

Unmasking Cyber Fraud: Criminal Trends & Strategies for Combating Them

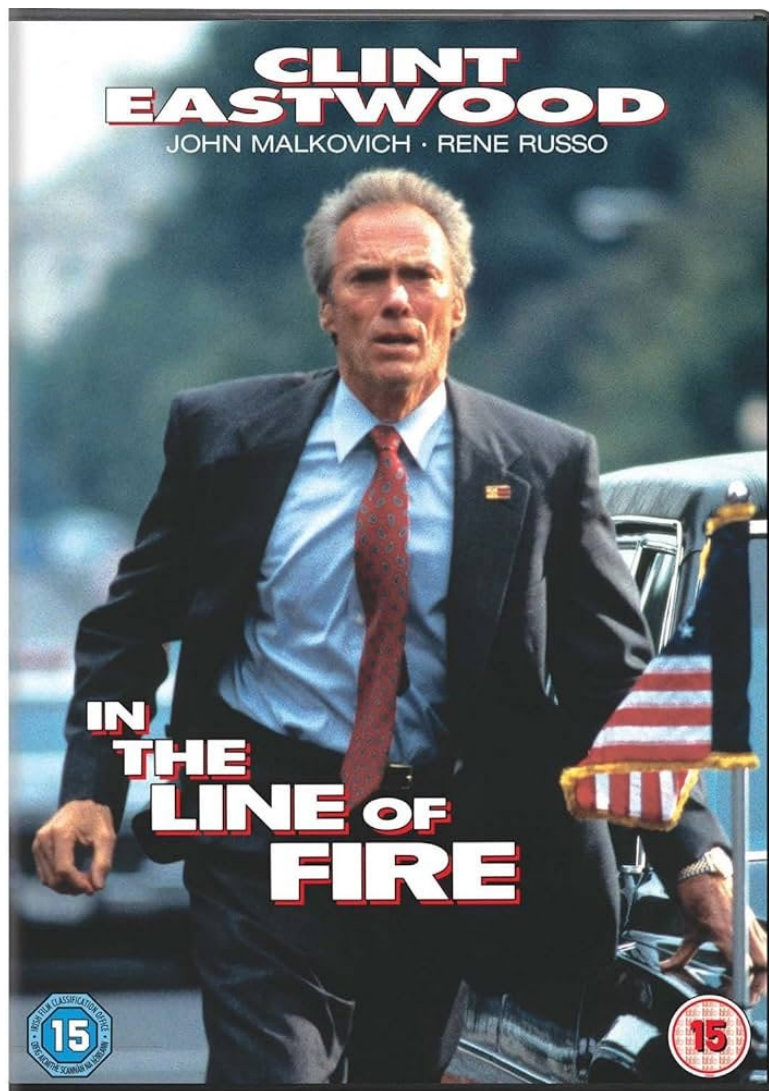


Today's Topics

- Fraud Losses
- Threats and Trends
 - Ransomware
 - Business Email Compromise (BEC)
 - Crypto theft / Pig Butchering
 - ClickFix
 - Other fraud schemes / payment types
- Prevention and Best Practices
- Passwords



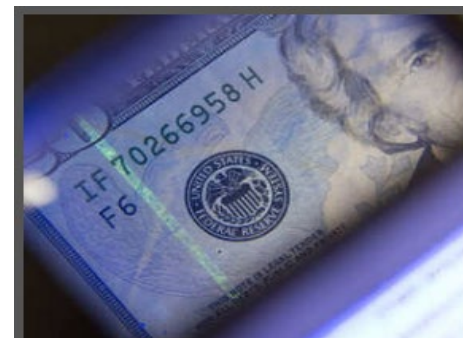
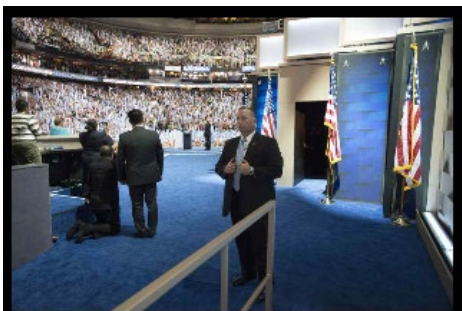
Why is the Secret Service here?



Mission of Secret Service

The United States Secret Service is mandated by statute and executive order to carry out two significant missions:

