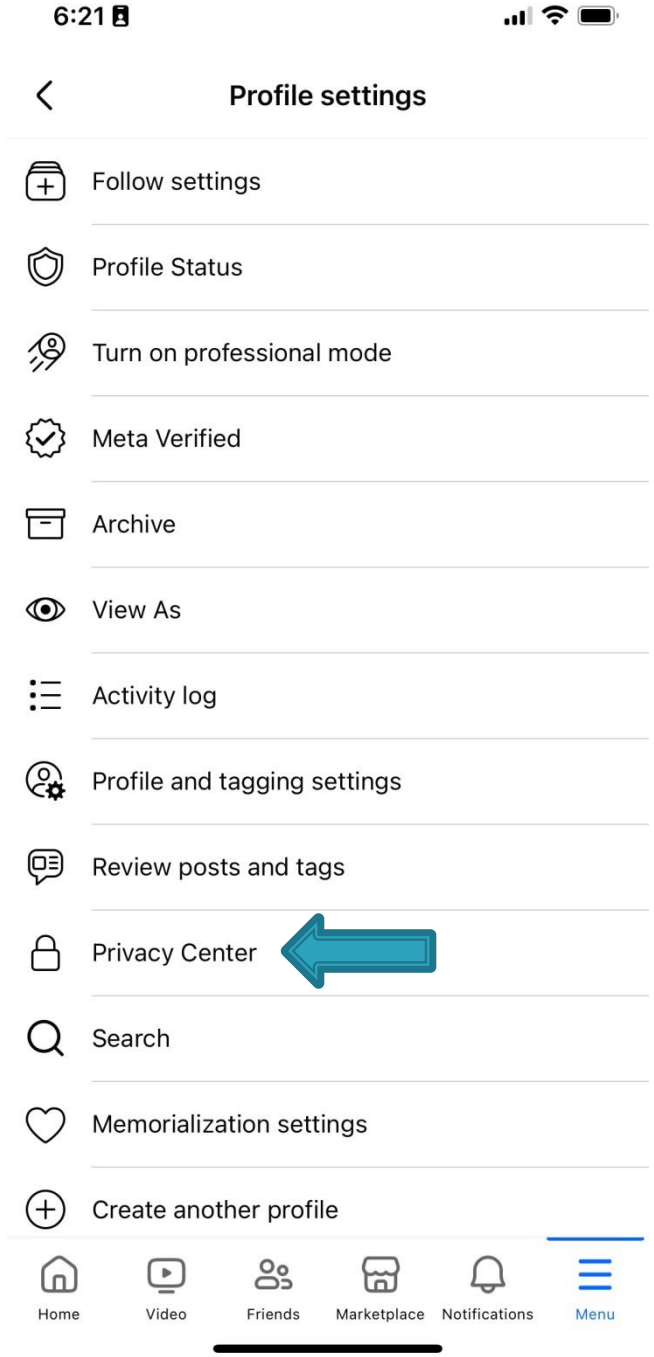
- Be cautious about what you share.
- Adjust privacy settings.
- Recognize fake profiles.

