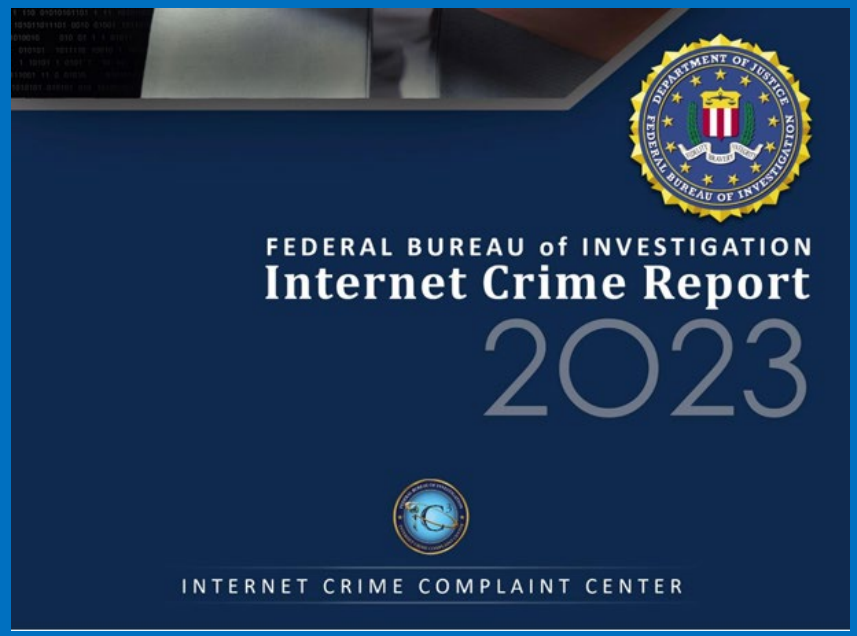
ELDER FRAUD


Operation
Boomerang


FEDERAL BUREAU of INVESTIGATION
Internet Crime Report
2023
INTERNET CRIME COMPLAINT CENTER

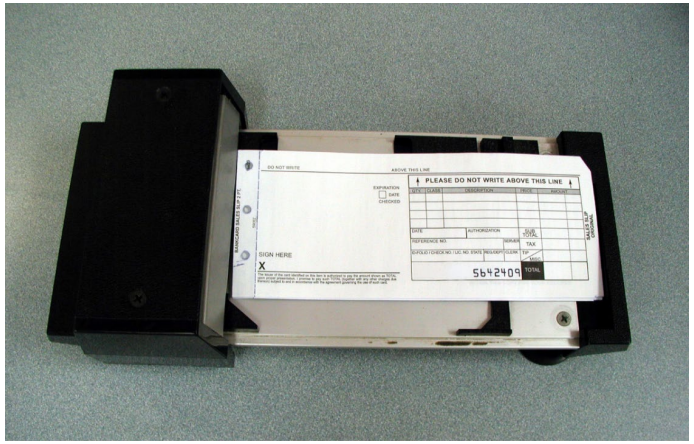
Operation: Boomerang

- Dave Johnson
- Pearl Technology, Managing Partner
- Leader, Peoria InfraGard
- 39 Years of IT/Cybersecurity Experience
- Graduate of FBI Citizens Academy
- Proud Father, Grandpa, and Boomer!

“E-mail will never be as popular as the United States Postal Service.”

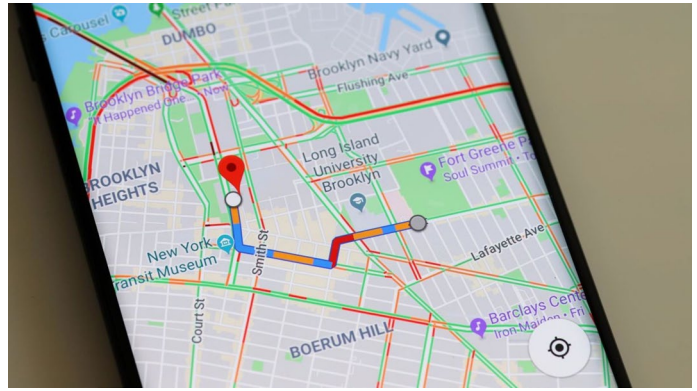
Dave Johnson 1985


phone


PLEASE DO NOT WRITE ABOVE THIS LINE
SIGN HERE
564209


ATM
RECEIPT
GENMEGA
CARD


9:41
Mail
Tuesday
12
Calendar
Photos
Camera
Maps
Clock
Weather
News
Home
Notes
Stocks
Reminders
TV
App Store
iTunes Store
iBooks
Health
Wallet
Settings


DUMBO
Brooklyn Navy Yard
Flushing Ave
Long Island University Brooklyn
BROOKLYN HEIGHTS
New York Transit Museum
Smith St
Court St
Lafayette Ave
BOERUM HILL

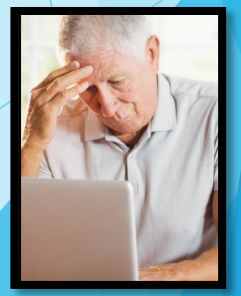

CREDIT
SALE
10.00
CHASE
VISA
DEBIT

BY THE NUMBERS

2023 IC3 Complaints by Age Group

Age Group	Complaints	Losses
Under 20	18,174	$40.7M
20-29	62,410	$360.7M
30-39	88,138	$1.2B
40-49	84,052	$1.5B
50-59	65,924	$1.7B
60+	101,068	$3.4B

*Some reports say less than 1 in 20 incidents of cybercrime and elder fraud get reported.



