

A close-up, slightly blurred image of the American flag, showing the blue field with white stars and the red and white stripes. The flag is draped diagonally across the left side of the frame.

INTERNET SAFETY, SCAMS IDENTITY THEFT, AND FRAUD

**COLORADO SPRINGS POLICE DEPARTMENT
CRIME PREVENTION UNIT**

OFC. MJ THOMSON (STETSON HILLS)

OFC. SCOTT MATHIS (SAND CREEK)

OFC. SID SANTOS (GOLD HILL)

OFC. BRIAN CORRADO (FALCON)



What you will learn...

- Basic internet safety
- Defend yourself from scams
- Protect your online identity
- Learn to be alert for fraud
- What to do if you're a victim

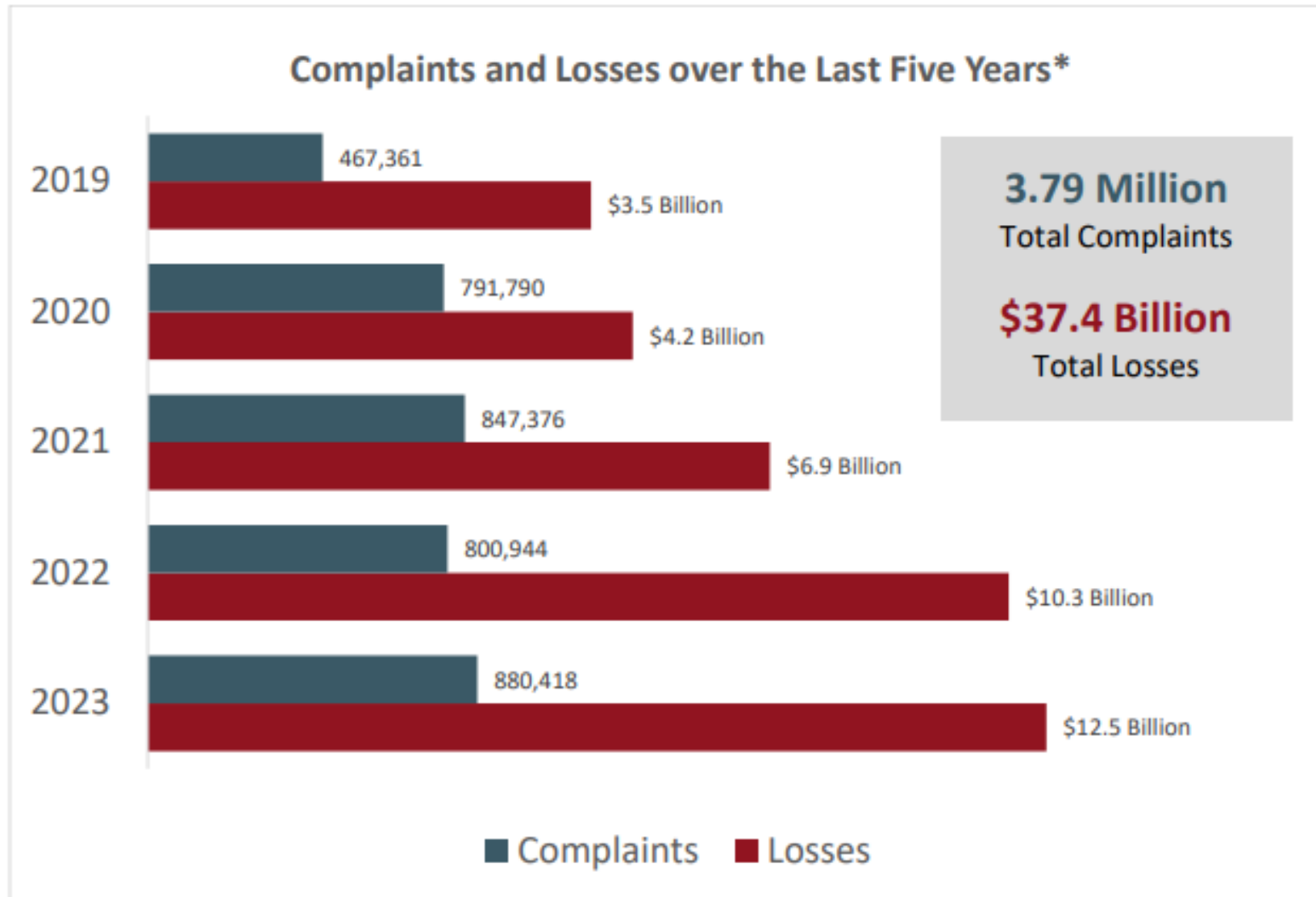


A close-up, slightly blurred image of the American flag, showing the blue field with white stars and the red and white stripes. The flag is draped diagonally across the left side of the frame.

THE DATA



How big is the problem?



Over the last five years, the IC3 (Internet Crime Complaint Center) has received an average of 652,000 complaints per year. These complaints address a wide array of Internet-related crimes affecting victims across the globe.

2022 to 2023 IC3 Breakdown



\$10.3 Billion

Victim losses in 2022



\$12.5 Billion

Losses in 2023



2,175+

Average complaints received daily



2,412

Average complaints received daily



651,800+

Average complaints received per



758,000+

Average complaints received per year (last 5 years)