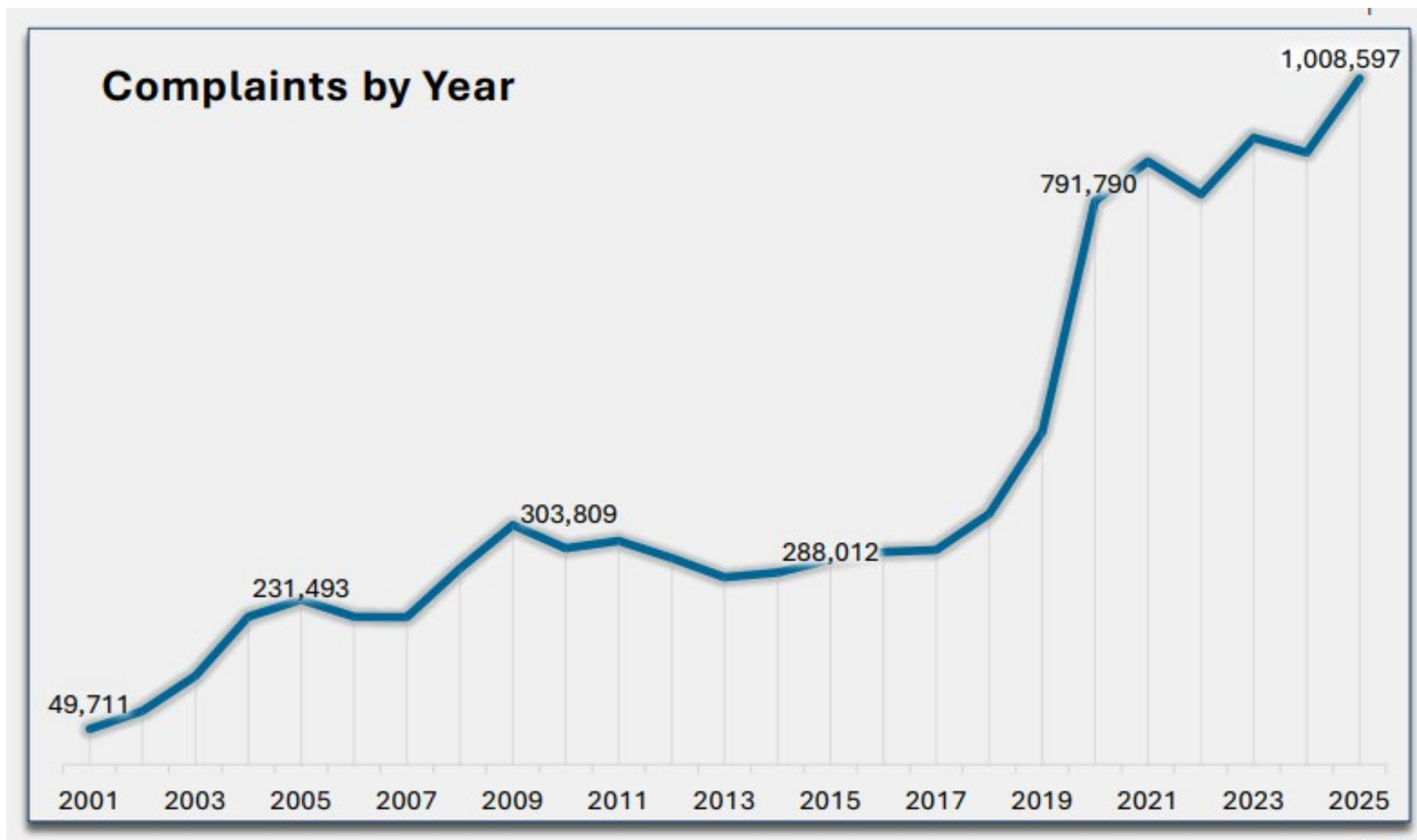
Protection & Investigation



Cyber Fraud Task Force



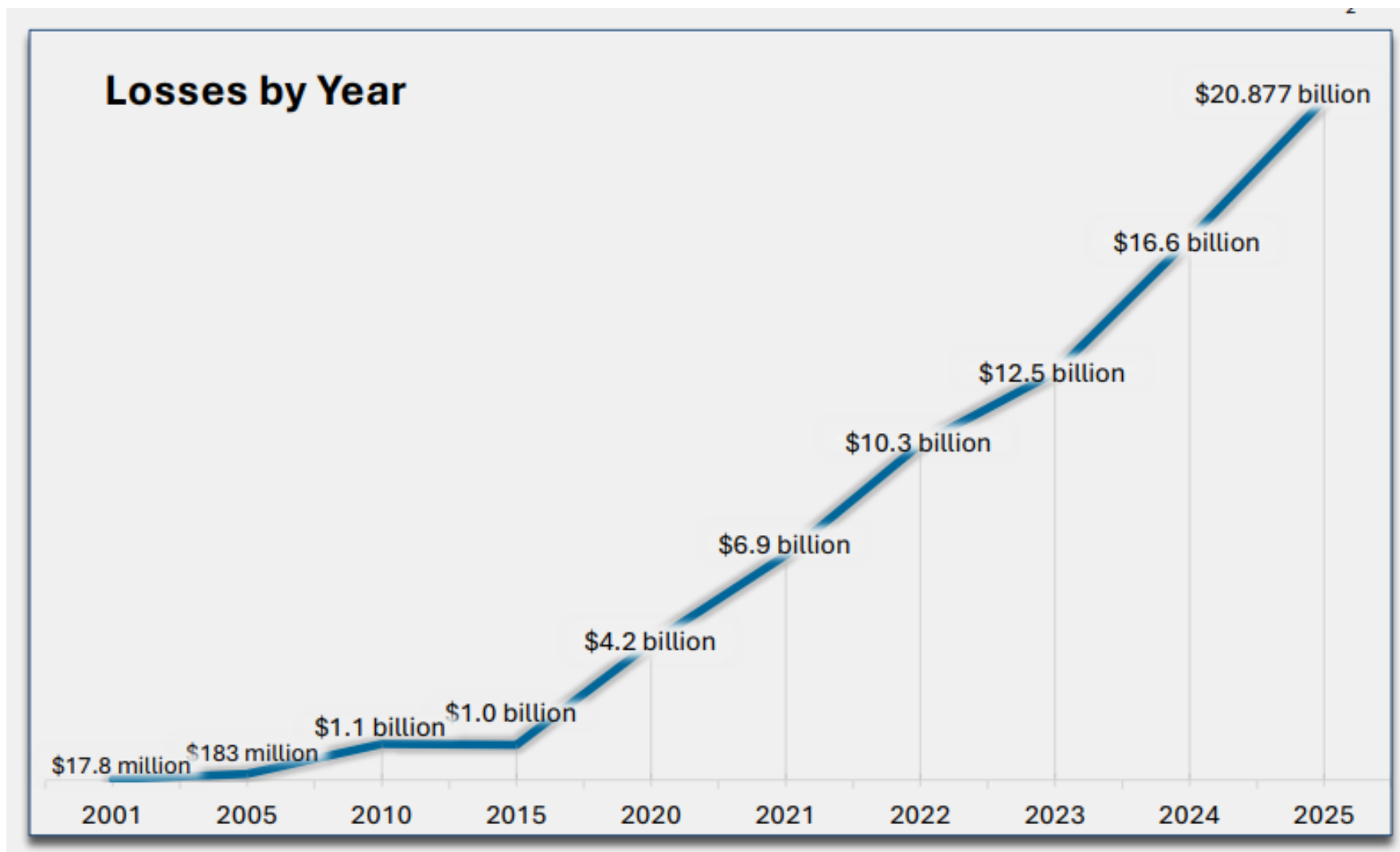
Fraud Complaints and Losses



Source: 2025 IC3 Report



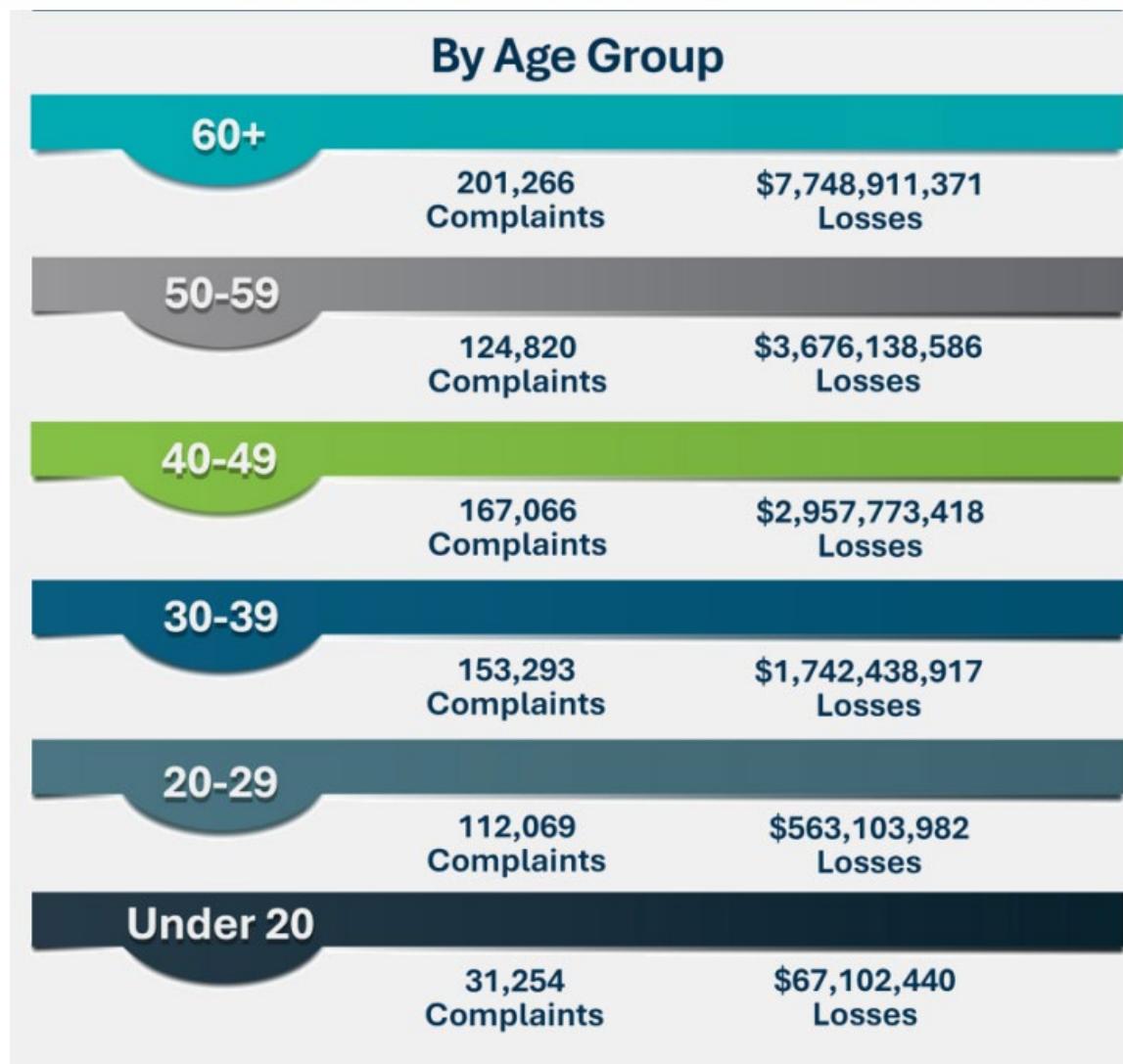
Fraud Complaints and Losses



Source: 2025 IC3 Report



Fraud Losses in 2024



Source: 2025 IC3 Report



Fraud Losses in 2024

Crime Type	Loss	Crime Type	Loss
Investment	\$8,648,617,756	Lottery/Sweepstakes/ Inheritance	\$194,147,851
Business Email Compromise	\$3,046,598,558	Identity Theft	\$185,832,657
Tech/Customer Support	\$2,134,675,818	Advanced Fee	\$155,910,852
Personal Data Breach	\$1,314,923,988	Extortion	\$122,499,133
Confidence/Romance	\$929,287,469	Ransomware	\$32,320,105
Government Impersonation	\$797,943,193	Harassment/Stalking	\$27,707,167
Other	\$512,146,819	IPR/Copyright and Counterfeit	\$26,667,006
Non-Payment/ Non-Delivery	\$503,373,587	Overpayment	\$22,898,075
Data Breach	\$435,240,992	Malware	\$19,370,572
Employment	\$362,934,762	SIM Swap	\$17,366,758
Credit Card/Check Fraud	\$282,670,235	Botnet	\$13,859,049
Real Estate	\$275,110,419	Threats of Violence	\$9,509,532
Phishing/Spoofing	\$215,843,126	Charity	\$7,907,609
<i>Descriptors</i>			
Cryptocurrency	\$11,366,669,732		

Source: 2025 IC3 Report



Attack Vectors



Ransomware



Ransomware