Types of crimes – by number of victims

2022 CRIME TYPES

VICTIMS OVER 60 COUNTS

Crime Type	Victims	Crime Type	Victims
Tech Support	17,810	Lottery/Sweepstakes/Inheritance	2,388
Non-payment/Non-Delivery	7,985	Other	2,016
Personal Data Breach	7,849	Real Estate	1,862
Confidence/Romance	7,166	Employment	1,286
Credit Card/Check Fraud	4,956	Overpayment	1,183
Identity Theft	4,825	Harassment/Stalking	754
Investment	4,661	Data Breach	333
Extortion	4,285	SIM Swap	301
Spoofing	4,201	IPR/Copyright and Counterfeit	235
Phishing	4,168	Ransomware	215
BEC*	3,938	Threats of Violence	166
(Reporting a potential business victimization)	*2,552*	Malware	125
(Reporting a personal victimization)	*1,386*	Crimes Against Children	84
Government Impersonation	3,425	Botnet	33
Advanced Fee	3,153		

Types of crimes – by amount of loss

2022 CRIME TYPES, *Continued*

VICTIM OVER 60 LOSSES			
Crime Type	**Loss**	**Crime Type**	**Loss**
Investment	$990,235,119	Spoofing	$22,261,276
Tech Support	$587,831,698	SIM Swap	$19,515,629
BEC*	$477,342,728	Data Breach	$17,681,749
(Reporting a potential business loss)	*$369,773,371*	Extortion	$15,555,047
(Reporting a personal loss)	*$107,569,357*	Phishing	$14,453,929
Confidence/Romance	$419,768,142	Overpayment	$10,977,231
Government Impersonation	$136,500,338	Employment	$6,403,021
Real Estate	$135,239,020	Malware	$1,851,421
Personal Data Breach	$127,736,607	Threats of Violence	$376,458
Lottery/Sweepstakes/Inheritance	$69,845,106	Harassment/Stalking	$254,659
Credit Card/Check Fraud	$61,649,198	Ransomware**	$210,052
Non-payment/Non-Delivery	$51,531,615	IPR/Copyright and Counterfeit	$203,140
Advanced Fee	$49,322,099	Botnet	$120,621
Identity Theft	$42,653,578	Crimes Against Children	$48,373
Other	$31,410,237		

How Prevalent is Elder Fraud in Illinois?

Number of victims

2022 OVERALL STATE STATISTICS

VICTIMS OVER 60 BY STATE*

Rank	State	Victims
1	California	11,517
2	Florida	8,480
3	Texas	5,674
4	New York	4,239
5	Arizona	3,543
6	Ohio	3,099
7	Colorado	2,925
8	Pennsylvania	2,901
9	Illinois	2,495
10	Virginia	2,447

Amount of loss

2022 OVERALL STATE STATISTICS,

VICTIMS OVER 60 LOSSES BY STATE*

Rank	State	Loss
1	California	$624,509,520
2	Florida	$328,114,489
3	Texas	$243,067,545
4	New York	$212,045,216
5	Washington	$96,213,728
6	New Jersey	$92,712,866
7	Arizona	$82,255,007
8	Pennsylvania	$80,250,904
9	Georgia	$78,736,227
10	Illinois	$75,905,639

Average loss per victim in Illinois is over $30K!

Today's Presentation

- Talk about the most common scams.
- For each type of scam -
  - Show examples.
  - Talk about staying safe.
- Review what to do and what not to do.
- Questions and answers.
- This presentation will be made available to you.

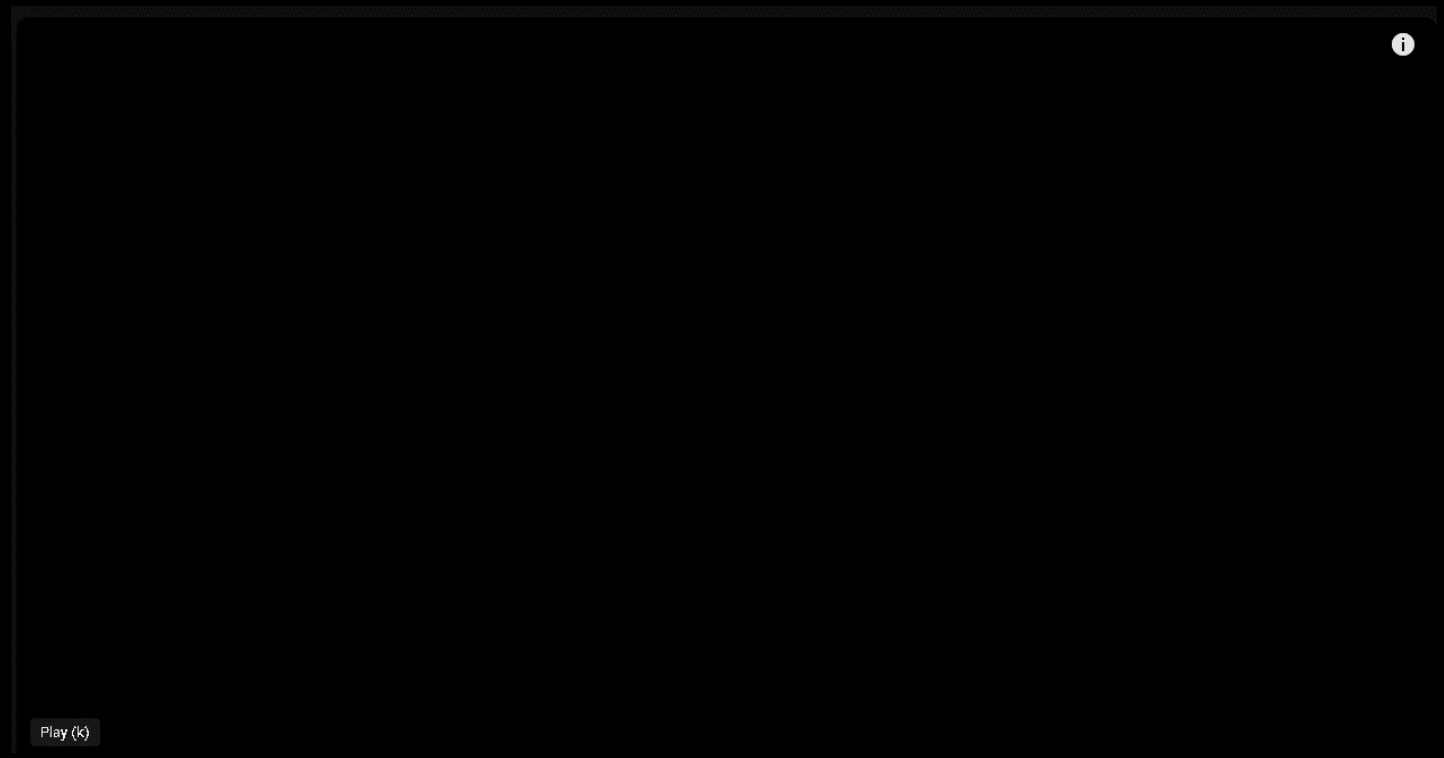
Tech Support Scam

Phone Call

“Hello. My name is Bill, and I am with Microsoft. We have noticed some unusual behavior on your computer, and we need to log in and make sure everything is OK.”