Over 7.3 M

Complaints reported since

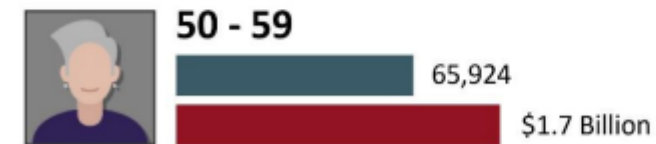
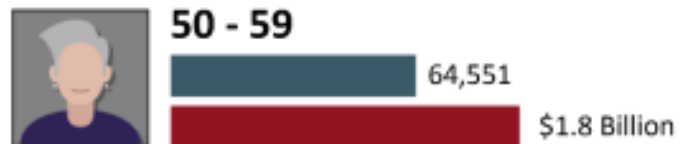
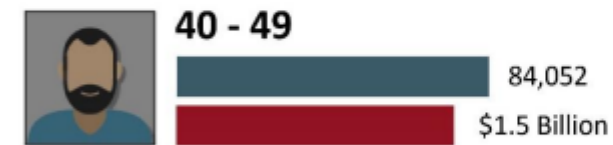
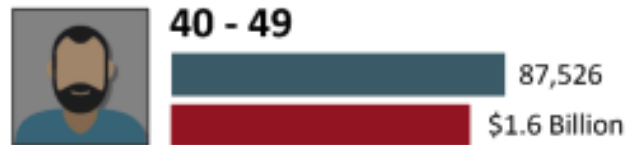
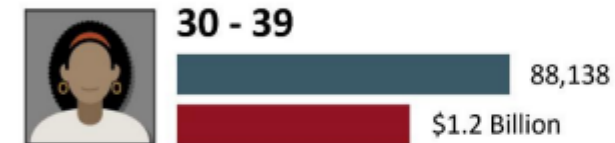
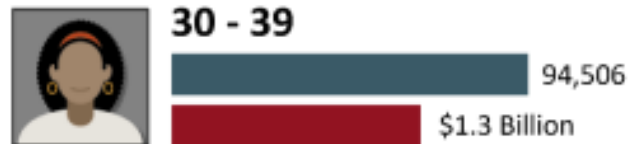
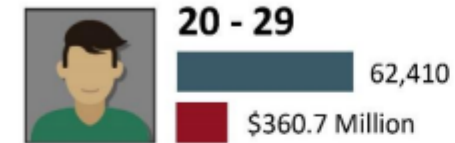
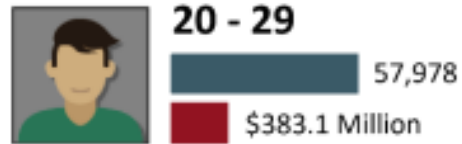