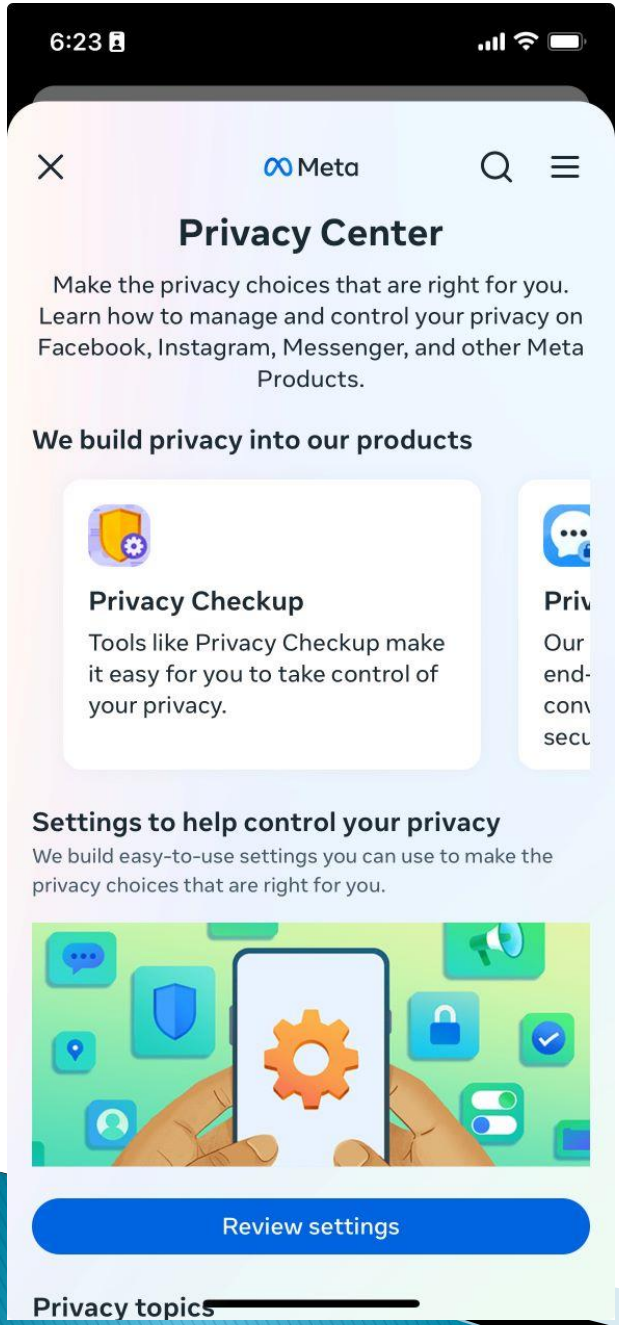
- https://myaccount.google.com/data-and-privacy?utm_source=chrome-settings
  - Settings
  - Autofill and passwords
  - Safety Check
  - Chrome found some safety recommendations for your review
  - Passwords


10:58
facebook
What's on your mind?
Create a story
Roger Segura
Dennis Lee
Minnat
Mary EJ Hemingway
Aug 3
A friend posted this today and I wanted to share it.
The world is changed by your example not by your opinion.
Home
Video
Friends
Marketplace
Notifications
Menu

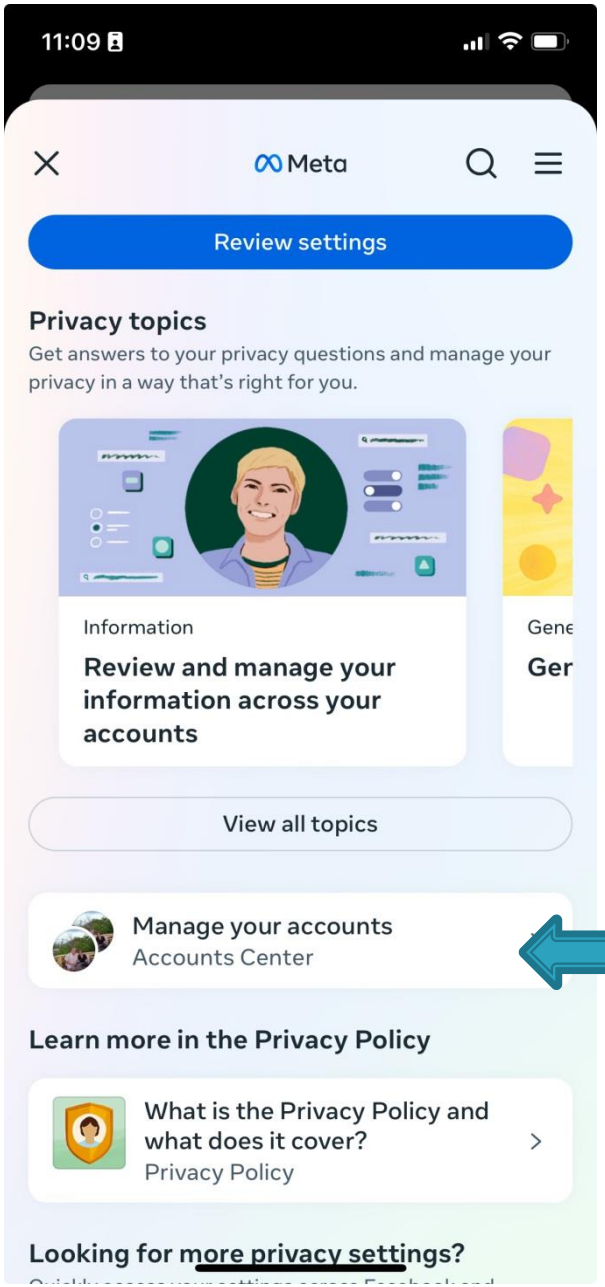

11:02
Menu
Anne Berinato Matheus
3
Create new profile or Page
Your shortcuts
Marist College C...
New Hamburg...
Seth Martel
Inside Hydroplan...
Memories
Saved
Groups
Video
Marketplace
Friends
Feeds
Events
See more
Home
Video
Friends
Marketplace
Notifications
1
Menu