Text Message

Pop-Up on Computer

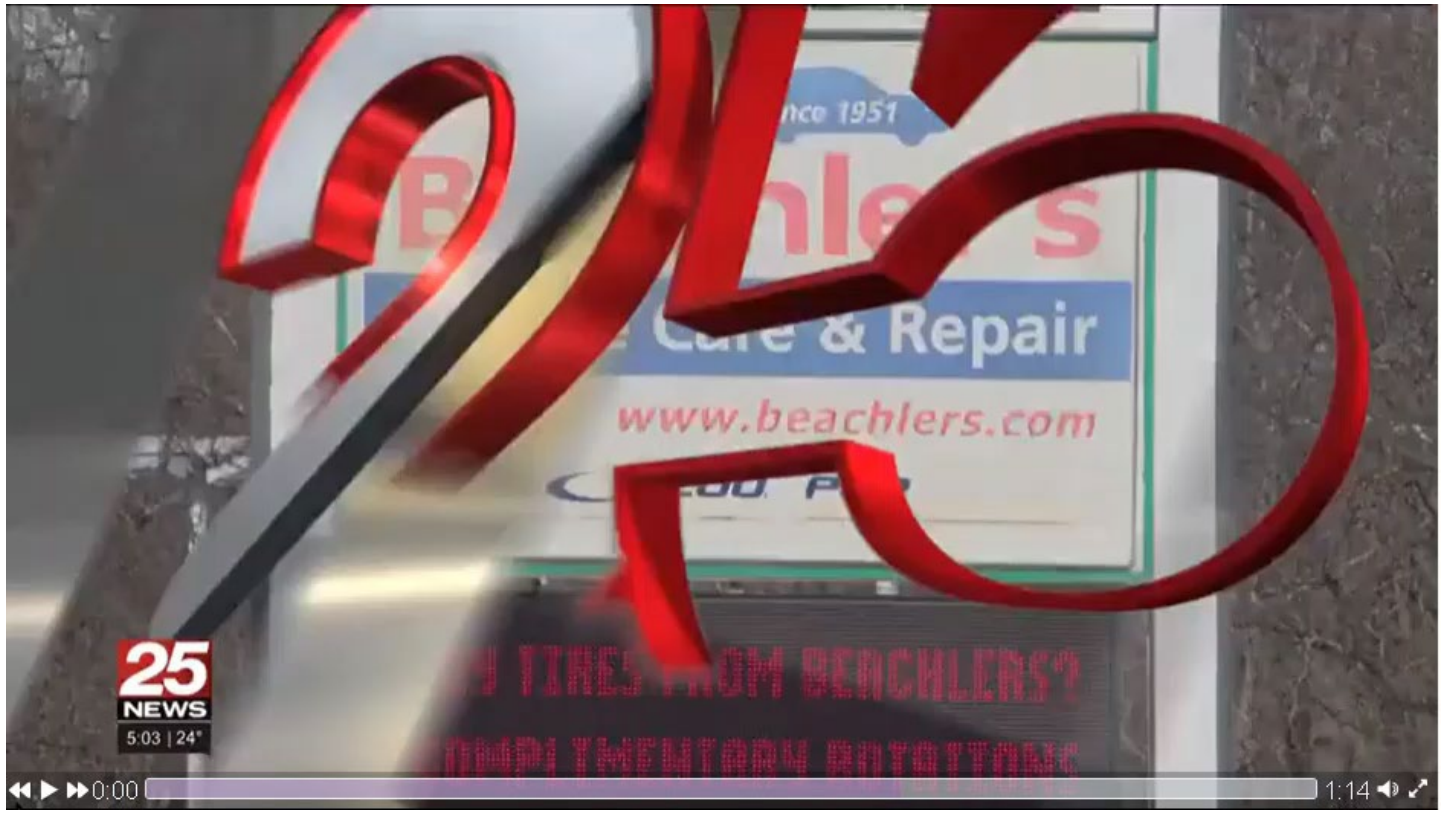


Tips for Staying Safe

- If you don’t recognize a phone number, don’t answer.
  - If it is important they will leave a message.
- If you get a text, don’t click on any links.
- Be very wary of any pop-ups on your computer.
  - Pop-ups are almost aways scams.
  - Turn on the pop-up blocker on your browser.
    - If you don’t know how, Google and YouTube are your friends.
- Never trust incoming calls or messages.
  - Instead, go to the source to verify.

Non-payment/Non-delivery Scam

Facebook Marketplace Scam



This is an actual email I received

A charge of $1899.00 has been made on your account- Your order has been dispatched

