



Nick Podhradsky

EVP, SBS CyberSecurity

nick@sbscyber.com | 605-770-3926



- Follow me on LinkedIn!
- Please interject your questions or comments!

The Cybercrime Empire













SCAM VICTIM

TELLS HER STORY



Darkside Mind Tricks



-  Trust/Gullibility
-  Ignorance
-  Fear
-  Greed
-  Group Mind
-  The Desire to Help
-  The Desire to be Liked
-  Curiosity

Jedi Training

1

Discuss
Trending Scams

2

Learn How to
Detect Scams
and What You
Should Do

3

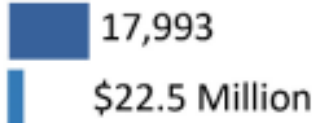
Empower You
to Be a Jedi
Master

2024 Complaints By Age Group

■ Complaints ■ Losses



Under 20



40 - 49



20 - 29



50 - 59



30 - 39



60+



[2024 IC3Report.pdf](#)

2024 CRIME TYPES

BY COMPLAINT COUNT

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

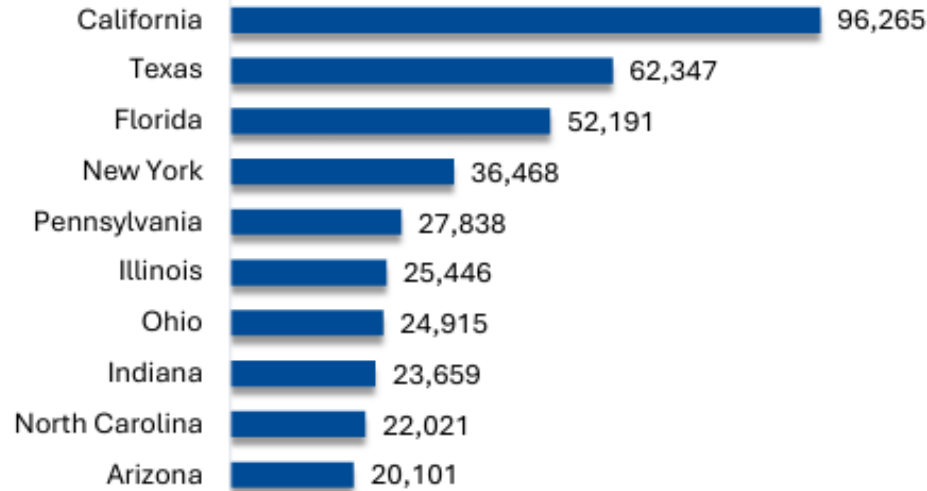


Top Ways Funds Are Lost in Fraud

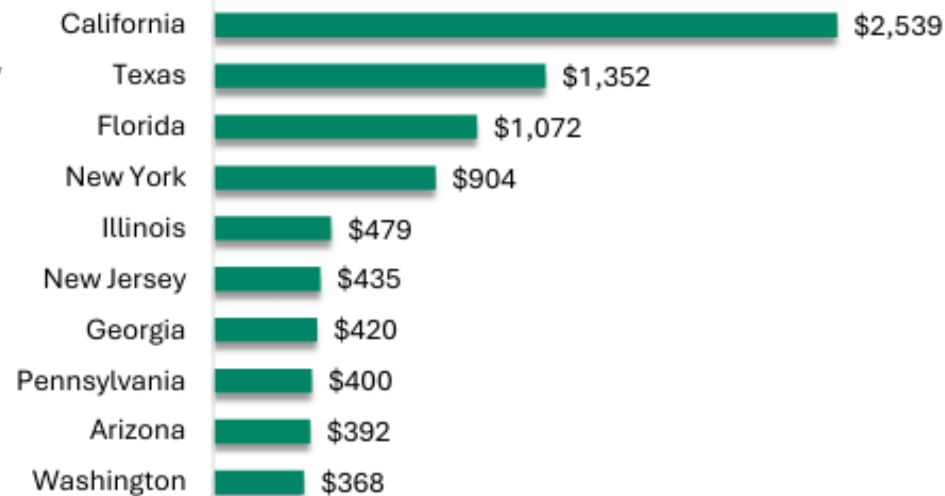


- Cryptocurrency
- Wire transfer/ACH
- Debit/Credit Card
- Peer-to-Peer Transfer
- Gift/Prepaid Card
- Check/Cashier's Check
- Cash

TOP 10 STATES BY NUMBER OF COMPLAINTS¹⁶



TOP 10 STATES BY LOSS (IN MILLIONS)¹⁷



Security Awareness Training

You are the first line of defense in a cybersecurity attack.

Teach/Train people!