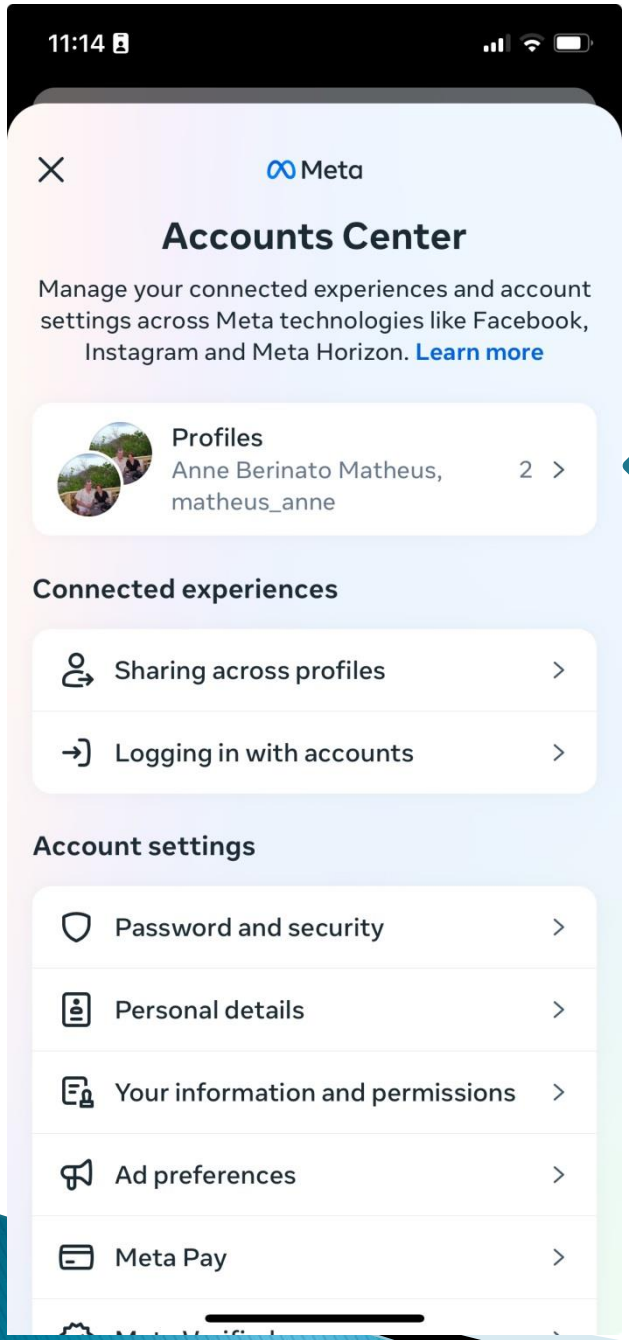

6:20
Anne Berinato Matheus 2
Anne Berinato Matheus
280 friends
+ Add to story
Edit profile
Posts
Photos
Videos
Details
Worked at Marist College
Studied at Marist College
Went to Our Lady Of Lourdes
Lives in Poughkeepsie, New York
Home
Video
Friends
Marketplace
Notifications
Menu