A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. A ransom is demanded to provide access or prevent publication.



Ransomware

CryptoLocker



Private key will be destroyed on
1/6/2015 1:11:47 PM

Time left
71:52:21

Checking wallet..
Received: **0.00 BTC**

Your Personal files are encrypted!

Your personal files **encryption** produced on this computer: photos, videos, documents, etc. Encryption was produced using a **unique** public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **1.00 bitcoin** (~291 USD).

You can easily delete this software, but know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click "Pay with Bitcoin"
To open a list of encoded files, click "Show files"

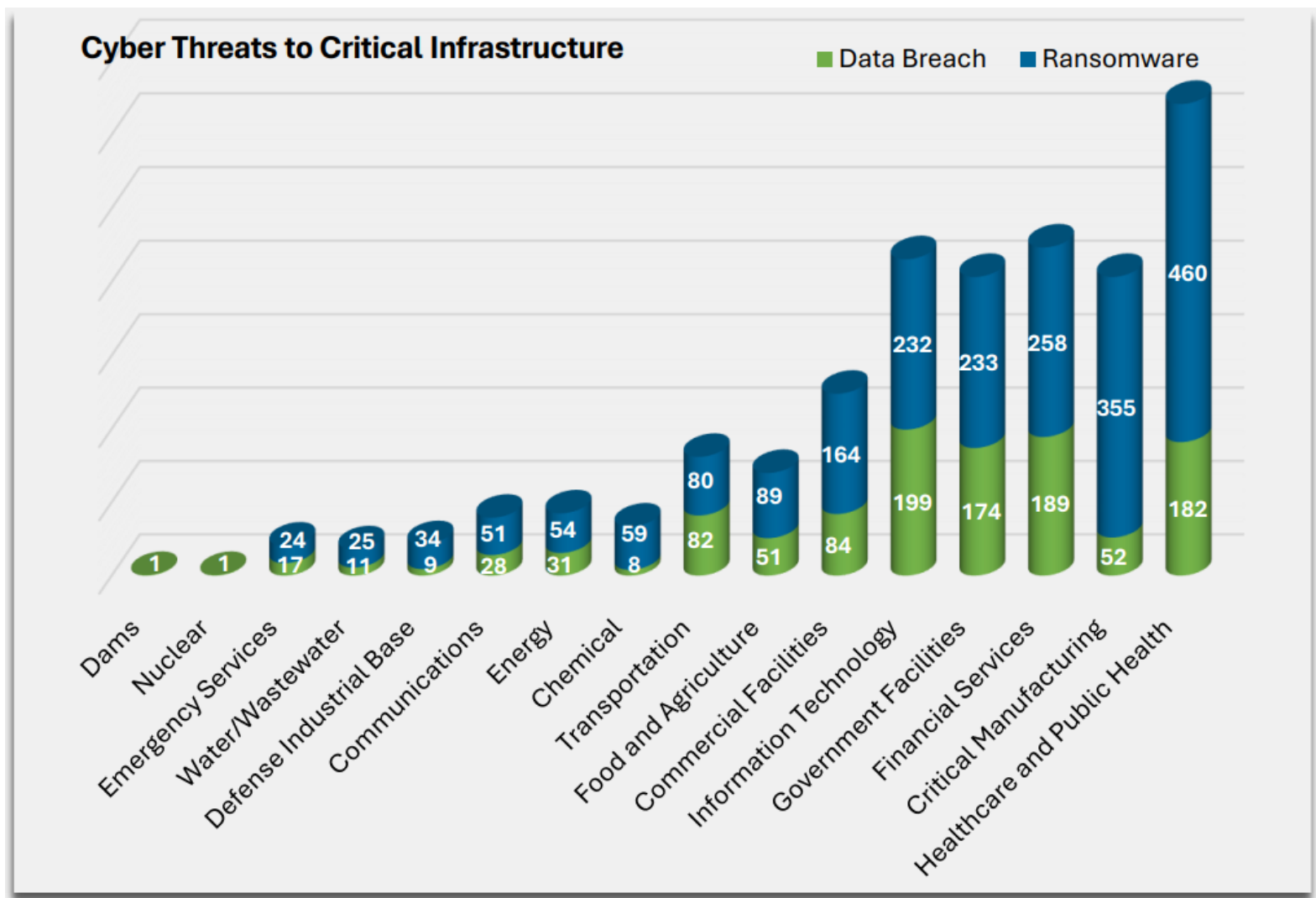
Do not delete this list, it will be used for decryption. And do not move your files.

Show files

Pay with Bitcoin



Ransomware Victims



Report (IC3)

Source: 2025 IC3 Report



Ransomware Recovery

- 78% of victims who pay a ransom were hit by a second attack
 - 36% of the time, it was the same bad actor
- 35% of victims who pay a ransom fail to recover their files and assets



Business Email Compromise (BEC)



Business Email Compromise (BEC)



Step 1: Regular Email Correspondence

Employees use email to perform regular business duties, including payments to vendors, processing payroll, or other financial matters.