Leonard Merrick <leonardmerrick638@gmail.com>
to bcc: me

Hey there

I hope you are well

Dear Client

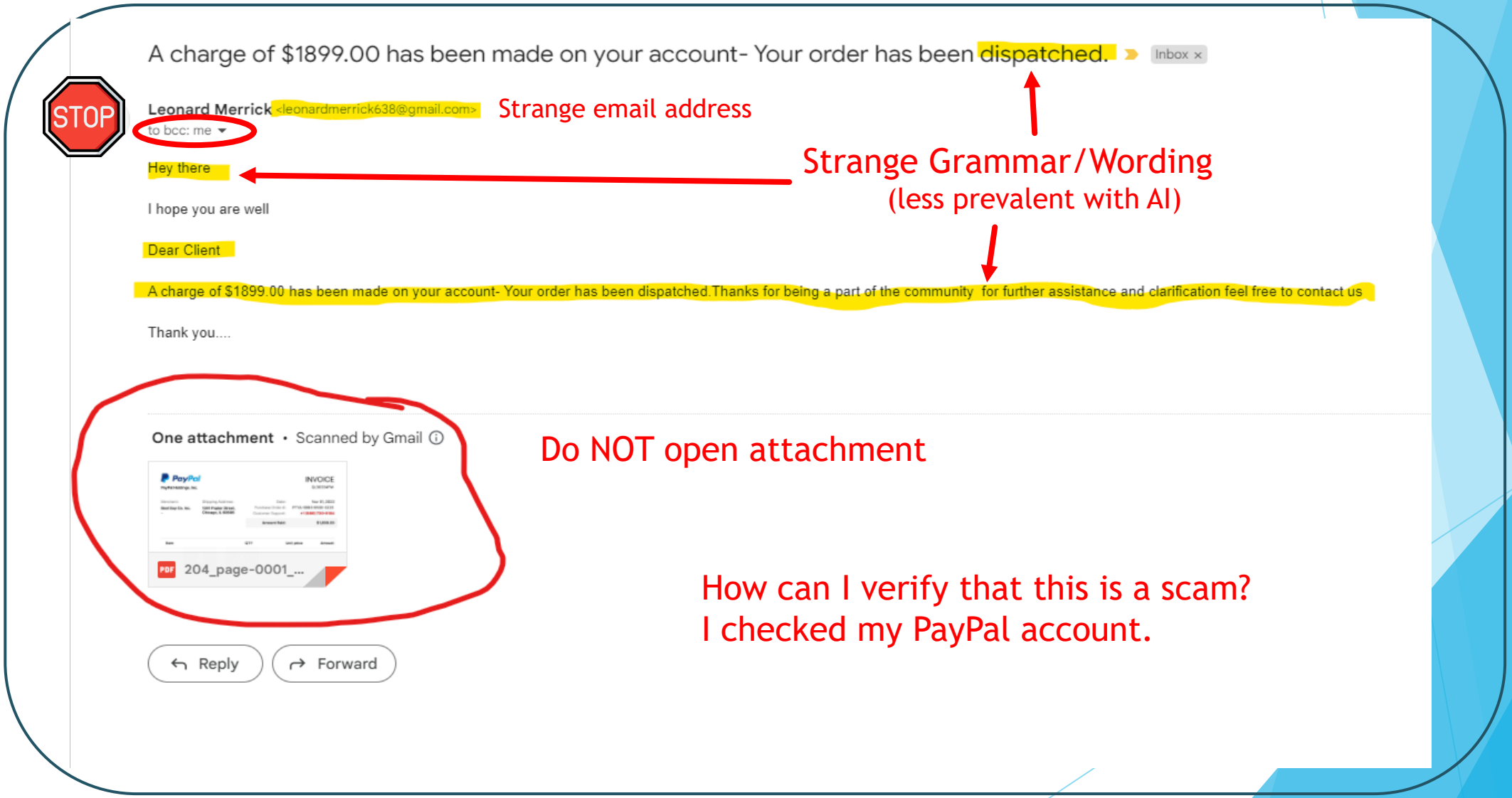
A charge of $1899.00 has been made on your account- Your order has been dispatched.Thanks for being a part of the community for further assistance and clarification feel free to contact us

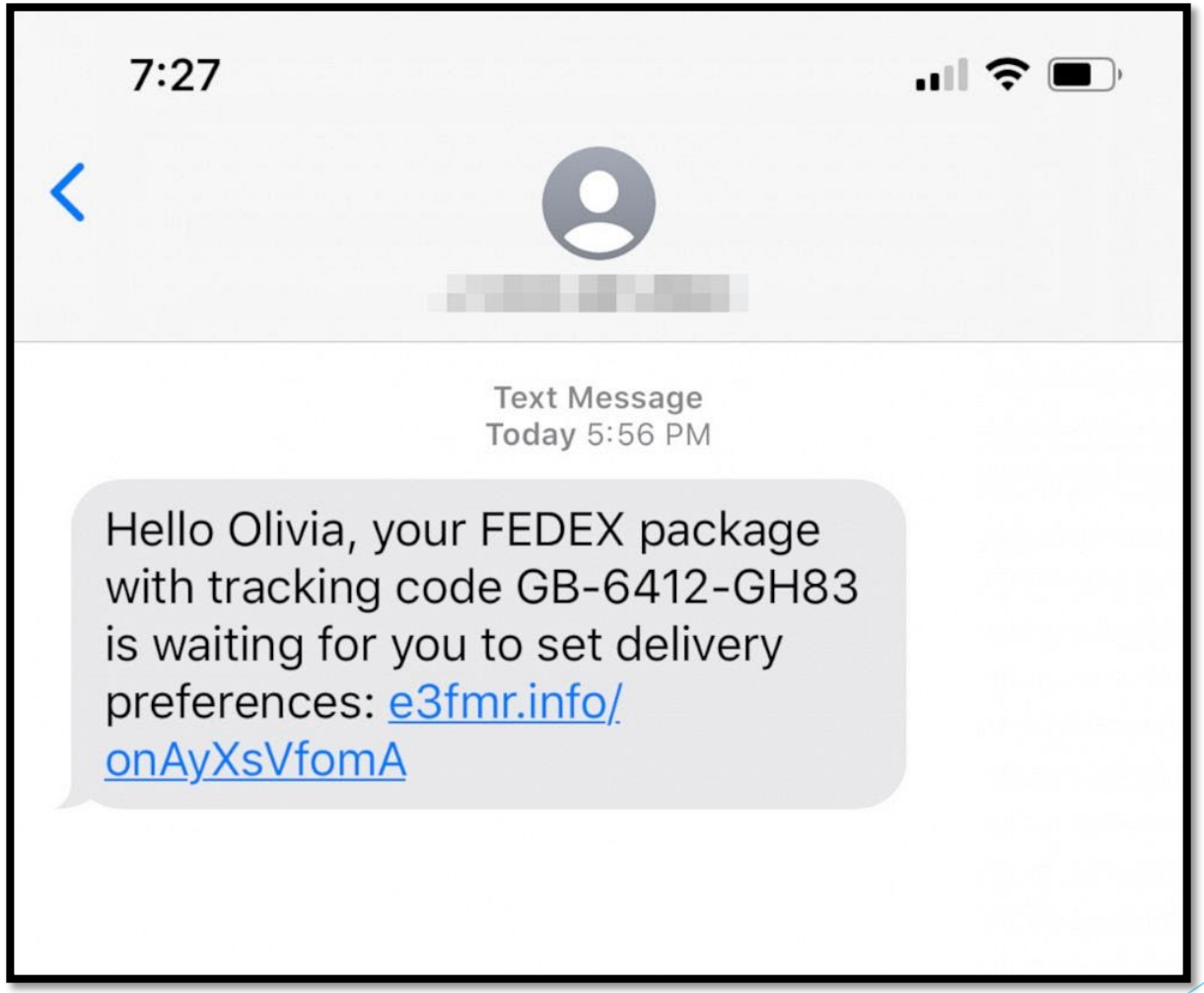
Thank you....