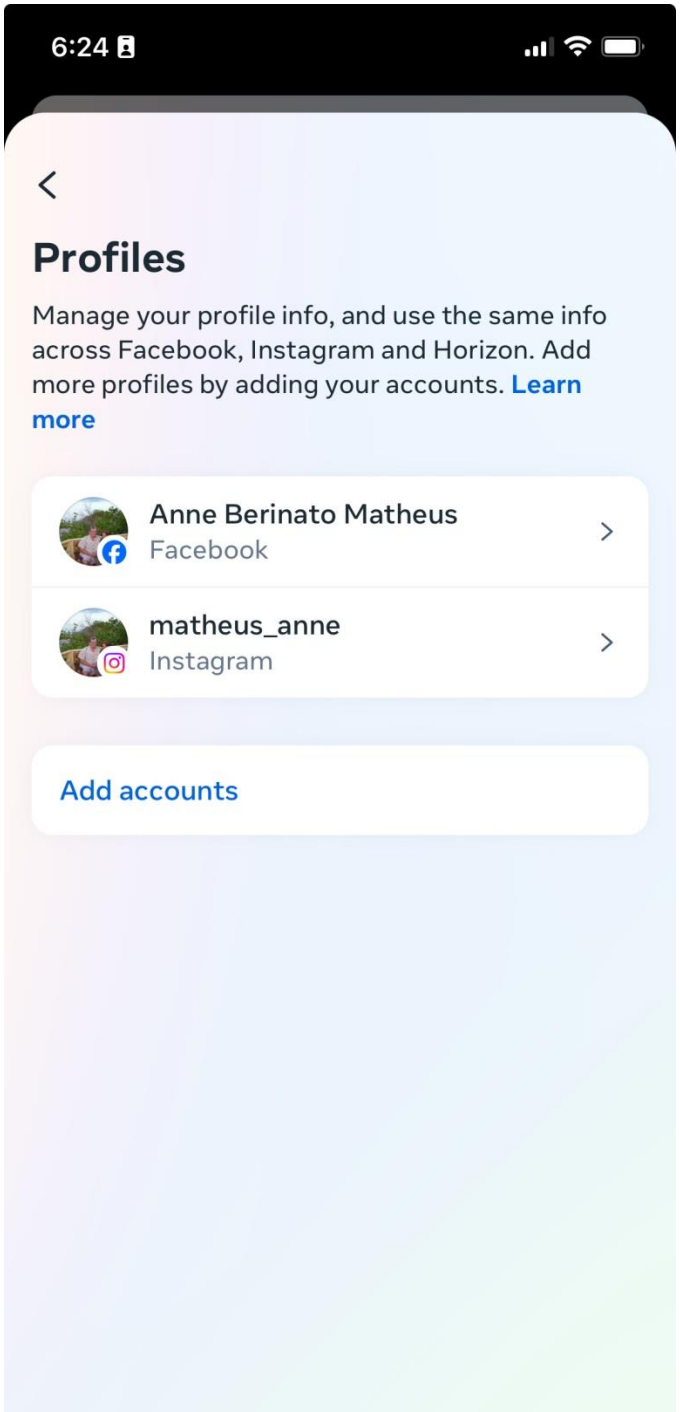

6:21
Profile settings
Follow settings
Profile Status
Turn on professional mode
Meta Verified
Archive
View As
Activity log
Profile and tagging settings
Review posts and tags
Privacy Center
Search
Memorialization settings
Create another profile
Home
Video
Friends
Marketplace
Notifications
Menu



This is the same screen, but you need to scroll down to find Manage your accounts