Over 8 Million

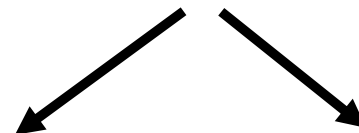
Complaints reported since inception



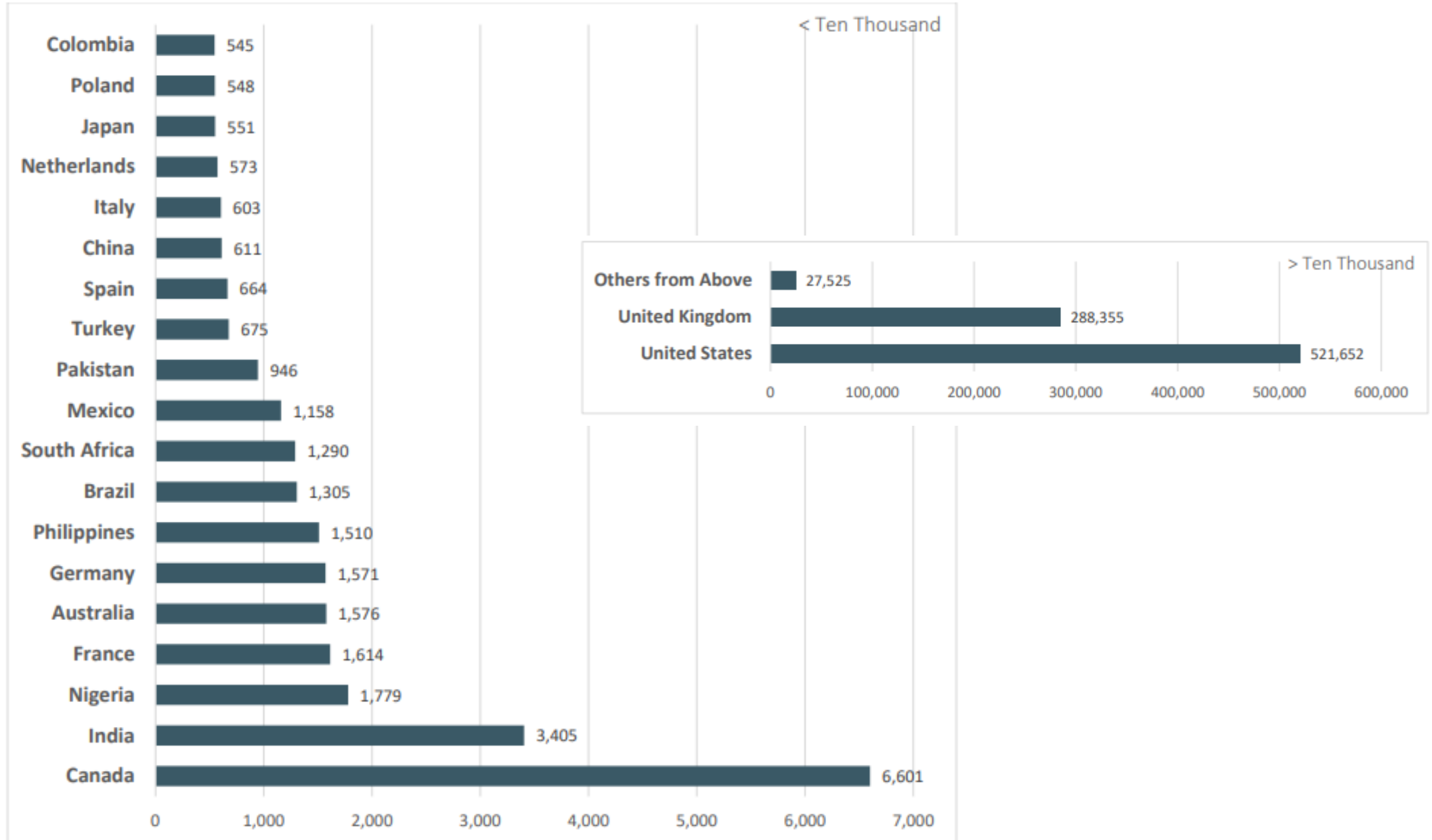
2022 to 2023– Victims by Age Group



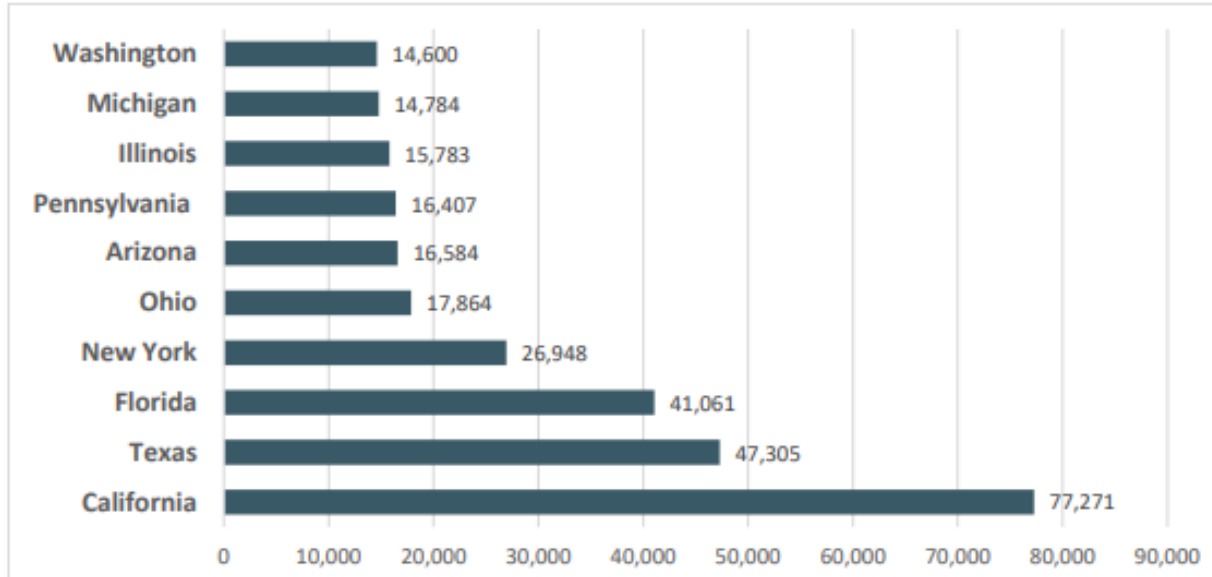
Victims over 60
account for 14% of the
complaints and 30% of
losses.



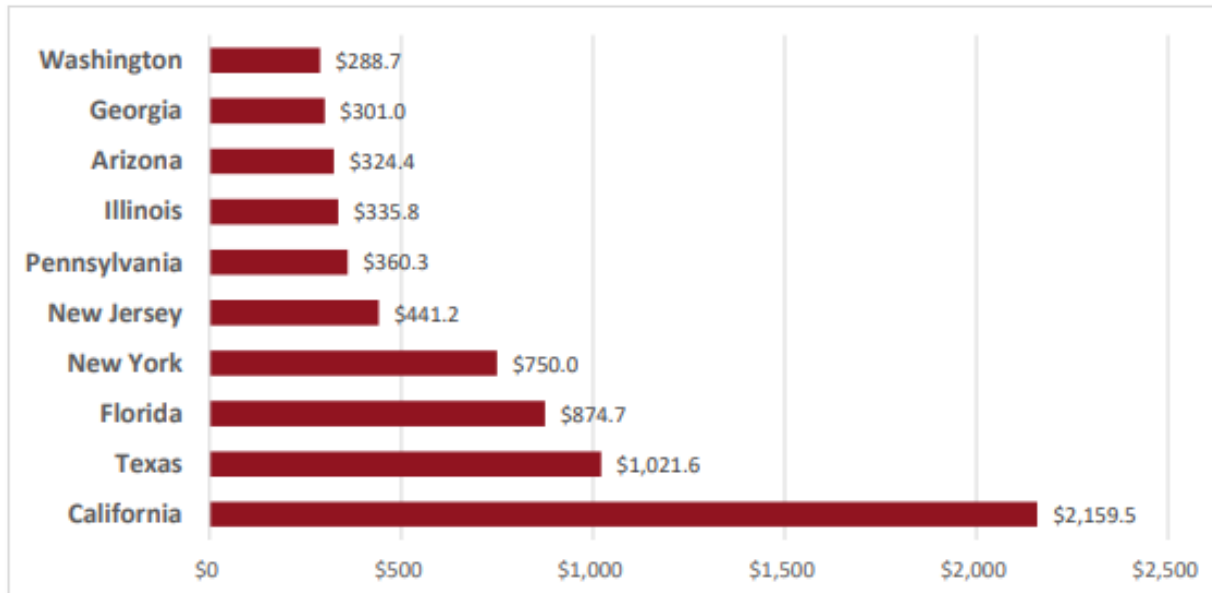
2023 – Top 20 International Victim Countries