Factors that reduced the average breach cost

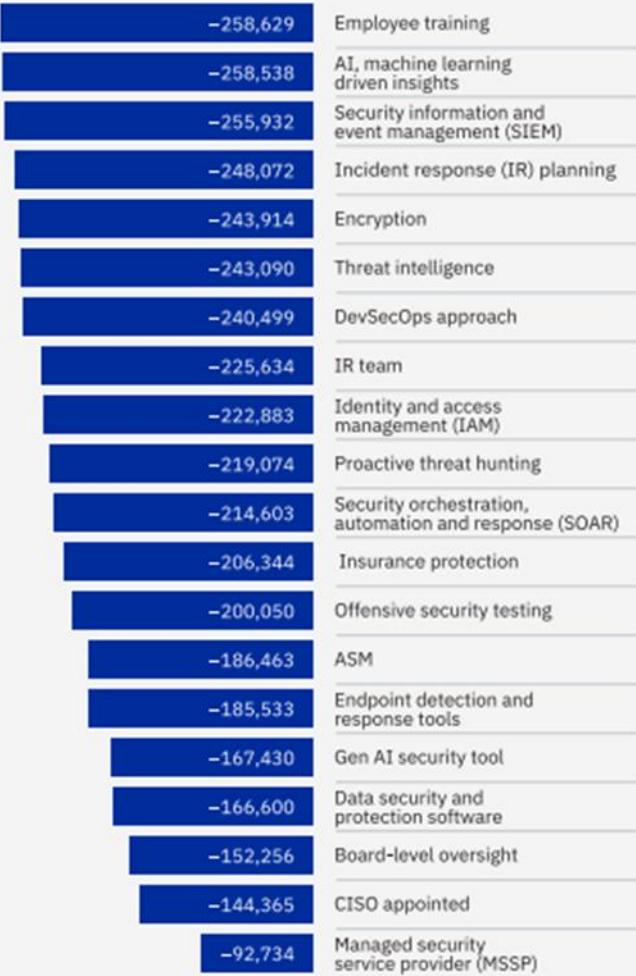


Figure 25. Cost difference from USD 4.88M breach average; measured in USD

Ransomware Growth

In 2024 there were about **5,414 published ransomware victim cases** globally, an 11% increase over 2023.

The second half of 2024 saw 46% more incidents than the first half, and 17% more than the same period in 2023.