One attachment • Scanned by Gmail

Reply Forward

This is an actual email I received




7:27
Text Message
Today 5:56 PM
Hello Olivia, your FEDEX package with tracking code GB-6412-GH83 is waiting for you to set delivery preferences: e3fmr.info/onAyXsVfomA

Cyperc FR
Sponsored ·

"🔥Today's special liquidation product is
🎉2023 New Laptop Spectre 15 I7-9710, Display Touch UHD+ da 17", Intel i7-11800H, GeForce RTX 3050, 64GB RAM, 4TB SSD, Wi-Fi 6, Win 10 Pro
🔰3 years warranty service
🛒Click on the picture to buy"

ENNELLK.ONLINE
🔥Today Only $ 23
Shop now
💥Clearance💥 2023 New Laptop

1.5K 920 comments 70 shares

Pollyna-CA
Sponsored ·

Compact and powerful, the EOS Rebel T7 is a stylish entry-level DSLR with versatile imaging capabilities and a useful feature set Buy Now https://bit.ly/3F3q9IG

POLLYNA.COM
Record life in HD
Shop now
Factory direct sales lowest price The product is manufactured in California L A...

105 63 comments 2 shares

Like Comment Share

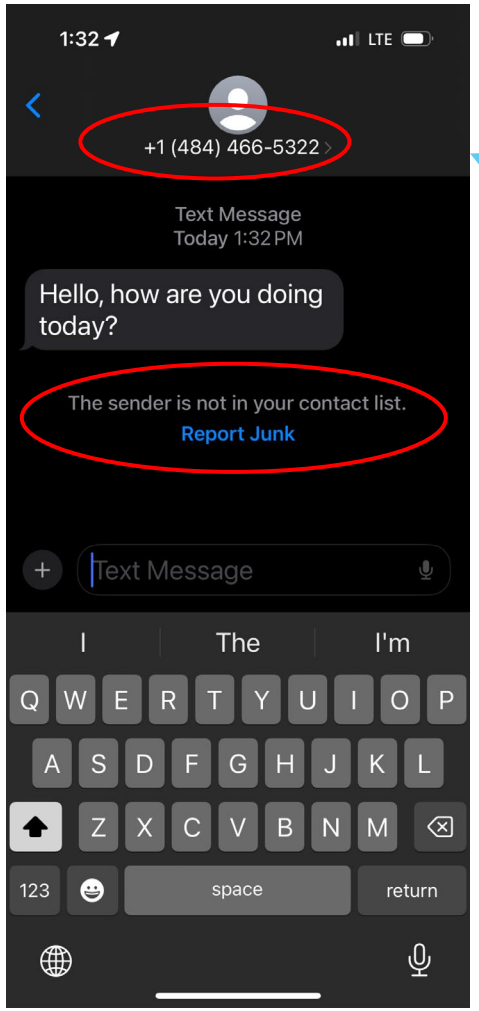
Tips for Staying Safe

- If you buy something from a person online:
  - Don’t give them money until you have seen the item.
  - Meet them in a safe place like a police department parking lot.

- If you get a text about a shipment, don’t respond to the text.
  - Go to the shipper’s website.

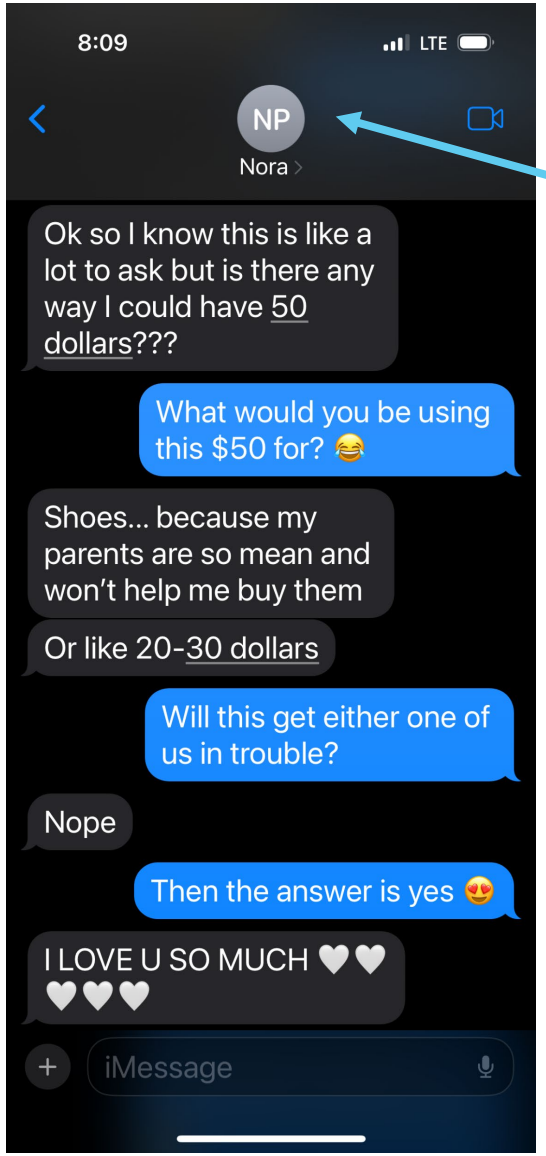
- If a deal looks too good to be true, it is too good to be true.