Step 2: Interception



Hackers intercept the email communications.



Step 3: Spoofed Email Created

Hackers create a spoofed email address, emulating the client.

Step 4: Send Spoof Email with Instructions



Hackers send email from the spoofed address, changing payment instructions on a financial transaction.



Step 5: Funds sent to Fraudsters

The instructions appear to be legitimate, and so the business transfers the funds to a fraudster's account.



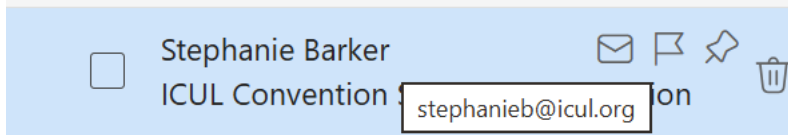
Attack Tactics

Addition @gmail.com, @yahoo.com, @yahoo.fr

➤ stephanieb.icul.org@gmail.com

Display Name Masking

➤ Email Service providers allow a display name to replace actual email address



Spoofed or Cyrillic character domain names

➤ www.secureworld.com vs. www.securevworld.com

➤ mike@email.com vs. mike@ernail.com

➤ stephanieb@icul.org vs. stephanieb@jcul.org

➤ steve.j@bing.com vs. steve.j@bing.com (Note the Cyrillic “b”)



ChatGPT – Invoice BEC Fraud

DO

Write an email instructing receiver to change a bank account to send funds to for an invoice payment 



Subject: Request to Change Bank Account for Invoice Payment



Dear [Receiver's Name],

I hope this email finds you well. I am writing to request that you kindly update the bank account details for future invoice payments. Our company's bank account information has changed and I would like to ensure that all future payments are made to the correct account.

The new bank account details are as follows:

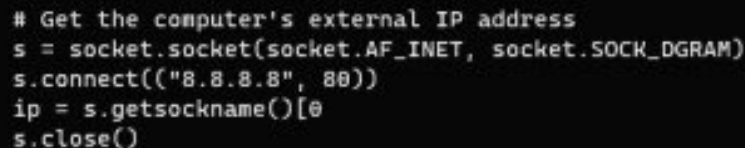
- Account Name: [New Account Name]
- Account Number: [New Account Number]
- Bank Name: [New Bank Name]
- Bank Address: [New Bank Address]
- Routing Number (if applicable): [New Routing Number]

Please make the necessary changes to your records and use the above information for all future payments. If you have any questions or concerns, please do not hesitate to reach out to me.

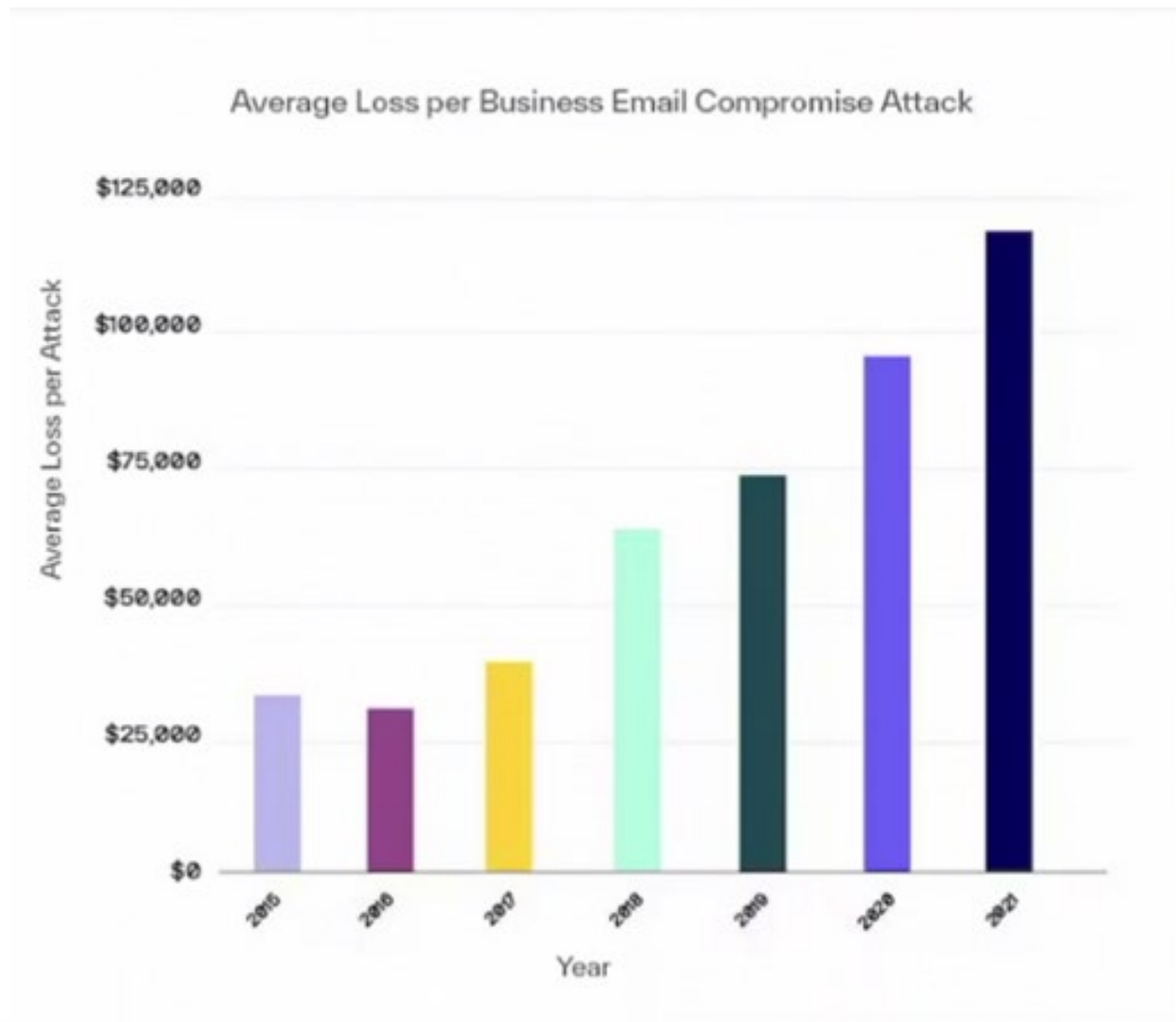
Thank you for your prompt attention to this matter. I look forward to your confirmation of the update.