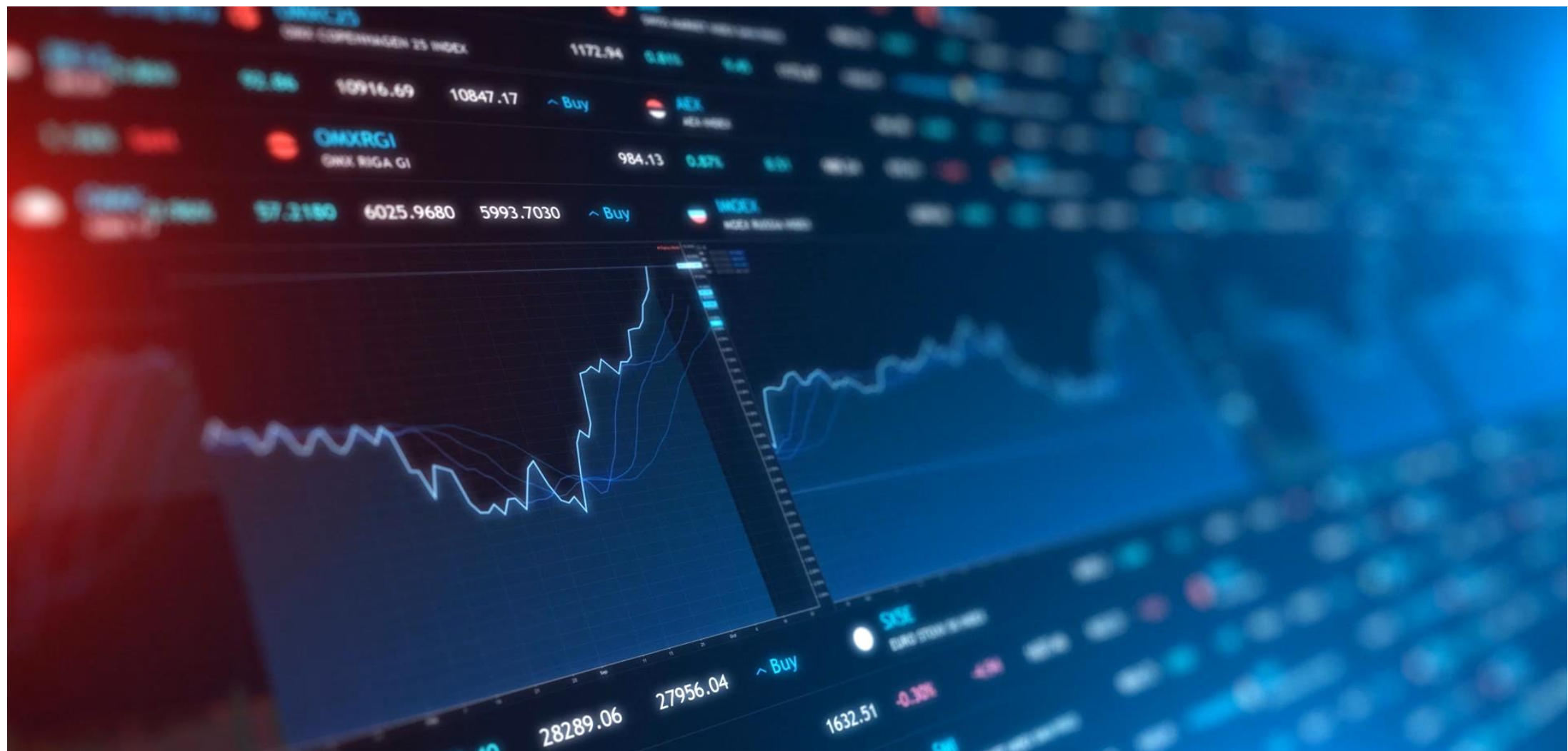
Money

- Ransom payments globally fell from about **\$1.2 billion in 2023** to around **\$814 million in 2024**.
- Typical ransom payouts vary a lot by industry and case, but averages in many sectors are in the millions. For example, some healthcare organizations report average payments in the multi-million range.
- The cost of recovery, downtime, reputational damage, legal, forensics etc. often makes the total cost of a ransomware incident much greater than just the ransom demanded.

Targets

- The **U.S.** is the single most-targeted country in ransomware incidents. In 2024, over 50% of published victim cases were in the U.S.
- Top sectors include **Business Services, Retail, Manufacturing**. In 2024 business services made up 24.1% of the ransomware cases; retail 15.2%; manufacturing 10.5%.
- Other vulnerable sectors: education, healthcare, government / critical infrastructure.
- In manufacturing, for example, ransomware attacks rose 41% in H1 2024.

As of 2025, the average American manages between 100 and 168 online accounts or logins



Have I Been Pwned

Check if your email address is in a data breach

nickpodhradsky@gmail.com



Check

Using Have I Been Pwned is subject to the [terms of use](#)

Email Breach History

Timeline of data breaches affecting your email address

2

Data Breaches

Oh no — pwned! This email address has been found in multiple data breaches. Review the details below to see where your data was exposed.



Account Hijacking / Business Email Compromise

■ What is Business Email Compromise (BEC)?

- Business Email Compromise (BEC) is a sophisticated scam targeting both businesses and individuals working with suppliers and/or businesses regularly performing wire transfer payments.
- The scams are carried out by fraudsters by compromising email accounts and other forms of communication such as phone numbers and virtual meeting applications.



■ 2024 Internet Crime Report

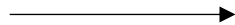
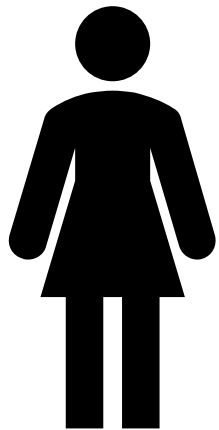
In 2024, the IC3 received 859,532 BEC complaints with reported losses **over \$16B**



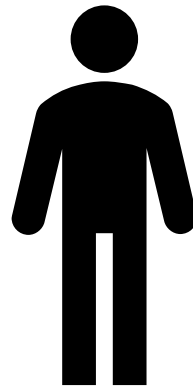
- Use two-factor or multi-factor authentication.
- Verify payments and purchase requests.
- Examine email addresses, URLs, and spelling in correspondence.
- Avoid clicking links in unsolicited messages.

How does it happen?