Confidence Scams
Romance Scams
Sextortion
“Pig Butchering”



This is How It Starts

- I don't know this person because their phone number is not in my Contacts.
- I do not recognize this number.
- This person is trying to draw me into a conversation that will ultimately lead to an investment scam, etc.
- Do not respond in any way. Block the number and Report Junk.



An Actual Text Message from My Granddaughter

- I know this is my granddaughter because her phone number is in my Contacts.
- If this request came from an unknown number, I would have called my granddaughter and asked her if she sent this message.
- I checked with her mother (my daughter).
  - Mom was not happy 😂
- I handed my granddaughter the cash in person.

Hey there. How are you?
My name is Kristen.

- My mom is in the hospital, and I need some money to help with expenses. Will you please help me? Can you send me $200 in Visa gift cards?

Or…

- I would love to send you some pictures of me in lingerie. How about you send me $100, and I'll send the pictures?

Or…

- I think older men are hot. Want to trade some sexy pictures?

Or…

- I've been killing it in cryptocurrency lately. Have you ever thought about investing?

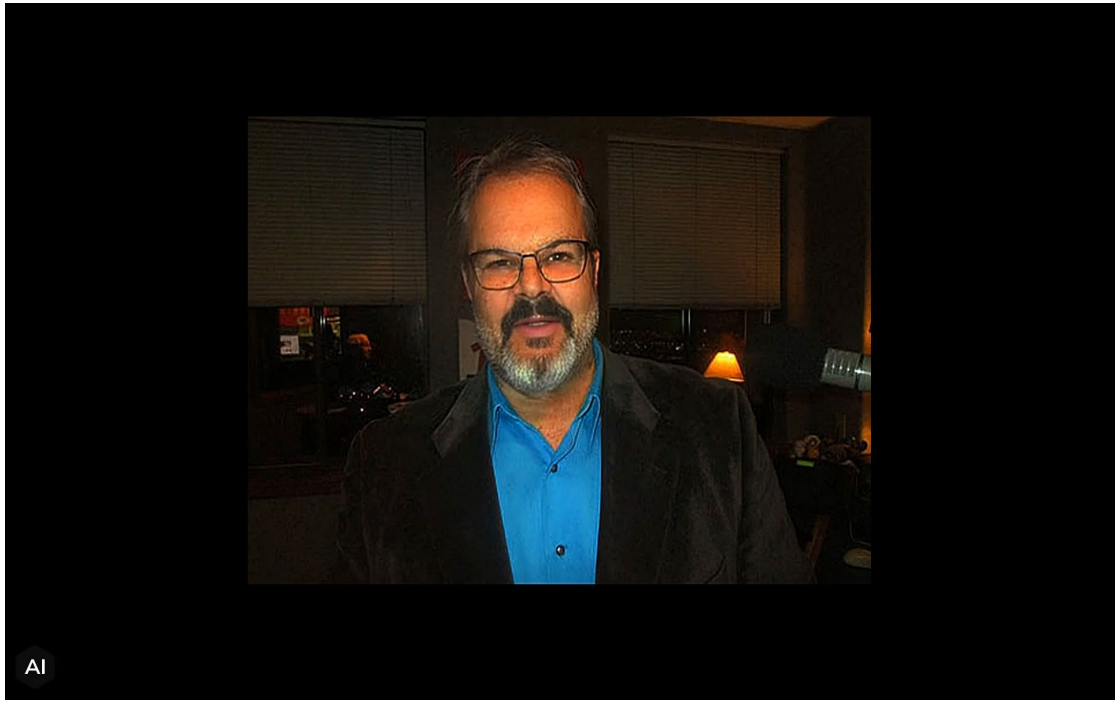
This photo is not even a real person. It was generated using AI. This person does not exist.

- Gift cards are very hard to trace, yet very easy to spend.
- If “Kristen” does send you pictures of herself in lingerie, they won’t show her face (not her) and will simply have been downloaded from the internet.
- Once “Kristen” gets a compromising picture of you, you will be extorted, or she will post your pictures online for the public to see. (Sextortion)
- “Kristen” will build an online relationship with you. She will get you to invest a small amount of money with her and you will actually make some money. Then she will ask for a much larger investment. Once you send that money, you will never see her or your money again. (Pig Butchering).

So, if Kristen doesn't really exist, who am I chatting with?

You are likely talking to someone like this guy. A lot of "romance scams" are run out of Nigeria.

Artificial Intelligence - AI



Tips for Staying Safe

- Keep your phone contacts up to date to make it easier to identify an incoming call or text.
- If you don’t know someone, don’t trust them.
- Do not carry on an online conversation with people you don’t know.
- NEVER send compromising photos, even to people you know. Once it has crossed the internet, it will always be on there.
- Be aware of AI and its capabilities.