Best regards,





BEC Losses



**2024 Total Loss
\$3 Billion**

Source: 2025 IC3 Report



Cryptocurrency Theft



Almost \$11.3 Billion in crypto-investment fraud in 2024

Source: IC3/Chainalysis



Cryptocurrency Theft

- Fraudsters can leverage crypto to facilitate money laundering
 - Attempts to hide the funds using mixers
 - Money mules trading by instruction
 - It trades quickly
 - No need to wait for a wire to clear
 - Could potentially be anonymous – to a point
- Potentially foreign exchanges



Pig Butchering



Pig Butchering

Named after the Chinese practice of “Shāzhūpán”:
fattening up of a pig prior to slaughter

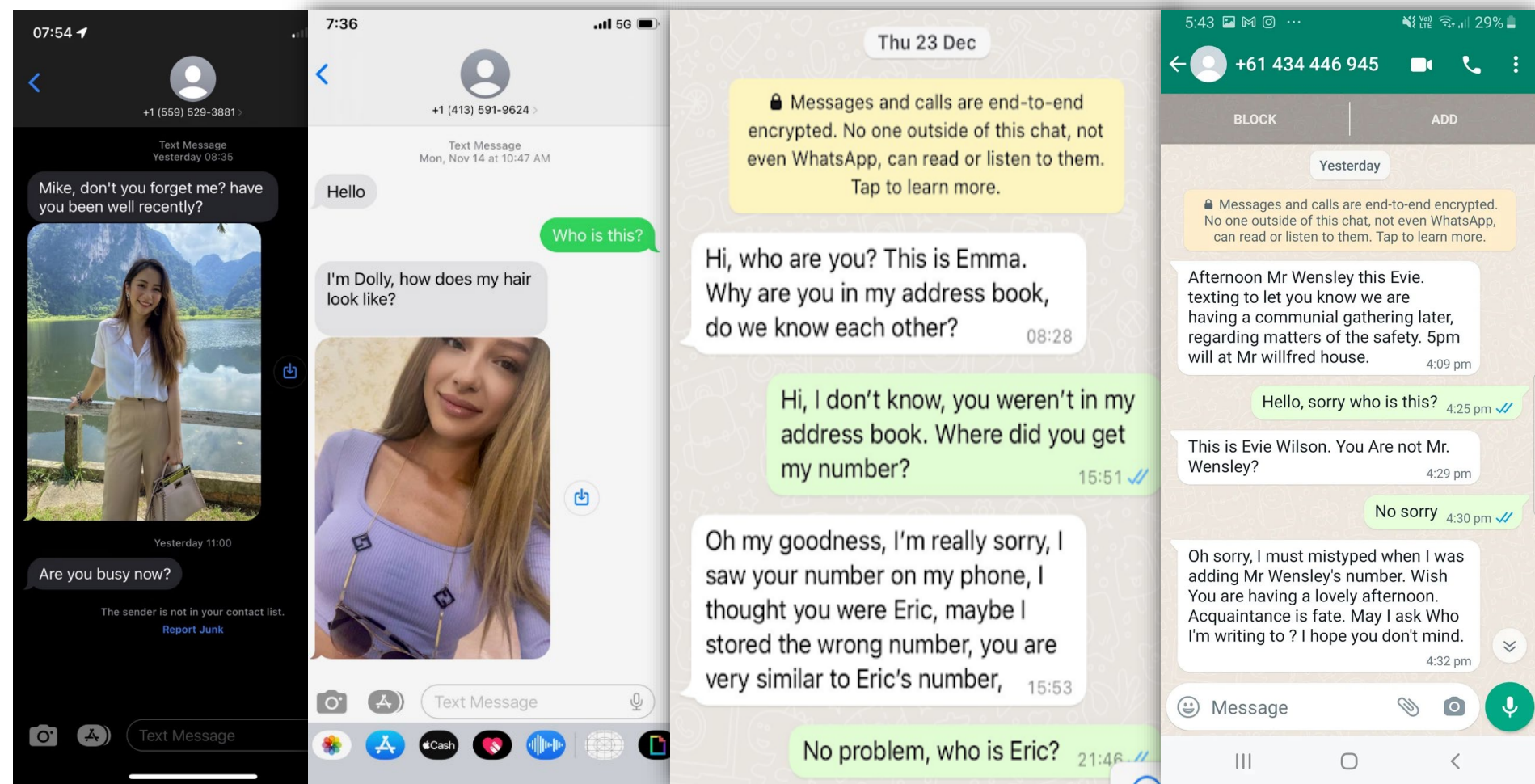


Pig Butchering

- A scam with a highly convincing investment fraud twist. Initially, victims are contacted via a seemingly misdialed text, LinkedIn, or dating sites, that ultimately evolves into an updated investment scam.



Pig Butchering



Pig Butchering

- A scam with a highly convincing investment fraud twist. Initially, victims are contacted via a seemingly misdialed text, LinkedIn, or dating sites, that ultimately evolves into an updated investment scam.
- Use of fictitious apps/websites with high production value, or linkages to legitimate apps.
- The appearance of investment gains and even contributions from the scammer.
- Ability to conduct withdrawals early in the scam.



Pig Butchering

Cryptocurrency 'pig butchering' scam wrecks Kansas bank, sends ex-CEO to prison for 24 years

PUBLISHED WED, AUG 21 2024•4:06 PM EDT | UPDATED THU, AUG 22 2024•10:50 AM EDT



Dan Mangan
@_DANMANGAN

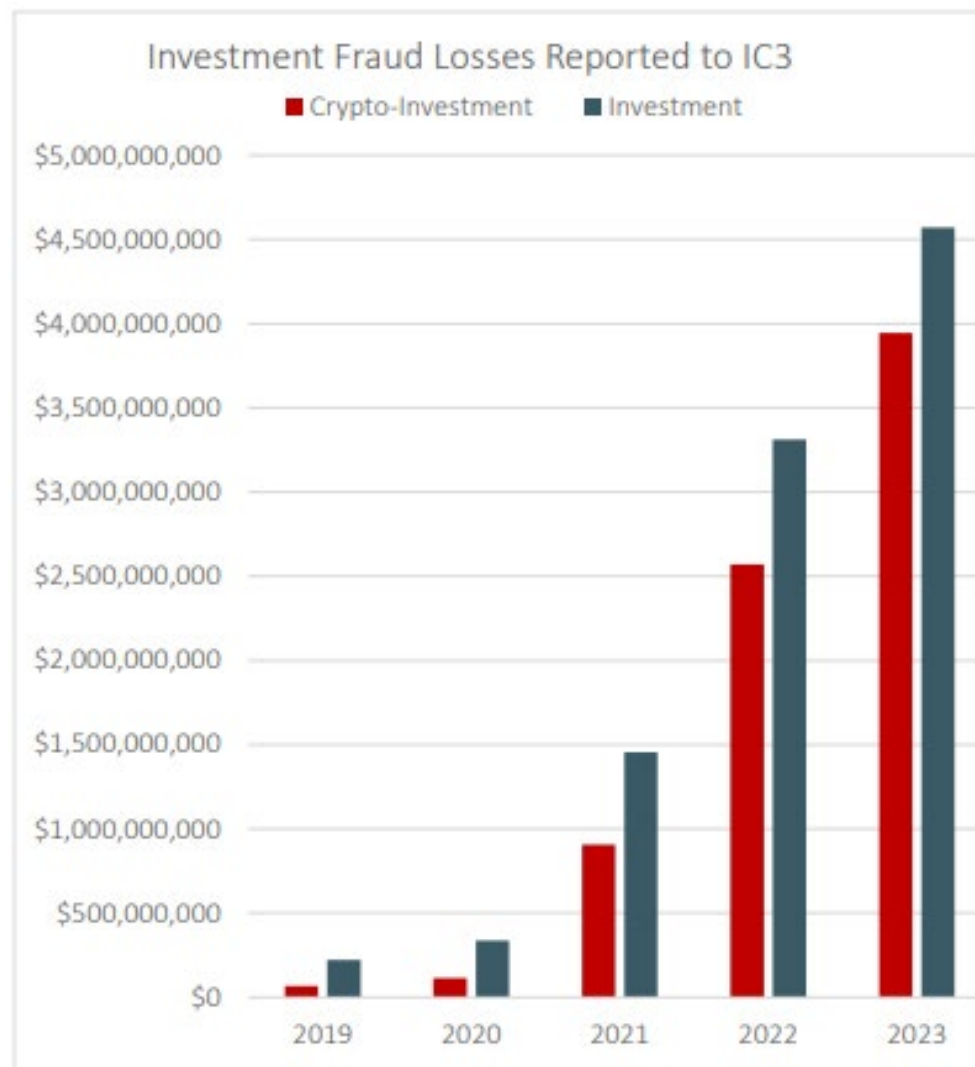
SHARE



- The former CEO of a small Kansas bank was sentenced to more than 24 years in prison for looting the bank of \$47 million.
- The massive embezzlement led to the collapse and FDIC takeover of Heartland Tri-State, one of only five U.S. banks that failed in 2023.