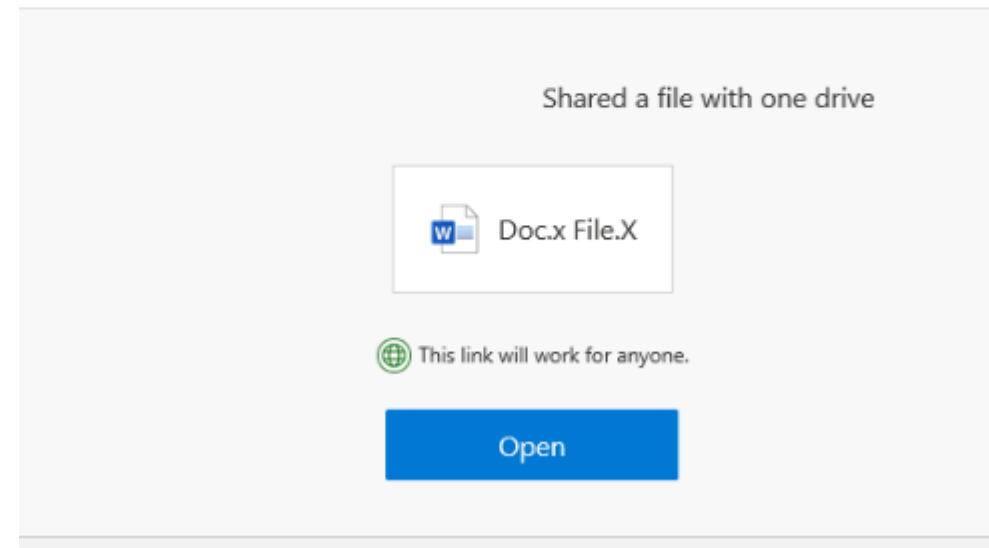
Cybercriminal

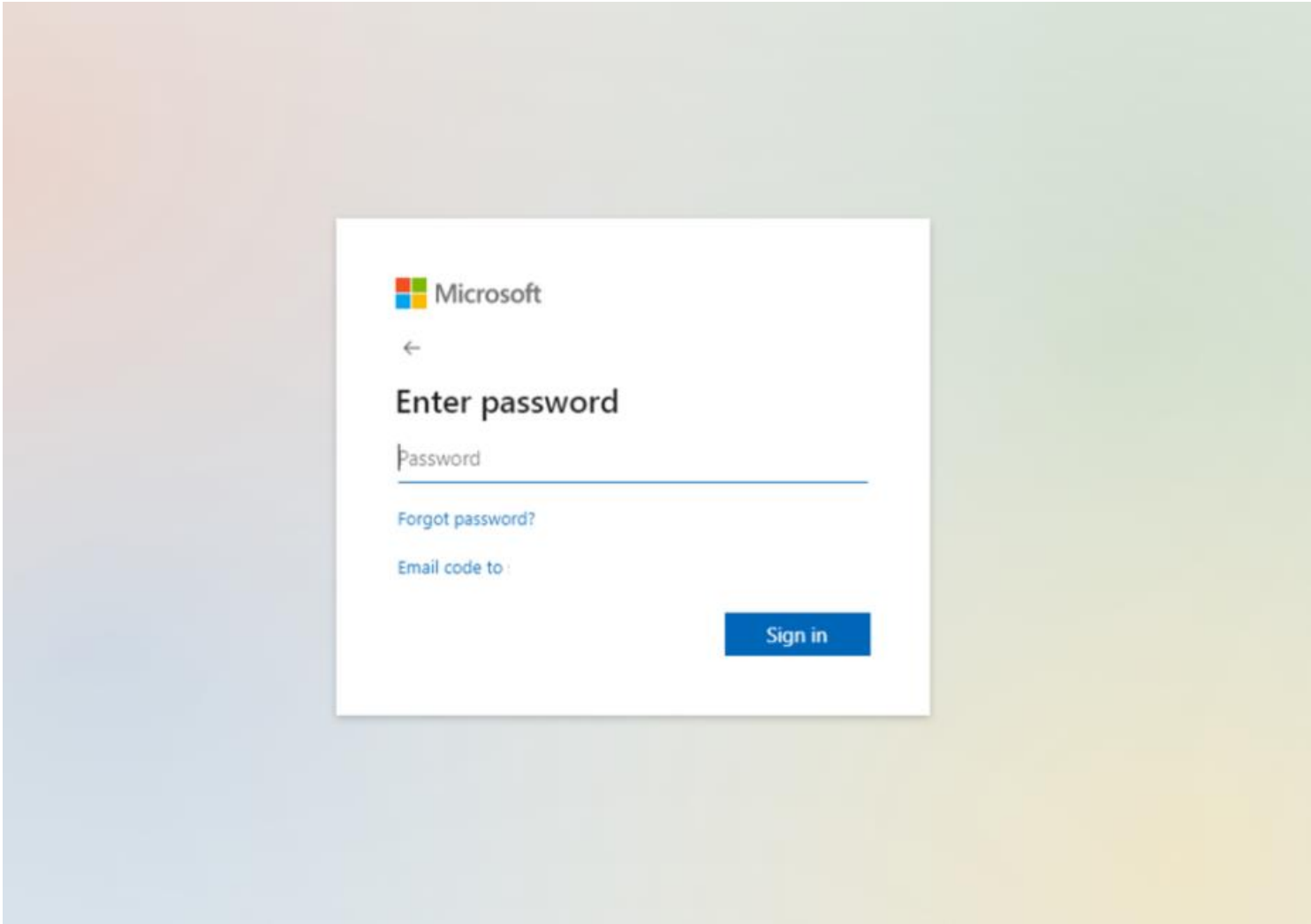


Company



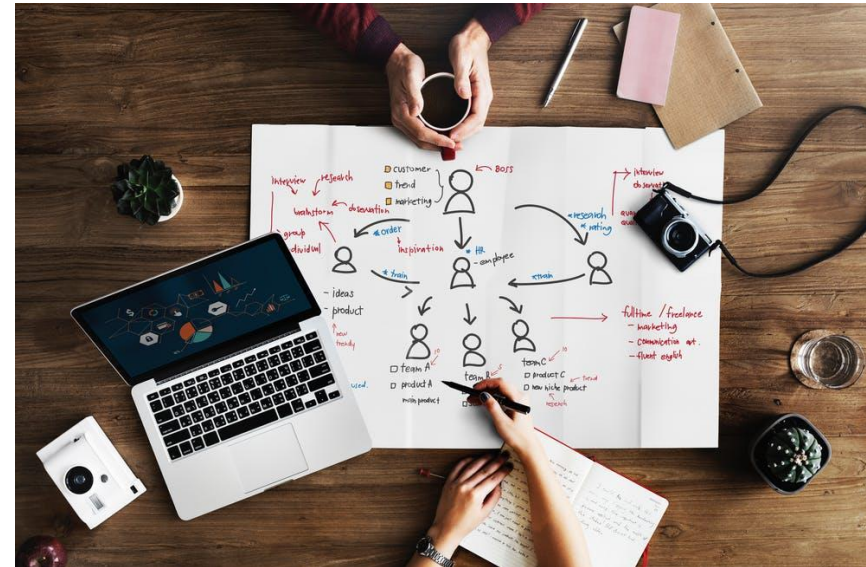
shared a file with you





■ Search Compromised Account

- Discover the flow of money and who the players are
- Search email history for key terms
 - Wire
 - Payment
 - Invoice





Forward the inbox
to another email
address



Delete messages
from upcoming
target list



From: Billing@Supply.com

To: AP@company.com

Subject: Updated Invoice for September

Hi AP,

Please find attached the updated invoice for September. We've recently changed our banking details, so kindly use the new account listed below.

- Bank Name: Global Trust Bank
Account Name: Acme Supply Ltd
Account Number: 1122334455

Let me know once payment is processed.

Best regards,
"Mark Jensen"
Acme Supply Ltd



From: ap@company.com

To: billing@acme-supply.com

Subject: RE: Updated Invoice for September

Hi Mark,

Thanks for the invoice. Can you confirm the change in banking details was approved internally? We don't have a record of this update.

Also, do you have a signed vendor update form?

- **From:** billing@acme-supply.com
To: ap@company.com
Subject: RE: Updated Invoice for September

Hi,

Yes, the change was approved last week. Our CFO signed off on it. Unfortunately, I'm traveling and don't have access to the signed form right now.

Please proceed with the payment to avoid late fees.

Appreciate your help!