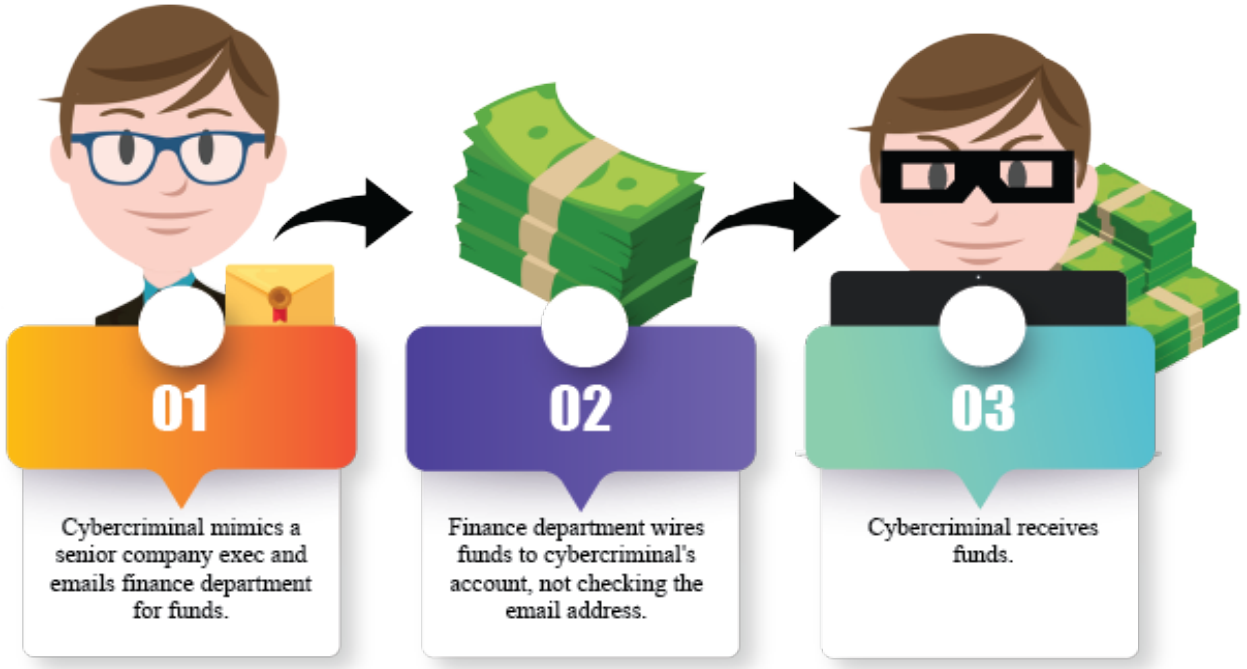
The Grandchild Scam

- You get a call from someone who says your grandchild is in trouble.
  - Sometimes AI is used to play a message that sounds like it is coming from your grandchild.

- You may be told that you need to get cash and a courier will pick it up.

- The person says the cash will be used to get your grandchild out of trouble.

Business Email Compromise



Business Email Compromise

- Someone pretends to be an executive at your company.
  - They may even have access to the executive's email account, so the email address looks legitimate.
  - They may have read through previous emails regarding wiring funds, so they have the correct wording.

- The perpetrator asks someone in accounting to wire money and gives the account and instructions.

- The request looks and feels legitimate.

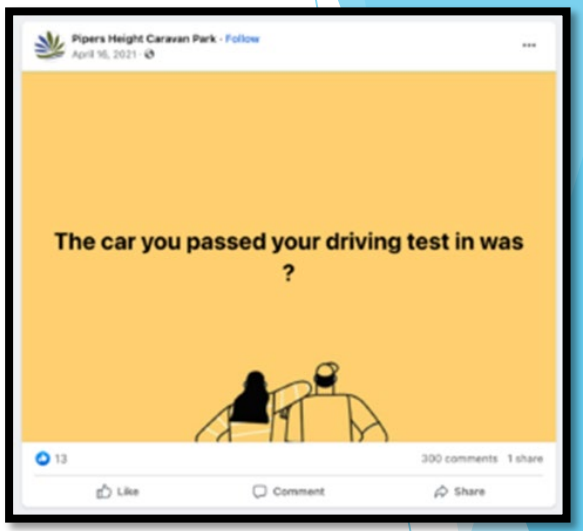
- The accountant wires the money, not knowing it is going to the criminal.

Tips for Staying Safe

- If someone claims that your grandchild is in trouble, call your grandchild and his/her parents immediately.
- If the grandchild is actually missing, call law enforcement **immediately.**
- If someone *you think you know* asks you to send money, call them to verify before doing anything.
- If someone *you don't know* asks you to send money, don't.
- If you already sent the money, notify law enforcement immediately. Time is of the essence.

Facebook Scams

Where did you grow up: **STOP**
Favorite Color: **GIVING**
First pet's name: **PEOPLE**
Street you grew up on: **YOUR**
Favorite child's name: **PERSONAL**
Favorite sports team: **INFORMATION**
High school mascot: **TO**
Favorite food: **GUESS**
What was you first car: **YOUR**
Mom's maiden name: **PASSWORDS**
First job: **AND**
Favorite band: **SECURITY**
Elementary school name: **QUESTIONS**



Facebook Scams

- Quizzes and Questionnaires
  - Post a picture of the High School you went to.
  - Post a picture of your first pet and tell us its name.
  - Show us a picture of your first car.

➥ *These are the same security questions you answer to reset a password!*

- Do “this” and it will change your Facebook algorithm so you see less ads.

➥ *Not true, never was true, never will be true.*

- Share your contact list with Facebook so you can find more of your friends.

➥ *Now when you get hacked, the hackers will have all your contacts and will try to scam them pretending to be you.*

How to Stay Safe on Social Media

- If you get it for free, YOU are the product!
- Use strong passwords and multi-factor authentication (MFA).
- Don’t post personal information.
- Don’t share vacation pictures until you are back home.
- Don’t accept new friend requests from people you are already friends with.
- Be skeptical of messages you receive from friends. They may have been hacked.

How to Stay Safe on Social Media

- Be very careful posting pictures of kids. Sexual predators are everywhere.

- Tighten down your privacy settings.
  - Who can post on your page.
  - Who can view your page.

- Don’t share other people’s posts. You could be sharing a scam or misinformation/disinformation.
  - Misinformation – What you read, or watch, is often not true.
    - If misinformation is shared enough, people think it is true.
  - Disinformation – Bots, Russia, China, Iran, and others purposely post things that are not true to create confusion and discord.

The “Go Ask Mom” Rule

Check suspicious requests by contacting the source directly.

Go Ask Mom - Examples

- If you are contacted (phone call, mail, text, email) by someone that appears legitimate, do not respond to the message. Instead, call the person or business directly.

- If you get an email from the IRS asking you to immediately pay them money, call the IRS phone number and ask if the email is from them.
  - The IRS does NOT contact you by email, phone, or text. They use the US Postal Service or come to your home in person.

- If someone contacts you, claiming to be from law enforcement, and asks you to send money…it's a scam.
  - Call the agency that supposedly contacted you.