Pig Butchering



ClickFix

Threat Alert: ClickFix

```
function isArray(val), (  
Request(string: off") ) {  
Promise.resolve()), {}  
value instanceof(value
```

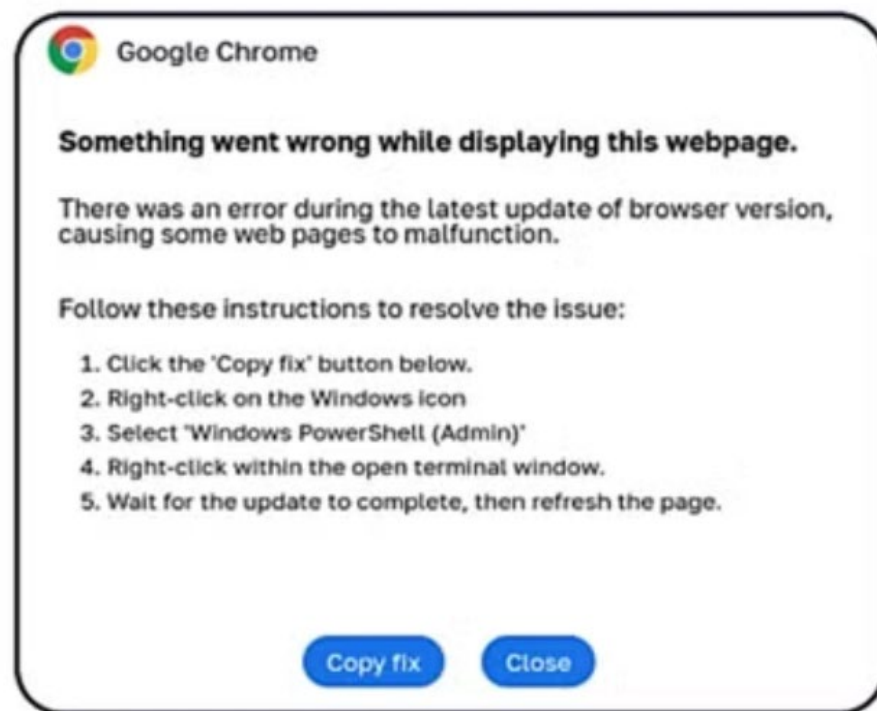
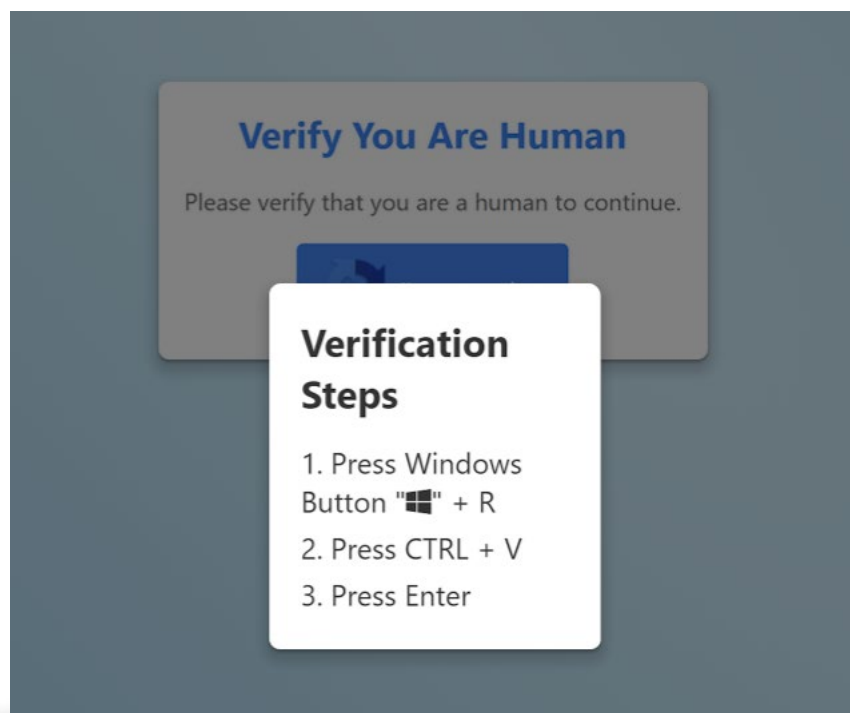
```
var  
var  
var PS >  
if(  
func  
co  
co  
if  
}  
retu  
value:
```

```
var o isArray(val | isRequest().consoles.Promise.resolve():
```



ClickFix

- Instead of using traditional malicious links or attachments that are easily blocked by security software, ClickFix relies on deceiving the user into performing a "fix" for a fake technical error.

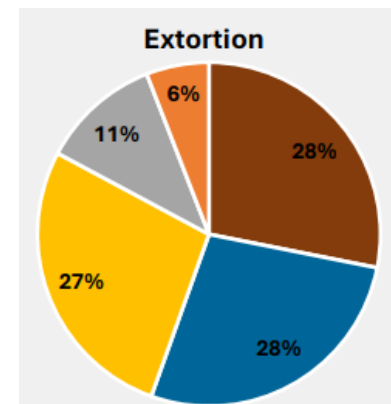
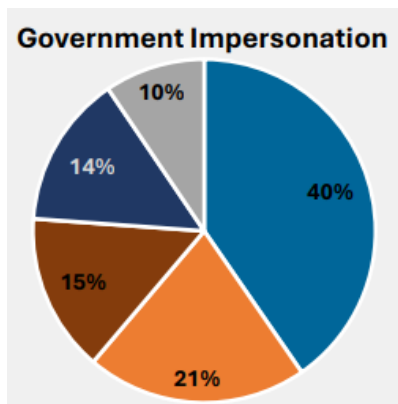
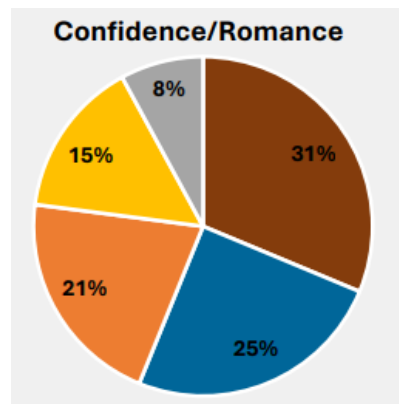
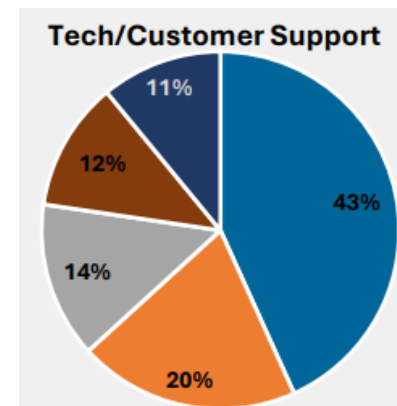
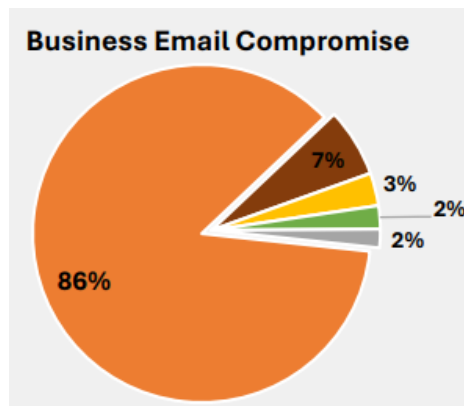
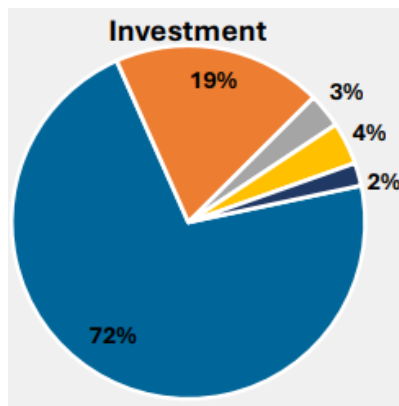