Mark


■ Sample Scenario

- The players

- Bob Buyer– Bob@gmail.com
- Lenny Lender- Lenny@CU.com
- Andy Admin- Andy@CU.com
- Rhonda Realtor- Rhonda@msn.com 
- Harry Hacker- Bobb@gmail.com, Lenny@gmail.com 

- Bob is purchasing a house. Rhonda is his realtor; Lenny is his mortgage lender. Lenny has an assistant named Andy. Unbeknownst to any of the parties, Harry Hacker has gained access to Rhonda's email account.

Email#1

- Date: 3-14-2019
From: Andy Admin (Andy@CU.com)
- To: Bob Buyer (Bob@gmail.com), Rhonda Realtor (Rhonda@msn.com) 
- CC: Lenny Lender (lenny@CU.com)



- Subject: Closing Date

- Hi Bob,
- Your closing date has been set for Wednesday, March 25th at 10:30 AM. It will be at Amazing Title Company.

- Please let me know if you have any questions.

- Andy Admin
- Mortgage Assistant
- Andy@CU.com


■ Email#2

- Date: 3-14-2019
- From: Rhonda Realtor (Rhonda@msn.com) -compromised 
- To: Andy Admin (Andy@CU.com), Bob Buyer (Bobb@gmail.com) Fake 
- CC: Lenny Lender (lenny@CU.com)

- Subject: RE: Closing Date

- I need the estimated settlement statement showing the estimated closing costs for the buyers.

Email#3



- Date: 3-14-2019
- From: Lenny Lender (lenny@CU.com)
- To: Bob Buyer (Bobb@gmail.com), Rhonda Realtor (Rhonda@msn.com) 
- CC:
- Subject: RE: Closing Date

- Good Afternoon Rhonda,
- Due to compliance, we can only share this information with the borrower. The borrower may choose to share with you if they decide.