2023 – Top 10 States



Top 10 States by Number of Victims



**Top 10 States by Victim Loss
(In Millions)**



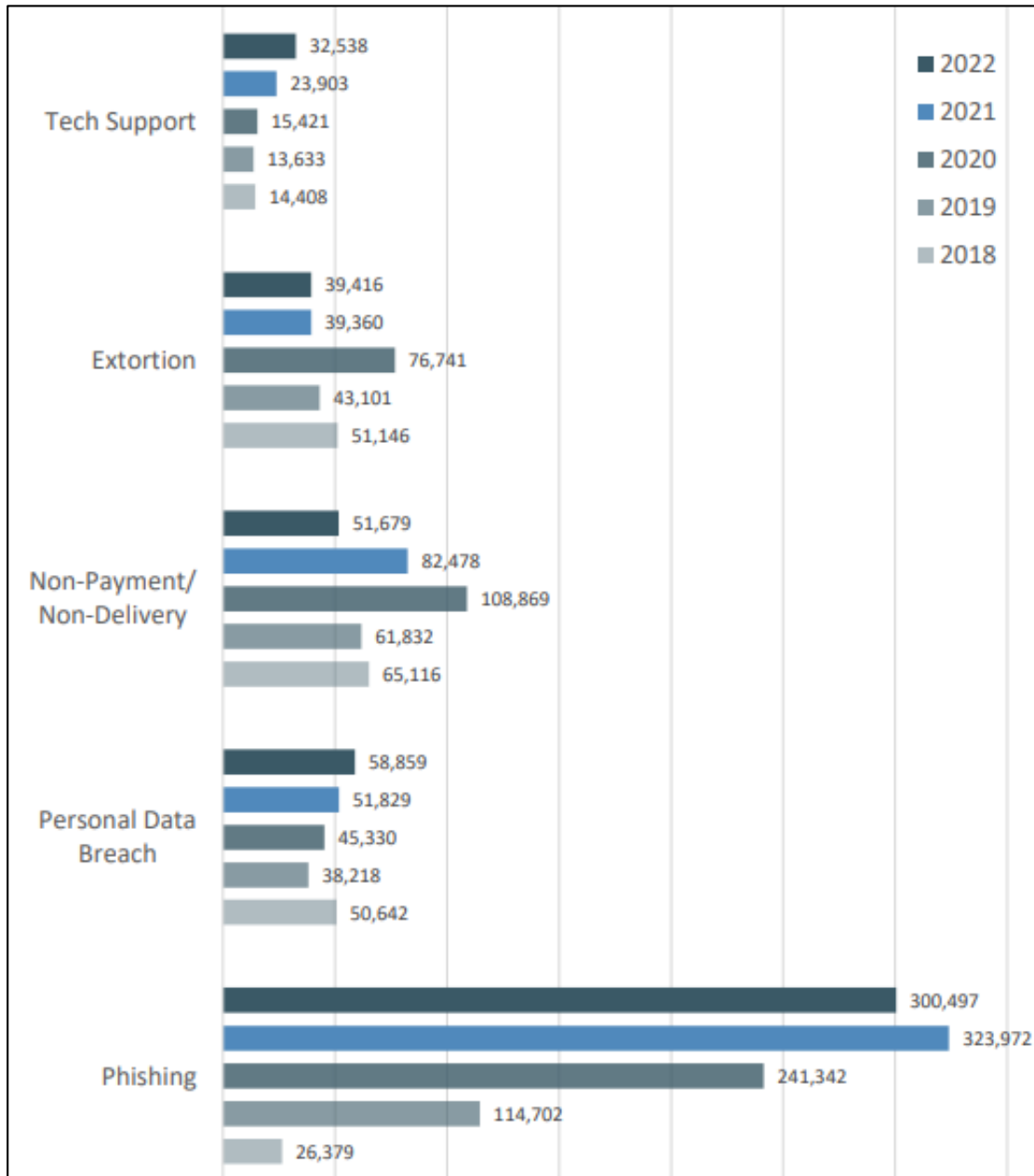
Overall State Statistics

Complaints per State*		
Rank	State	Complaints
1	California	77,271
2	Texas	47,305
3	Florida	41,061
4	New York	26,948
5	Ohio	17,864
6	Arizona	16,584
7	Pennsylvania	16,407
8	Illinois	15,783
9	Michigan	14,784
10	Washington	14,600
11	Georgia	13,917
12	Virginia	12,711
13	North Carolina	12,282
14	New Jersey	12,253
15	Colorado	11,475
16	Indiana	11,097
17	Massachusetts	9,915
18	Nevada	9,893
19	South Carolina	9,736
20	Maryland	9,717

Losses by State*		
Rank	State	Loss
1	California	\$2,159,454,513
2	Texas	\$1,021,547,286
3	Florida	\$874,725,493
4	New York	\$749,955,480
5	New Jersey	\$441,151,263
6	Pennsylvania	\$360,334,651
7	Illinois	\$335,764,223
8	Arizona	\$324,352,644
9	Georgia	\$301,001,997
10	Washington	\$288,691,091
11	Virginia	\$265,073,590
12	Massachusetts	\$235,890,173
13	North Carolina	\$234,972,238
14	Maryland	\$221,520,527
15	Michigan	\$203,445,988
16	Nevada	\$200,995,121
17	Ohio	\$197,365,326
18	Minnesota	\$193,949,414
19	Colorado	\$187,621,731
20	Indiana	\$162,259,036



Top 5 Crime Type Comparison



- Chart includes a victim loss comparison for the top five reported crime types for the years of 2018 to 2022.

2023 Crime Types

By Complaint Count

<i>Crime Type</i>	<i>Complaints</i>	<i>Crime Type</i>	<i>Complaints</i>
Phishing/Spoofing	298,878	Other	8,808
Personal Data Breach	55,851	Advanced Fee	8,045
Non-payment/Non-Delivery	50,523	Lottery/Sweepstakes/Inheritance	4,168
Extortion	48,223	Overpayment	4,144
Investment	39,570	Data Breach	3,727
Tech Support	37,560	Ransomware	2,825
BEC	21,489	Crimes Against Children	2,361
Identity Theft	19,778	Threats of Violence	1,697
Confidence/Romance	17,823	IPR/Copyright and Counterfeit	1,498
Employment	15,443	SIM Swap	1,075
Government Impersonation	14,190	Malware	659
Credit Card/Check Fraud	13,718	Botnet	540
Harassment/Stalking	9,587		
Real Estate	9,521		

Descriptors*

Cryptocurrency	43,653	Cryptocurrency Wallet	25,815
----------------	--------	-----------------------	--------



2023 Crime Types

By Complaint Loss			
Crime Type	Loss	Crime Type	Loss
Investment	\$4,570,275,683	Extortion	\$74,821,835
BEC	\$2,946,830,270	Employment	\$70,234,079
Tech Support	\$924,512,658	Ransomware*	\$59,641,384
Personal Data Breach	\$744,219,879	SIM Swap	\$48,798,103
Confidence/Romance	\$652,544,805	Overpayment	\$27,955,195
Data Breach	\$534,397,222	Botnet	\$22,422,708
Government Impersonation	\$394,050,518	Phishing/Spoofing	\$18,728,550
Non-payment/Non-Delivery	\$309,648,416	Threats of Violence	\$13,531,178
Other	\$240,053,059	Harassment/Stalking	\$9,677,332
Credit Card/Check Fraud	\$173,627,614	IPR/Copyright and Counterfeit	\$7,555,329
Real Estate	\$145,243,348	Crimes Against Children	\$2,031,485
Advanced Fee	\$134,516,577	Malware	\$1,213,317
Identity Theft	\$126,203,809		
Lottery/Sweepstakes/Inheritance	\$94,502,836		
Descriptors**			
Cryptocurrency	\$3,809,090,856	Cryptocurrency Wallet	\$1,778,399,729

A close-up, slightly blurred image of the American flag, showing the blue field with white stars and the red and white stripes. The flag is draped diagonally across the left side of the frame.

BASIC INTERNET SAFETY



Safe Clicking

- Between work and home, the average person clicks a mouse about 8000 times a day, or 40,000 times a week!
- Any one of those clicks can:
 - Steal or encrypt data
 - Steal your identity
 - Steal system resources
 - Steal your money