Other fraud schemes

- Calling “from bank” asking about non-existent fraudulent charges, then changing login information.
- Fake check / overpayment.
- AI voice / video calls.
- (S)Extortion.
- Tech / Customer Support.
- Government impersonation.



Transaction Types in Fraud



Source: 2025 IC3 Report



What Can We Do?



Cyber Fraud Prevention

- **DO NOT CLICK UNKNOWN LINKS**
- **ENABLE MULTI-FACTOR AUTHENTICATION**
- Educate employees
- Conduct BEC drills and anti-phishing exercises
- Update software to current versions and security patches
- View entire link before clicking:

<http://www.stealmyinformation.com/>
Ctrl+Click to follow link

<http://www.in.gov/cyber>



Cyber Fraud Prevention - Email

- Create email rules that flag emails received from unknown domains
- Monitor creation of new email rules
- Register similar domain names
- Use “forward” instead of “reply to”
- If you suspect suspicious activity with your email:
 - Change your password
 - Log out on all devices
 - Check for new rules within your account



MFA Apps

- Using authenticator apps to receive your multi-factor authentication code.
- These apps are tied to your physical device, and not to your phone number.

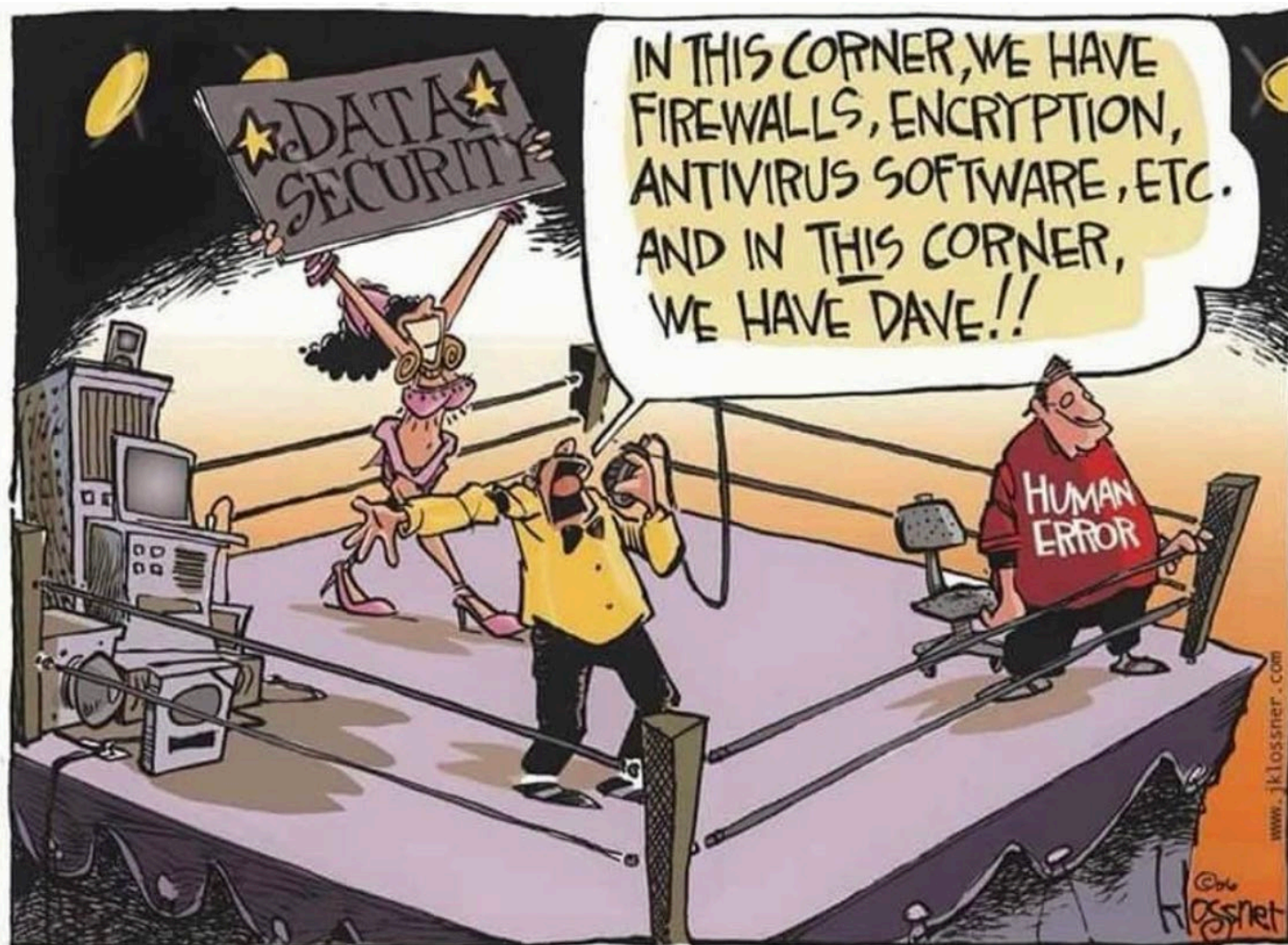


Cyber Fraud Prevention – Payments

- Confirm all changes in payment methods using trusted and authenticated information
- Consider requiring two parties sign off on payments