- We do not have the settlement statement balance with the title company at this time. We will have the closing disclosure balanced and in the borrowers hands not later than 3/21/2019

- Lenny Lender
- Mortgage Lender
- Lenny@CU.com


Email#4

- Date: 3-14-2019
 - From: Bob Buyer (Bobb@gmail.com), 
 - To: Lenny Lender (lenny@CU.com)
 - CC: Rhonda Realtor (Rhonda@msn.com),  Andy Admin (Andy@CU.com)
 - Subject: RE: Closing Date
-
- Lenny,
 - We need the estimated settlement statement as we need an estimate of closing costs.
-
- Bob
 - Sent from my iphone


Email#5

- Date: 3-14-2019
- From: Lenny Lender (lenny@CU.com)
- To: Bob Buyer (Bobb@gmail.com), 
- CC: Rhonda Realtor (Rhonda@msn.com),  Andy Admin (Andy@CU.com)
- Subject: RE: Closing Date
- Bob,
- I have just sent you the closing statement **via our secure email system**. Please let me know if you have any questions.
- Lenny Lender
- Mortgage Lender
- Lenny@CU.com


Email#6

- Date: 3-14-2019
- From: Lenny Lender (llenny@gmail.com) 
- To: Bob Buyer (Bob@gmail.com)
- Subject: 123 New House Drive.
- Good morning Bob,
- I just you a copy of your original loan estimate that was issued 3-6-2019. I had to email it encrypted due to sensitive information. Please be advised that you are required to wire the estimated cash to close cost to Amazing Title Agency account not later than Tuesday March 19th.
- I'll be sending you wiring instructions shortly
- Lenny Lender
- Mortgage Lender
- Lenny@CU.com

Email#7

- Date: 3-14-2019
From: Bob Buyer (Bob@gmail.com)
- To: Lenny Lender (llenny@gmail.com) 
- Subject: RE: 123 New House Drive.
- Lenny,
- Did you send this message?
- Sent from my iPhone

Email#8

- Date: 3-14-2019
- From: Lenny Lender (llenny@gmail.com) 
- To: Bob Buyer (Bob@gmail.com)
- Subject: RE: 123 New House Drive.
- Hi Bob,
- I sent the email. Please advise if you'd be able to wire funds tomorrow. Here is the account number#####
- Lenny Lender
- Mortgage Lender
- Lenny@CU.com

■ BEC Controls

- Get educated on Phishing and BEC Scams
- Email Configurations
 - SPF, DKIM, DMARC
 - Email Sandboxing
 - Conditional Access Controls
 - Audit Logging and Alerts
 - Exchange Online Protections
 - External Email Flags
- Enforce MFA on Everything
- Password Managers
- Dual Authorization/Dual Signature
- In Person/Voice Verification or Call Backs
- Geo location IP Blocking

Pig Butchering



Pig Butchering

- Pig butchering is a type of scam where fraudsters build trust with victims over time, often through social media or dating apps, and then deceive them into investing in fake cryptocurrency or other fraudulent investment schemes.
- The term refers to the practice of fattening pigs before slaughter, symbolizing how scammers "fatten" their victims with false promises of high returns before stealing their assets.

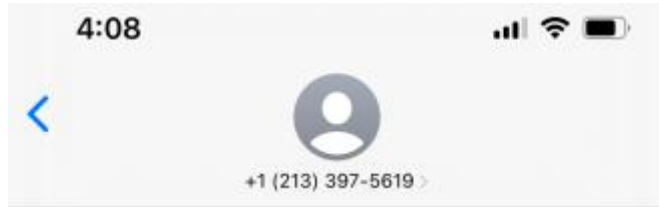
How It Starts - Initial Contact



Hi Nick, are you available at the moment?

The sender is not in your contact list.

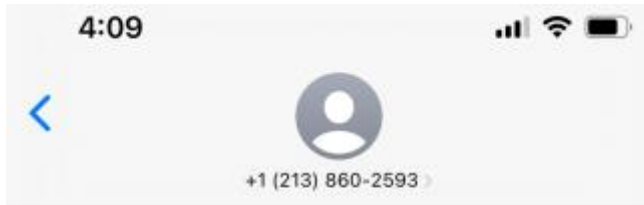
[Report Junk](#)



When are we going to play golf?

The sender is not in your contact list.

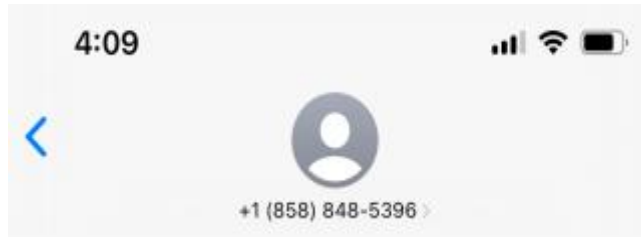
[Report Junk](#)



Hey! Want to grab some dinner together?

The sender is not in your contact list.