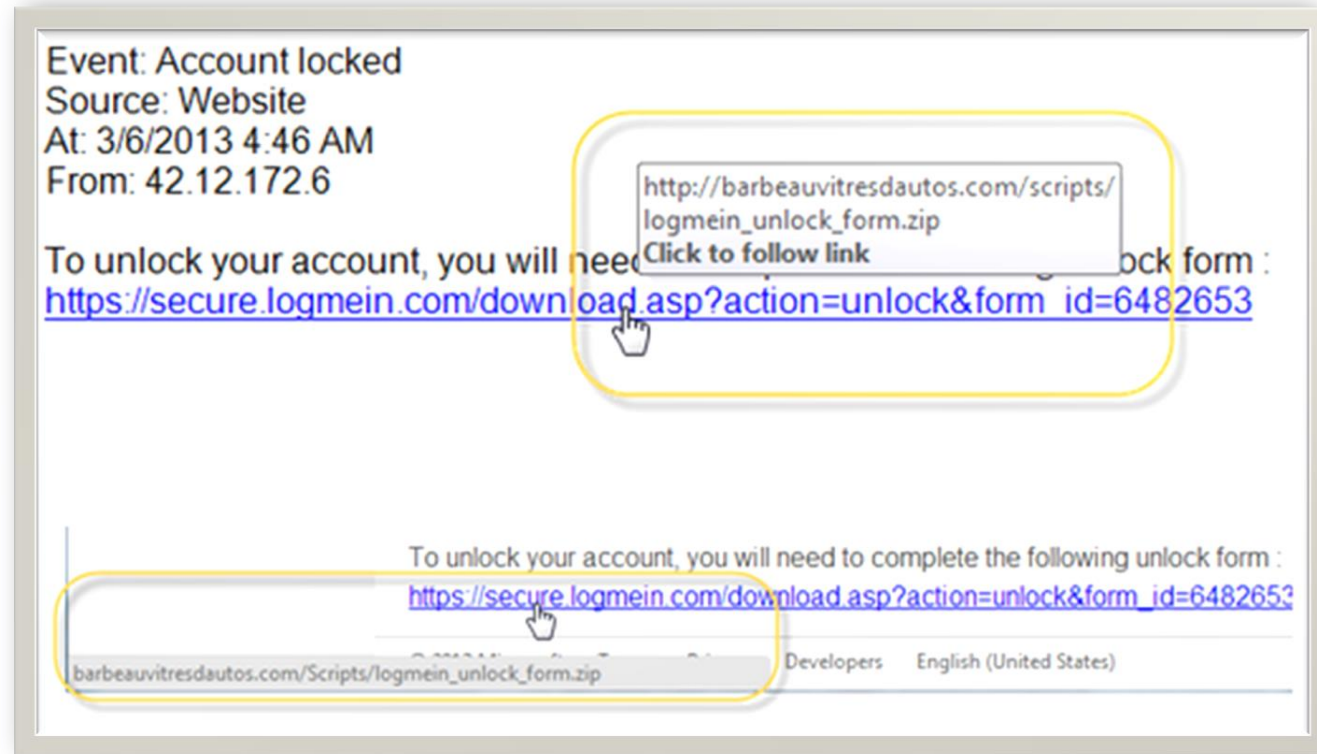


****The City of Colorado Springs has approximately 3,000 city accounts, which means 24,000,000 clicks per week, and 96,000,000 clicks per month.**



URLs

- Uniform Resource Locators (URLs).
- Cyber Criminals use links to trick you into downloading malicious software or steal information.
- Hover your mouse over a link to display the destination address.



Attachments

- Be wary of archives – hackers try to hide malicious files in these.
- Office files with Macros – don't click on “enable content” unless you are certain the file can be trusted.
- Don't trust files with double extensions (the one that matters is the last one).



.zip



.rar



.7z



.docm



.xlsm



.pptm



file.gif.exe

Take care of your own tech security

- Keep your computer and device security updated
- Don't use easily-hacked or common passwords
- Be wary of WiFi connections, hotspots, or unknown LANs
 - Don't automatically connect to networks
- Consider a VPN (Virtual Private Network) connection



A close-up, slightly blurred image of the American flag, showing the blue field with white stars and the red and white stripes. The flag is draped diagonally across the left side of the frame.

THE SCAMS



What is a Scam?

- A dishonest trick used to cheat someone out of something, especially money.
- After building trust with a victim, the scammer will defraud or steal from the victim.
- Scammers don't care about you; they only want cooperation to gain something from you.
- Can be in-person, over the phone, via email, or by mail.
- Often use Social Engineering and Phishing.



Four Signs It's 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.



What is Social Engineering?



Email Phishing

What is Phishing?



Email Phishing

What is Phishing?

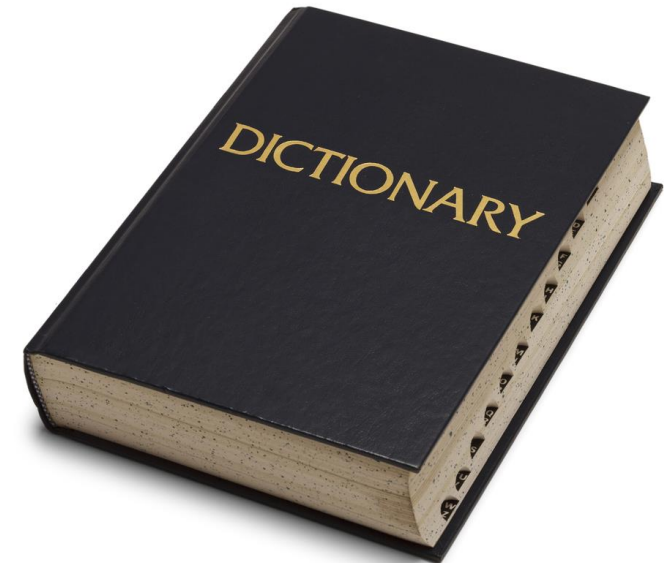
- The fraudulent practice of sending emails purporting to be from reputable companies, organizations, or service providers in order to induce individuals to reveal personal information, such as passwords and credit card numbers or to send money.



Email Phishing

How to recognize Phishing?

- Legit companies don't request your sensitive information!
- Legit companies usually call you by your name.
- Legit companies know how to spell.
- Legit companies don't force you to their website.
- Legit companies don't send unsolicited attachments.



Clues for spotting fake emails/profiles

Scammers can easily fake an official-looking email, using the same logo and design as the real company.

! RE: TJ2034SD Digital imaging accessories URGENT

To Whom it May Concern,

The Customs Office formally presents a notification regarding the immediate suspension of your consign-

Feigns a sense of urgency so victims don't inspect closely

Uses a generic greeting and doesn't address you or your organisation directly



Government of Australia
Office of Revenue Affairs

The organisation or company might not even exist

..Pursuant to article 107, section 39, sub section iv of the *1998 INTERNAL REVENUE ACT*, said Forces and Persons are hereby required to..