Bank Text Scam

Tips for protection

- Recognize scam attempts and end all communication with the perpetrator. ***BE SUSPICIOUS***.

- Resist the ***pressure to act quickly***. Scammers create a sense of urgency to produce fear and lure victims into immediate action.

- Be cautious of ***unsolicited*** phone calls, emails, texts, mailings, and door-to-door service offers.

- Never give or send any personally identifiable information, money, jewelry, gift cards, checks, or wire information to ***unverified people or businesses***.

Tips for protection

- Update computer, anti-virus.
  - On your phone as well.
- Never give ***unknown or unverified persons remote access*** to devices or accounts.
- Never open an ***email attachment*** from someone you do not know and be wary of email attachments forwarded to you.
- If possible, use Visa gift cards for online purchases.
  - You can load it just prior to making the purchase.

Tips for protection

- Take precautions to protect your identity if a criminal gains access to your device or account. ***Immediately contact your financial institutions*** to place protections on your accounts and monitor your accounts and personal information for suspicious activity.

- Be careful what you post and make public online. Scammers can use details shared on social media and dating sites to better understand and target you or know when you are out of town on vacation.

- Government or law enforcement officials will not demand payment by cryptocurrency, prepaid cards, wire transfers, or overnight mailed cash, nor contact a subject by phone to notify they are under investigation.

If you don’t remember anything else…

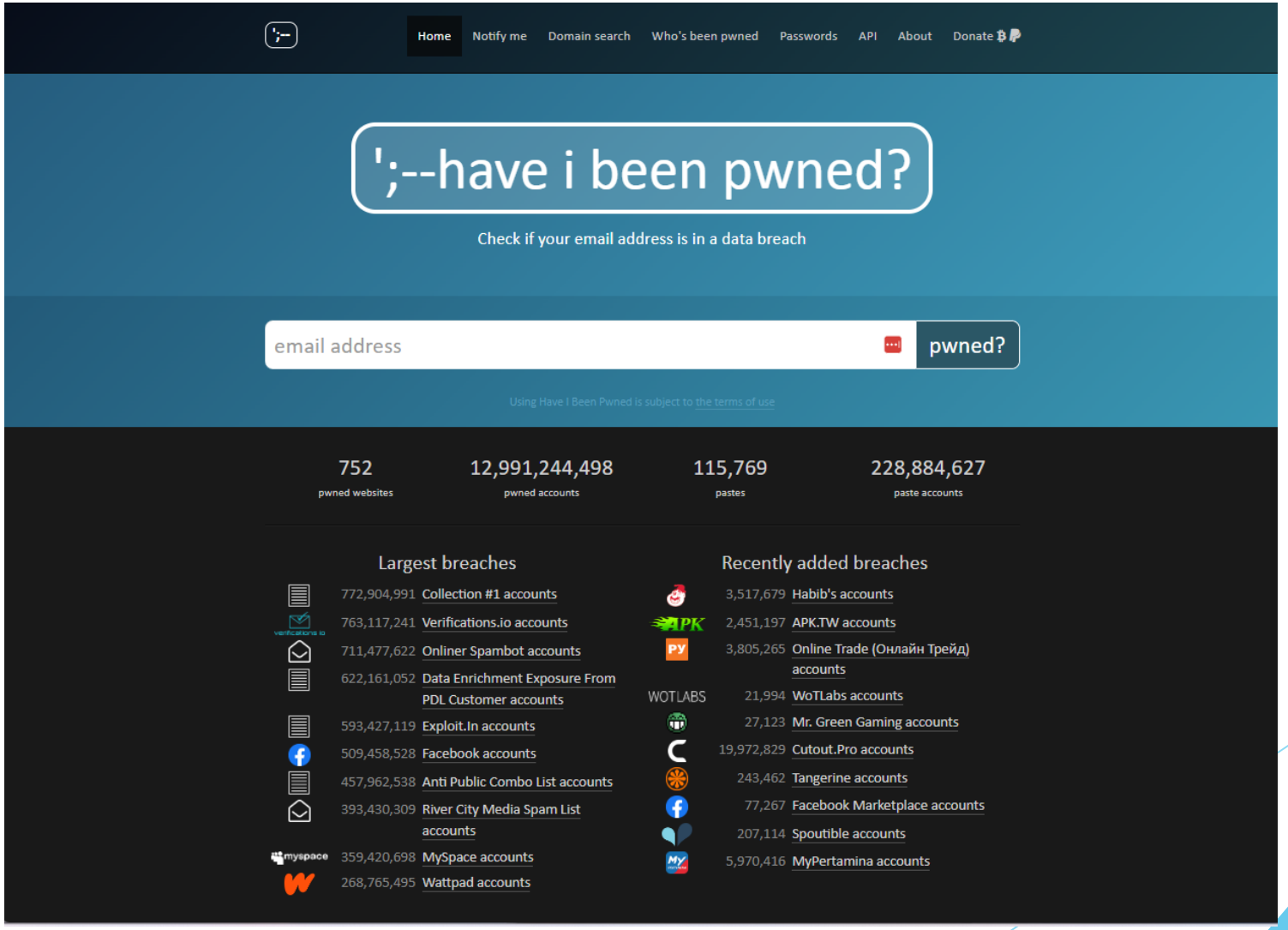
- Use strong passwords.
  - Not easy to guess.
  - Not a pet’s name.
  - Not a birthdate.
  - Not “1234”.

- Don’t use the same password on more than one account.

- Use a password manager.
  - 1Password
  - LastPass

- Use Multi-factor Authentication MFA) whenever possible.

Haveibeenpwned.com



If you are the victim of online scam or fraud.

- Report it to the FBI
  - https://www.ic3.gov/
  - They will look for the criminal.
  - Persons 60 and older may call the National Elder Fraud Hotline at (833) 372-8311 for assistance in filing with IC3.

- Report it to the FTC
  - https://reportfraud.ftc.gov/#/
  - They will tell you what steps you should take to recover your money, if possible.

More Information

- The Greg and Dan Show – WMBD Radio
  - Mondays at 7:25am
  - 1470 AM and 100.3 FM

Questions?