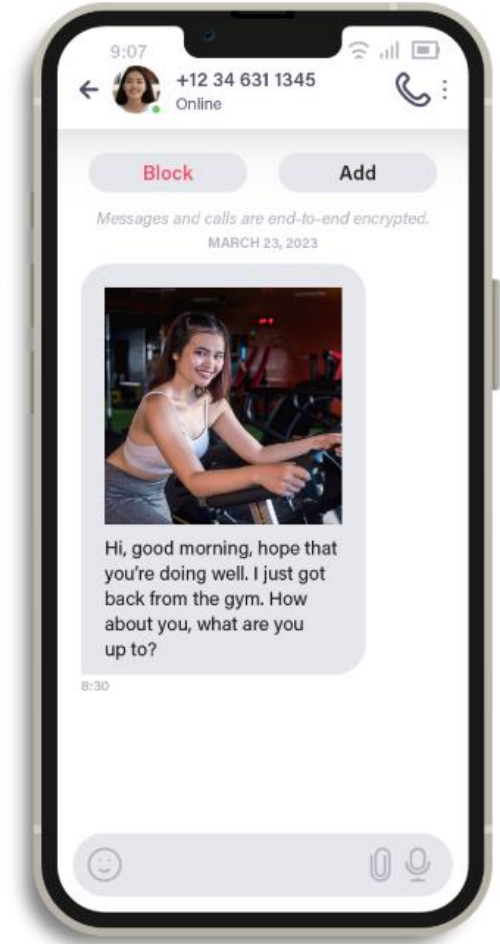
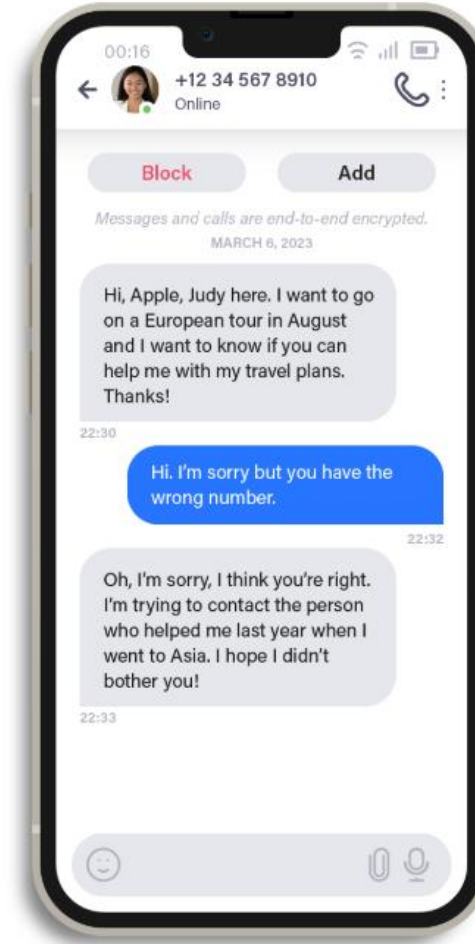
[Report Junk](#)



Hey what are you doing

The sender is not in your contact list.

[Report Junk](#)



Building Trust

- Multiple contacts and friendly conversations
- Personal stories and pictures
- Goal is to build an emotional connection

Introduction of Investment

- Persuasion to make a small initial investment
- Scammer points to fake website for investments
- Allows to withdraw some profits to build further confidence
- Encourages larger investments

- Dashboard
- Deposit
- Withdraw
- Transfer
- Secured deal
- Staking
- Trading
- History
- Settings

Profile icon, Username: [redacted].com (UID: [redacted]), Last login date: [redacted], Last login IP: [redacted]

Enable 2FA Verified Premium Spot Orders: 0 Margin Orders: 0

Estimated Total Value: **24118,00 USD**

Search

Coin	Available	On Orders	USD Valuation	Action
BTC	0.691864	0	24118,31	Deposit Withdraw Trade
ETH	0	0	0,00	Deposit Withdraw Trade
XRP	0	0	0,00	Deposit Withdraw Trade
DOT	0	0	0,00	Deposit Withdraw Trade
ADA	0	0	0,00	Deposit Withdraw Trade
EOS	0	0	0,00	Deposit Withdraw Trade
XMR	0	0	0,00	Deposit Withdraw Trade
KSM	0	0	0,00	Deposit Withdraw Trade