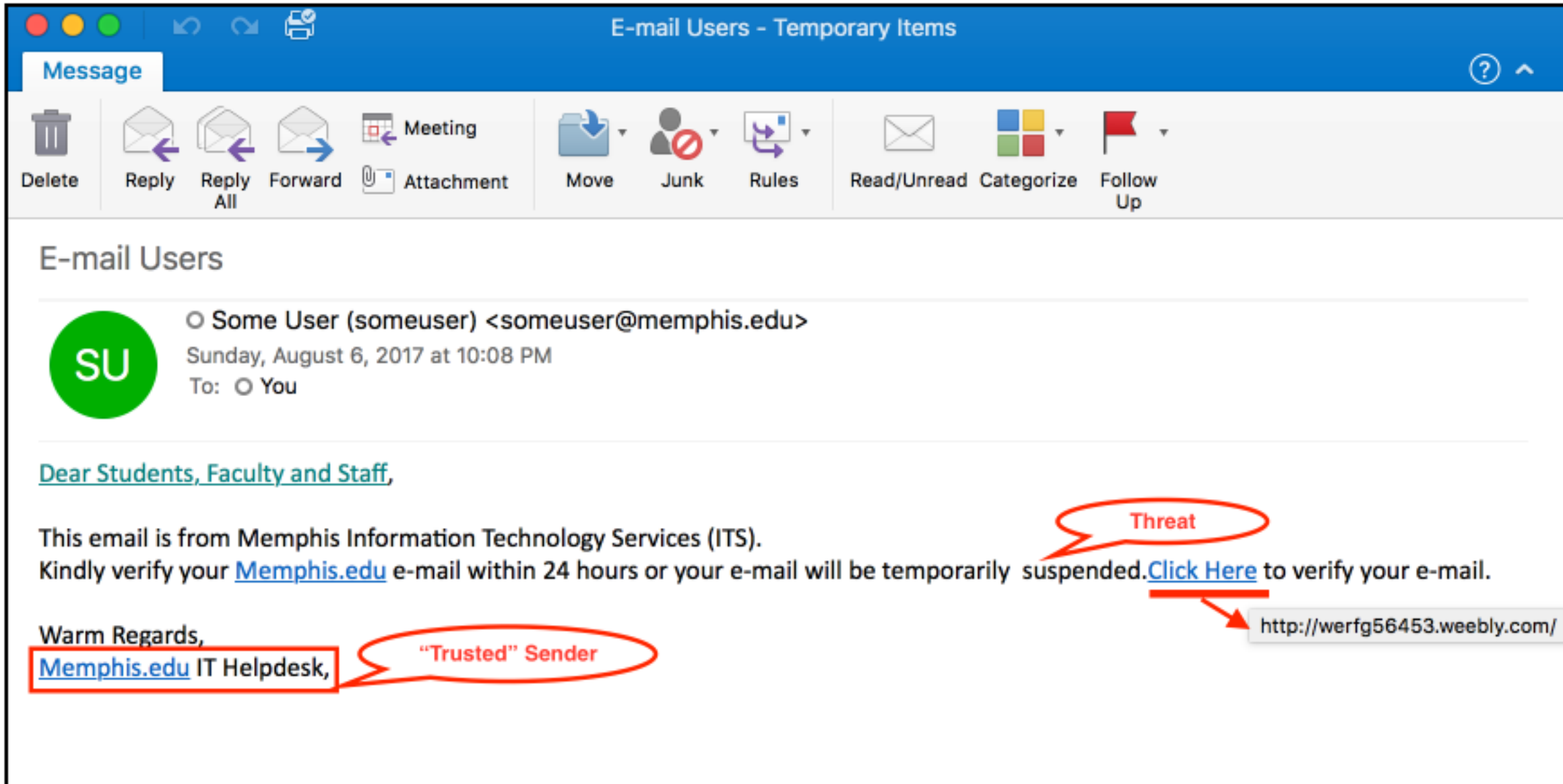
..has affected the delivery of a parcel containing some valuables and **sum large amount** on your package in favor of the above mentioned beneficiary address.

May contain official sounding language to make it look more genuine

Poor grammar, spelling and punctuation



Use the mouse pointer to hover over links...



The screenshot shows an email client window titled "E-mail Users - Temporary Items". The "Message" tab is active. The email is from "Some User (someuser) <someuser@memphis.edu>" dated "Sunday, August 6, 2017 at 10:08 PM". The email body contains the following text:

[Dear Students, Faculty and Staff,](#)

This email is from Memphis Information Technology Services (ITS).
Kindly verify your [Memphis.edu](#) e-mail within 24 hours or your e-mail will be temporarily suspended. [Click Here](#) to verify your e-mail.

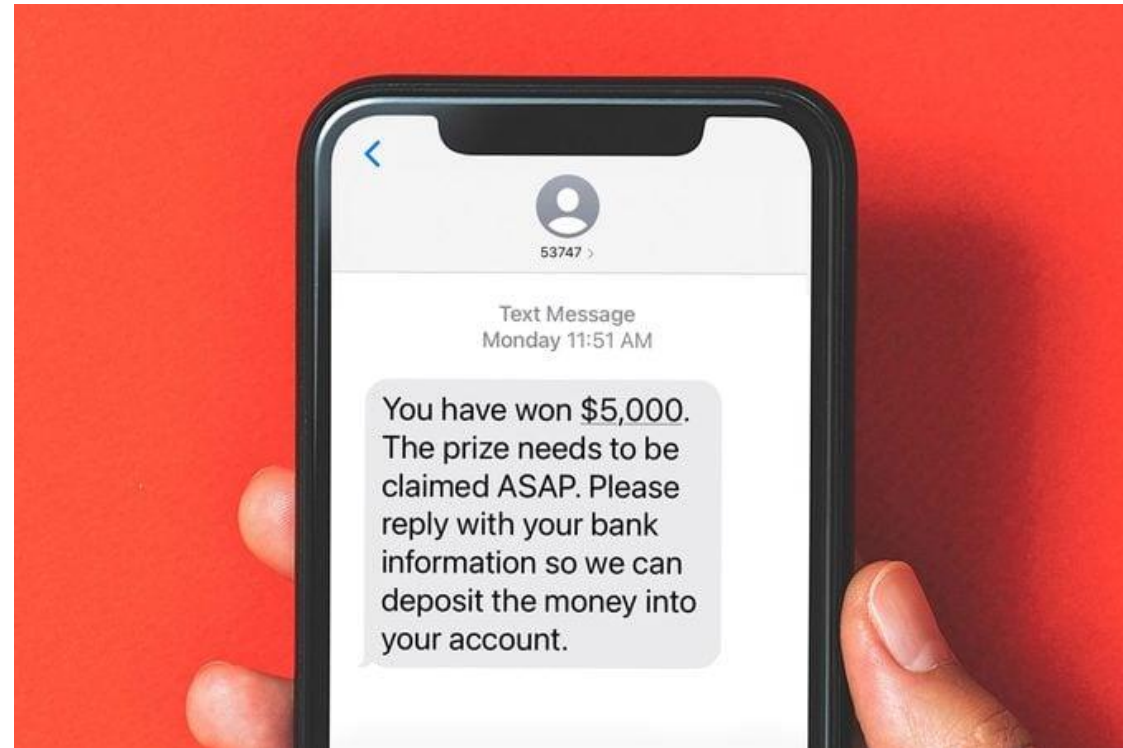
Warm Regards,
[Memphis.edu](#) IT Helpdesk,

The email also includes a red speech bubble pointing to the "Click Here" link with the text "Threat" and another red speech bubble pointing to the "Memphis.edu" link with the text "Trusted" Sender". The "Click Here" link is underlined and points to the URL <http://werfg56453.weebly.com/>.