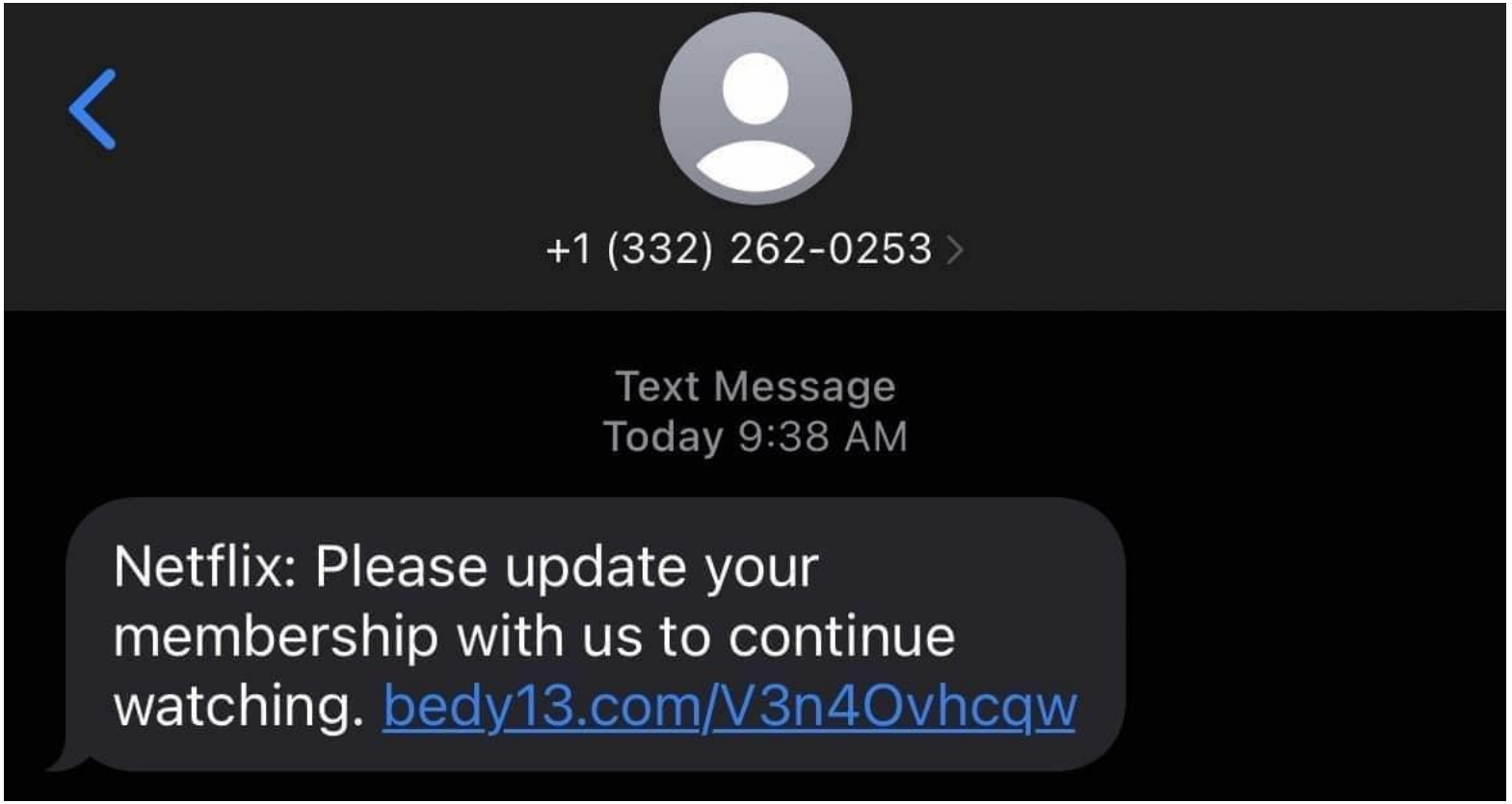



11:14
Meta
Accounts Center
Manage your connected experiences and account settings across Meta technologies like Facebook, Instagram and Meta Horizon. Learn more
Profiles
Anne Berinato Matheus, matheus_anne
2
Connected experiences
Sharing across profiles
Logging in with accounts
Account settings
Password and security
Personal details
Your information and permissions
Ad preferences
Meta Pay

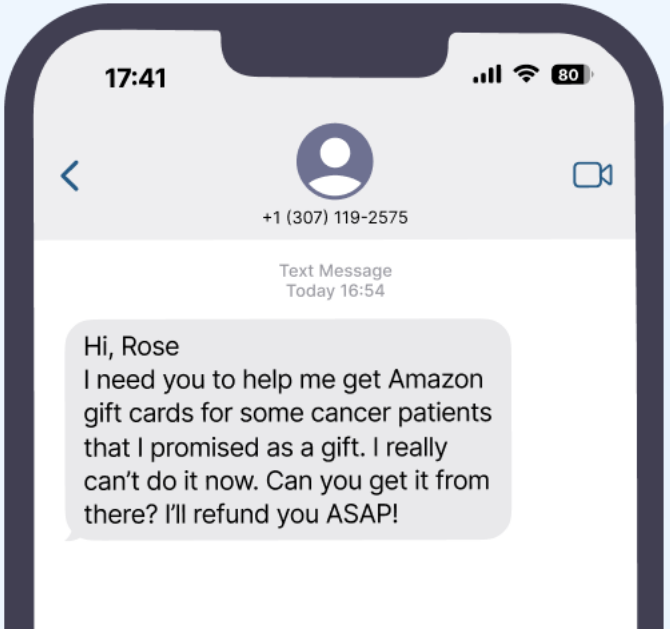

6:24
Profiles
Manage your profile info, and use the same info across Facebook, Instagram and Horizon. Add more profiles by adding your accounts. Learn more
Anne Berinato Matheus
Facebook
matheus_anne
Instagram
Add accounts