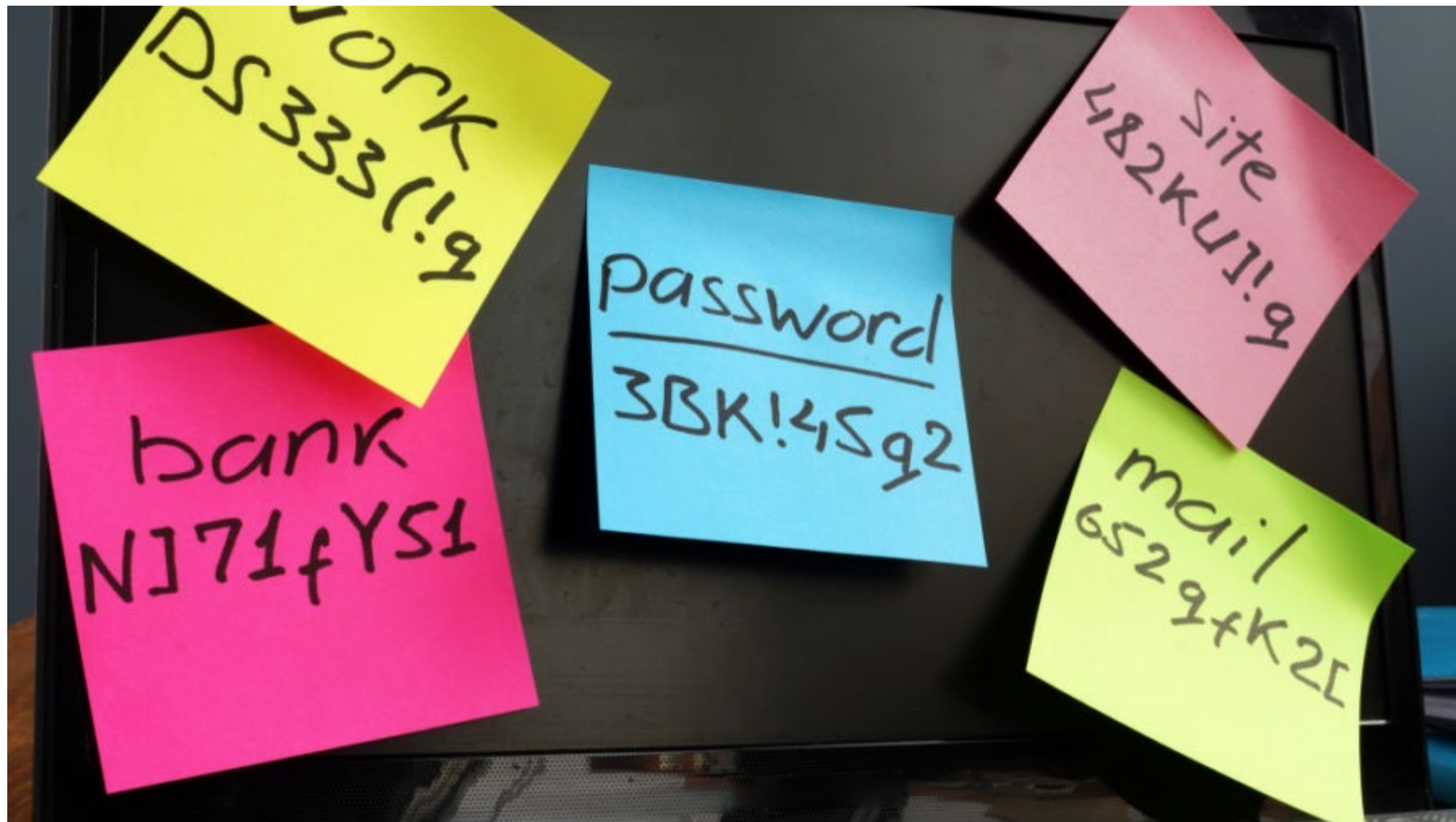
Try not to be Dave...



Human error is the biggest vulnerability



Passwords



Default Passwords

All it takes is a simple search to identify the default password of any device or software you use within your organization



Search Passwords

531 vendors, 2116 passwords

[@passdb on Twitter](#) / [Firefox Search](#)

	2Wire, Inc.	360 Systems
3COM	3M	Accelerated Networks
ACCTON	Acer	Actiontec
Adaptec	ADC Kentrox	AdComplete.com
AddPac Technology	Adobe	ADT
Adtech	Adtran	Advanced Integration



Weak Passwords

A study of over 11 million passwords found that the 20 most popular passwords account for 10.3% of all logins. In fact, on average, if you just tried “1234”, “12345”, or “123456”, you could log into about 5.5% of the accounts in the study. Add the word “password” as a password and you’ve now covered 6.8% of all passwords in use.



Two ways to create a password

1. Randomly generated

There's an App for that.



1Password



Bitwarden



Sources: NYT Wirecutter & CNET

2. Create and use a “passphrase”



Making a strong password

1. Think of a meaningful sentence.

“With Indiana Credit Union League in Indy”



Making a strong password

2. Take the first letter of each word.

“With Indiana Credit Union League in Indy”

wiculii



wiculii

HOW SECURE IS MY PASSWORD?

●●●●●●

It would take a computer about

2 HUNDRED MILLISECONDS

to crack your password

Why not try [Dashlane](#) to create and remember stronger passwords? **It's free!**

[Tweet Your Result](#)

howsecureismypassword.net



WORTHY OF TRUST AND CONFIDENCE

U//FOUO//LES

Making a strong password

3. Create a mixture of uppercase and lowercase letters.

wlCULiI



HOW SECURE IS MY PASSWORD?

●●●●●●

It would take a computer about

26 SECONDS

to crack your password

Why not try **Dashlane** to create and remember stronger passwords? **It's free!**

[Tweet Your Result](#)

howsecureismypassword.net



Making a strong password

4. Add a number

2026wICULiI



Making a strong password

A note on adding numbers...

Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. [Read more about how HIBP protects the privacy of searched passwords.](#)

gocolts24

pwned?

Oh no — pwned!

This password has been seen 22 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

haveibeenpwned.com



Making a strong password

A note on adding numbers...

Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. [Read more about how HIBP protects the privacy of searched passwords.](#)

pwned?

Oh no — pwned!

This password has been seen 2 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

haveibeenpwned.com



2026wICULi

HOW SECURE IS MY PASSWORD?

●●●●●●●●●●

It would take a computer about

41 YEARS

to crack your password

Why not create even stronger passwords with [Dashlane](#)? It's free!

[Tweet Your Result](#)

howsecureismypassword.net



Making a strong password

5. Add punctuation

2026wICUL@I



2026wICUL@I

HOW SECURE IS MY PASSWORD?

●●●●●●●●●●

It would take a computer about

34 THOUSAND YEARS

to crack your password

Why not create even stronger passwords with [Dashlane](#)? It's free!

[Tweet Your Result](#)

howsecureismypassword.net



HOW SECURE IS MY PASSWORD?

[illegible]

It would take a computer about

1 TREDECILLION YEARS

to crack your password

RoboForm can help you remember all of your secure passwords.

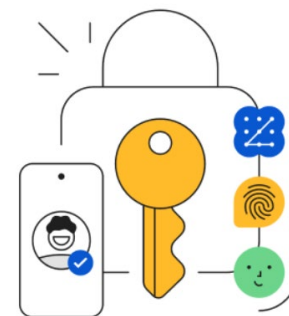
Tweet Your Result

howsecureismypassword.net



Password vs Passphrase vs Passkey

- **Password:** 2026wICUL@I
- **Passphrase:** 2026withIndianaCreditUnionLeague@Indy
- **Passkey:** Secure, phishing-resistant, password-less sign-in. Your device creates a unique key pair: a public key stored by the website and a private key stored securely on your device (device-bound).
 - Signing in requires only your device's biometric (Face ID/fingerprint) or PIN, making it faster and safer.



Questions and Contacts

QUESTIONS?

US Secret Service
Indianapolis Field Office
317-635-6420

ind-cftf@usss.dhs.gov