Smishing

What is Smishing?

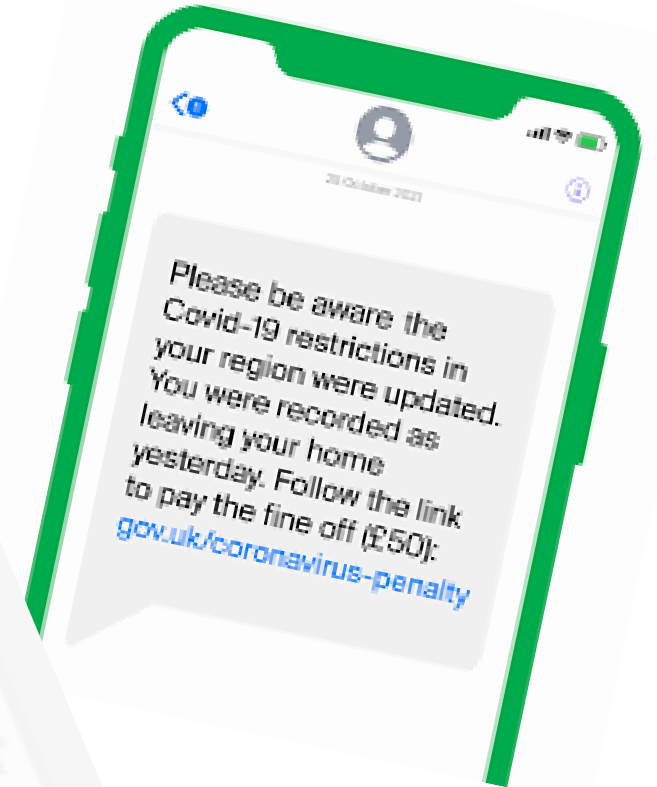
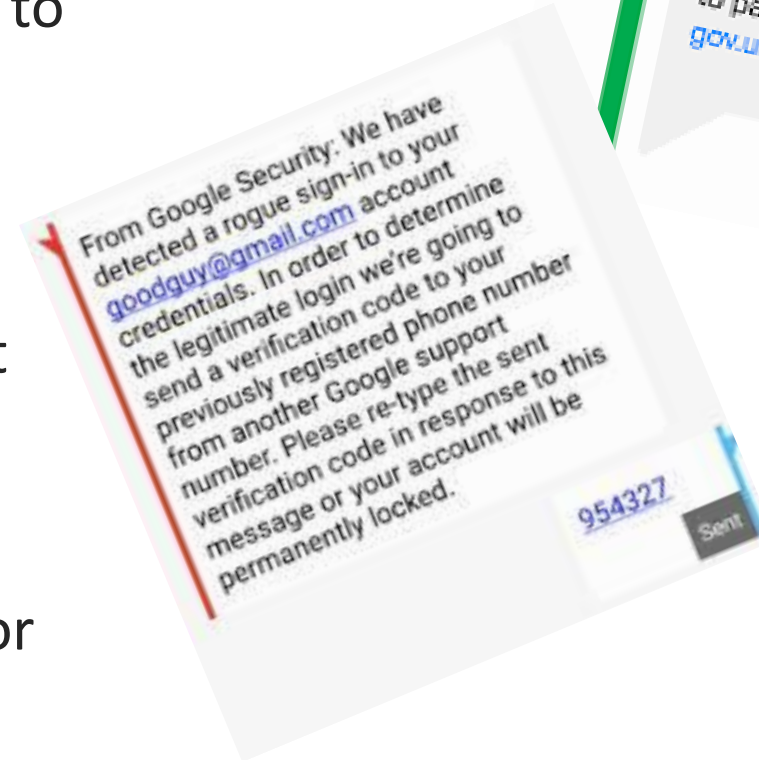
Smishing (SMS Phishing) – “The fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information.”



Smishing

Smishing Warning Signs

- A text message requests personal information, such as your Social Security number or an online account password.
- The message asks you to click a link to resolve a problem, win a prize or access a service.
- The message claims to be from a government agency. Government bodies almost never initiate contact with someone by phone or text, according to the FCC.
- The text offers coronavirus-related testing, treatment or financial aid, or requests personal data for contact tracing.



Smishing (Text Scam) Samples

< 117 +1 (206) 304-2917 >

Text Message
Today 8:55 AM

██████, urgent
notification
regarding the USPS
delivery S46K5 from
04/04/2020. Go to:
[m9sxv.info/
lbJ0nVq6Ft](http://m9sxv.info/lbJ0nVq6Ft)



+1 (214) 384-1289 >

Text Message
Sun, Mar 21, 4:21 PM

Tonia, you still have \$130
Amazon Bonus credit:
v4fzc.info/CKQp0ZDGkv See
what you can buy before it
expires on 03/22 [v4fzc.info/
CKQp0ZDGkv](http://v4fzc.info/CKQp0ZDGkv)



Smishing (Text Scam) Samples

- Did you receive a text message from yourself?