Common Scams

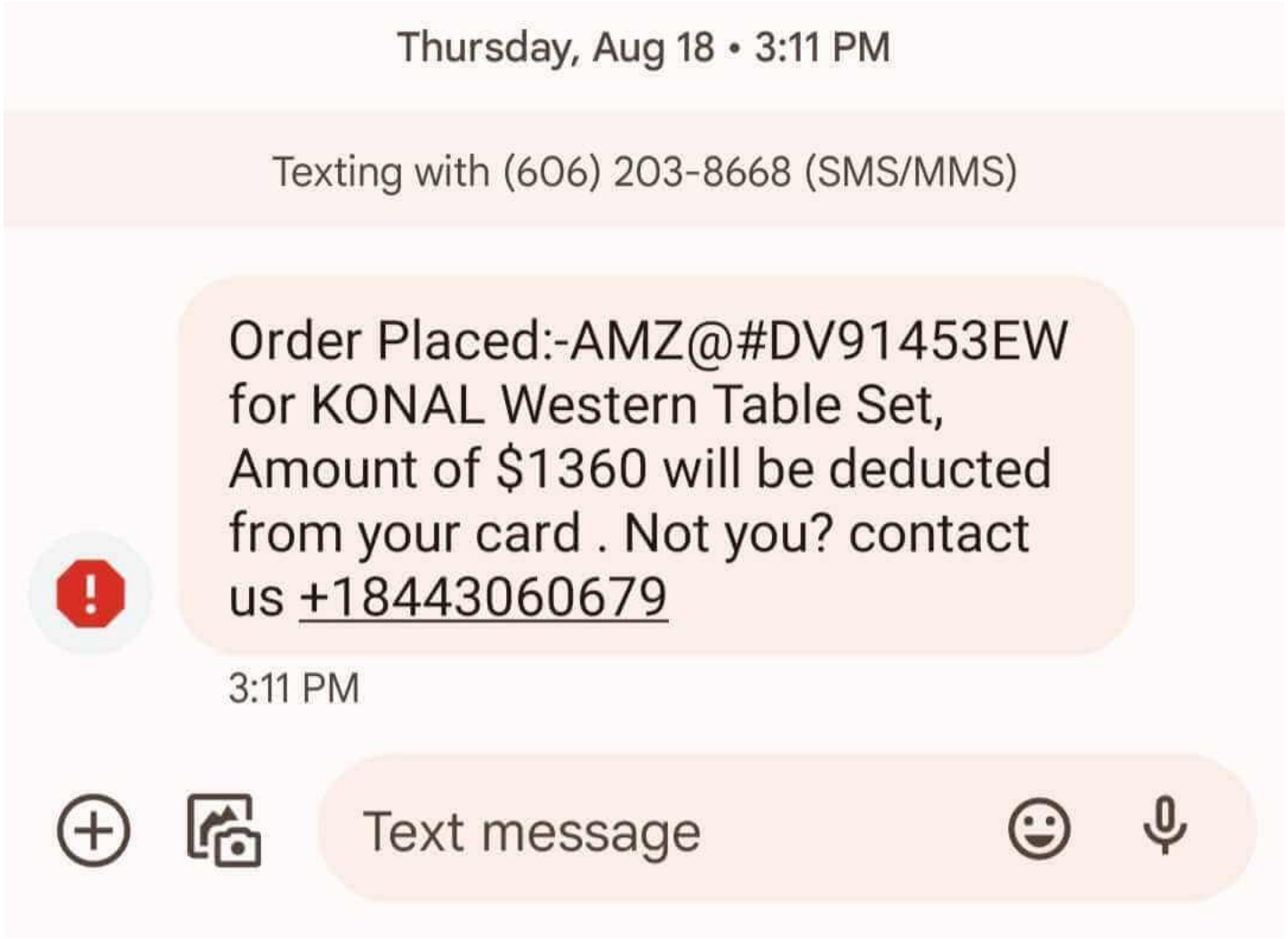
- Tech support scams.
- Lottery and prize scams.
- Romance scams.


+1 (332) 262-0253
Text Message
Today 9:38 AM
Netflix: Please update your membership with us to continue watching. bedy13.com/V3n4Ovhcqw

Romance scams



TextMagic


Thursday, Aug 18 • 3:11 PM
Texting with (606) 203-8668 (SMS/MMS)
Order Placed:-AMZ@#DV91453EW for KONAL Western Table Set, Amount of $1360 will be deducted from your card . Not you? contact us +18443060679
3:11 PM
Text message

Conclusion

- Recap of key points
- Stay vigilant.