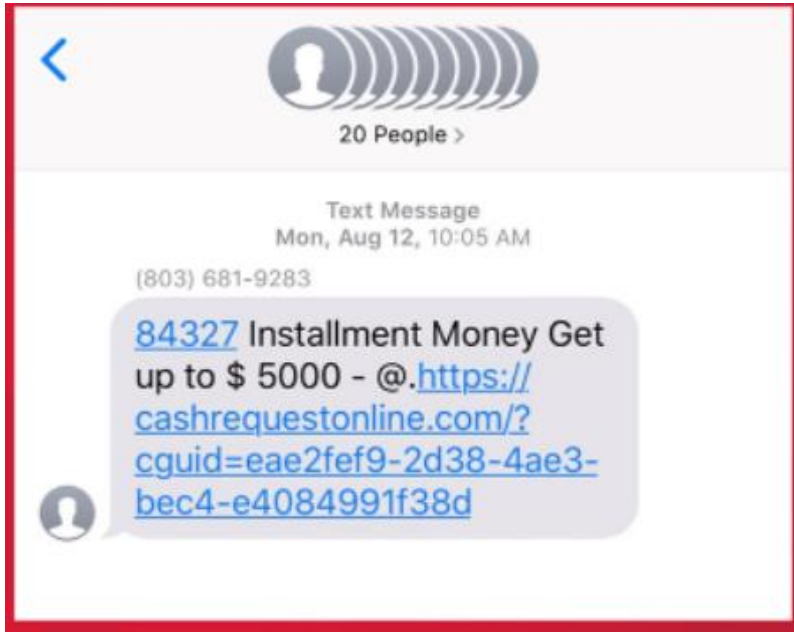
Text Message
Today 9:14 AM

Free Msg: Your bill is paid for March.
Thanks, here's a little gift for you:
um3yy9.rczt35.xyz/1clh

- Did you get a random picture from an unknown person?



Group Text Message Scams



Q: Does replying with **“STOP”** to unwanted text messages really work?

A: NO! If the message is clearly a scam or an attempt to “phish” information from you, replying with **“STOP”** is not only ineffective, it’s also an invitation to be bombarded by lots of junk messages in the future.

When they receive the **“STOP”** response from you, they will know that your phone number is both active and responsive. This will lead to your number getting placed on an active list that is sold and resold countless times amongst the bad actors.



How to Block Unwanted Group Text Messages

iPHONE:

Open the text message you received. Tap the phone number/group at the top of the screen and then tap the **Info** button. At the next screen, select **Block this Caller** and then tap **Block Contact** to confirm.

ANDROID:

Navigate to the group chat. Tap on the three vertical dots in the upper right corner to open the group text's setting page. Select "People & Options." At this point, you should see a list of all the group text members. Find the original number for the text and tap on their name/number and select "block."



Social Engineering - Vishing



Cryptocurrency

- Cryptocurrency is becoming a preferred payment method for all types of scams – SIM Swaps, Tech/Customer Support fraud, Employment schemes, Romance scams, and even some Auction fraud.
- It is extremely pervasive in Investment scams, where losses can reach into the hundreds of thousands of dollars per victim.
- The largest losses among victims over 60 are cryptocurrency-related Investment scams.

USE OF CRYPTOCURRENCY KIOSKS REPORTED IN IC3 COMPLAINTS – 2023

Age Range	Complaints	Losses
Under 20	65	\$252,198
20 - 29	416	\$3,529,680
30 - 39	451	\$8,651,706
40 - 49	391	\$9,634,346
50 - 59	476	\$11,409,372
Over 60	2,676	\$124,332,127

TOP FIVE CRIME TYPES INVOLVING CRYPTOCURRENCY KIOSKS IN IC3 COMPLAINTS -- 2023

Crime Type	Percent of Total Complaints
Tech Support	46%
Extortion	17%
Government Impersonation	10%
Investment	8%
Confidence/Romance	6%



Common Types of Frauds/Scams

- Romance scam
- Tech Support scam
- Grandparent scam
- Government Impersonation scam
- Sweepstakes/charity/lottery scam
- Home Repair scam
- Family/Caregiver scam

Many more!



A close-up, slightly blurred image of the American flag, showing the blue field with white stars and the red and white stripes. The flag is draped and occupies the left side of the frame.

IDENTITY THEFT



What is Identity Theft?

- When someone *STEALS* some piece of your personal information and uses it without your knowledge to commit fraud or theft
- When someone *PRETENDS* to be you to obtain credit, cash or goods or to commit other crimes
- It is a *CRIME* with two victims, the lender or service provider and the person who had their identity stolen



What are the effects of Identity Theft?

- On average, victims spend 6 months and 200 hours and \$1,300 in out-of-pocket expenses to clear their names
- Can negatively impact credit score
- ID theft affects victims of all ages, races and economic status



ID Theft trends in Colorado

Most information is taken by opportunistic criminals

- Vehicle break-in (BMV)
- Unsecured or stolen mail
- Personal belongings
- Receipts, records, and other documents
- Personal Identifying Information (PID)



Prevention

- Never leave receipts and shred old or unnecessary documents
- Promptly remove your mail from your mailbox
- Take outgoing mail to the post office or mail drop
- Empty your wallet or purse of extra items
- Memorize your social security # and all of your passwords
- DO NOT write down personal numbers or passwords and never give out personal information over the phone, internet or for a sweepstakes
- Consider using a reputable password generator or storage app



A close-up, slightly blurred view of the American flag, showing the blue field with white stars and the red and white stripes. The flag is draped diagonally across the left side of the frame.

PROTECT YOURSELF!



Be your own best defense!

- Recognize scam attempts and end all communication with the perpetrator.
- Search online for the contact information (name, email, phone number, addresses) and the proposed offer.
- Resist the pressure to act quickly!
- Be cautious of unsolicited phone calls, mailings, and door-to-door services offers.
- Never give or send any personally identifiable information, money, jewelry, gift cards, checks, or wire information to unverified people or businesses!



Protect your devices and your information!

- Make sure all computer anti-virus and security software and malware protections are up to date.
- Disconnect from the internet and shut down your device if you see a pop-up message or locked screen.
- Be careful what you download!
- Delete sensitive information from, and dispose of, old devices.
- Take precautions to protect your identity if a criminal gains access to your device or account.



Report a Crime

- Always remember: STAY ALERT! Don't be a victim.
- Please report suspected crimes via 911 (emergency only), 719-444-7000 (non-emergency), or online @ <https://coloradosprings.gov/police-department/page/report-crime-online?mlid=4841> (minor crimes only).
- Report to www.ic3.gov
- Contact your bank/credit card and credit reporting agencies.



Resources

- www.FBI.gov
- www.ic3.gov
- <https://reportfraud.ftc.gov/#/>
- www.coag.gov (Colorado Attorney General - Scams)
- www.consumerfinance.gov
- www.ncoa.org (National Council on Aging)
- www.justice.gov
- www.ovd.ojp.gov (Office for Victims of Crime)
 - National Elder Fraud Hotline 1-833-372-11)
- www.stopfraudcolorado.gov
- www.consumer.ftc.gov



The Social Security Administration says it best...





QUESTIONS?



Contact your Crime Prevention Officer for additional information or with questions.