Disappear

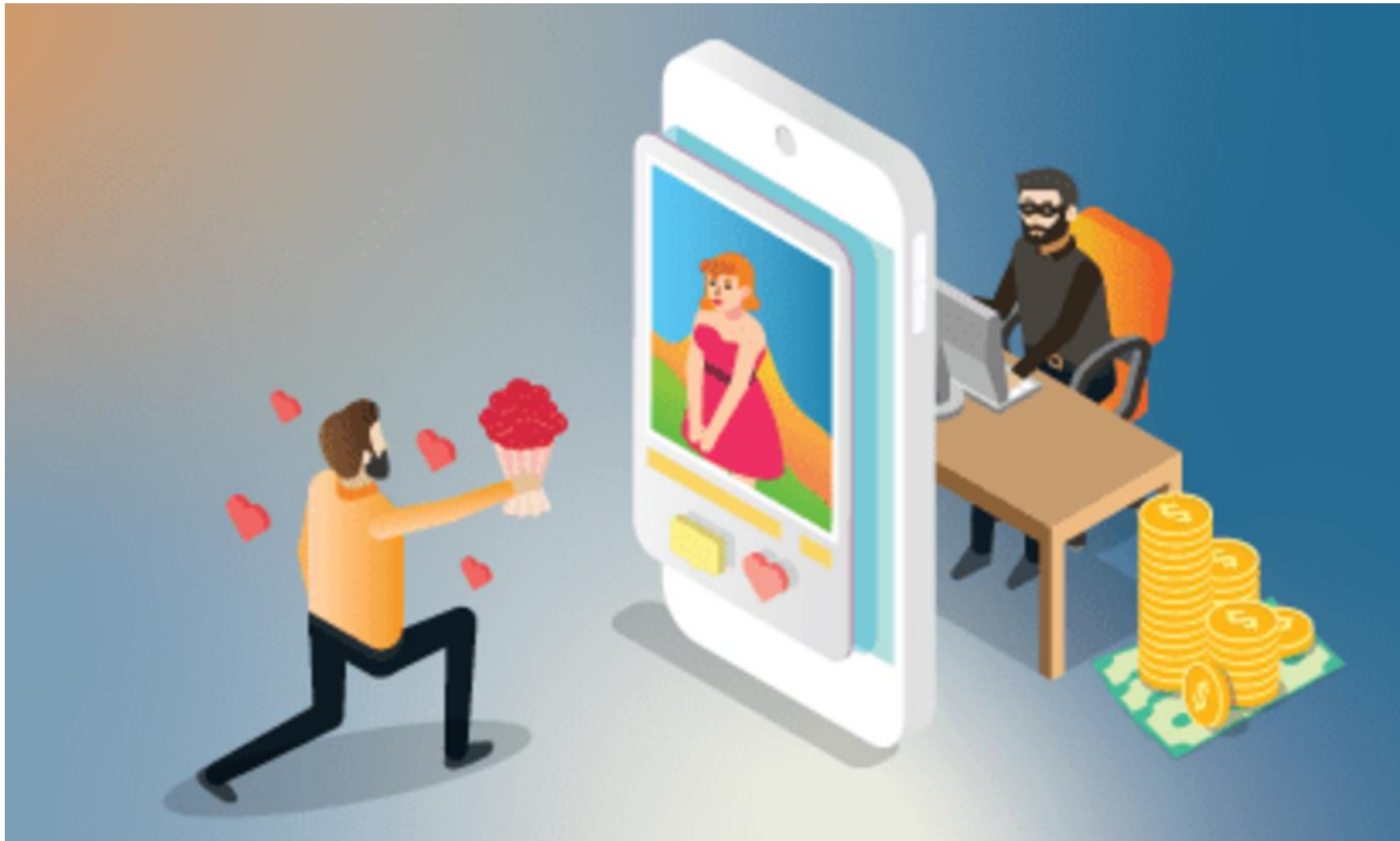
- Once the investments stop coming, the scammer cuts off all communication.

Pig Butchering - Human Trafficking

- Fake job ads to economically vulnerable
- Recruitment - pay for travel expenses
- Arrival - confiscate passports and identification and taken to camps
- Coercion and control
- Both the scammers and scammed are victims



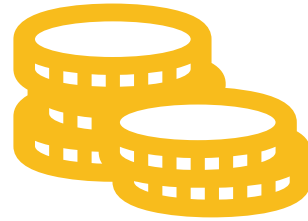
Romance Scams



Detect Pig Butchering/Romance Scam



Be skeptical
of
unsolicited
messages



Do research
(especially
involving
crypto
currency)



Confess their
love early
and often



Avoid
meeting
up and
video
chats



Always
have
sudden
urgent
financial
needs

SMSHING - Text Message Phishing

Text Message
Today 3:40 PM

WARNING:(Criminal Investigation Division) I.R.S is filing lawsuit against you, for more information call on [+1 7038798780](tel:+17038798780) on urgent basis, Otherwise your arrest warrant will be forwarded to your local police department and your property and bank accounts and social benifits will be frozen by government.

South Dakota Department of Vehicles(DMV) Final Notice: Enforcement Penalties Begin on June 10.

Our records show that as of today, you still have an outstanding traffic ticket. In accordance with South Dakota State Administrative Code 15C-16.003, if you do not complete payment by June 9, 2025, we will take the following actions:

1. Report to the DMV violation database
 2. Suspend your vehicle registration starting June 10
 3. Suspend driving privileges for 30 days
 4. Transfer to a toll booth and charge a 35% service fee
 5. You may be prosecuted and your credit score will be affected
- Pay Now:

<https://dot.gou-yzbu.icu/us>

Please pay immediately before enforcement to avoid license

Pay your FastTrak Lane tolls by January 15, 2025 to avoid a fine and keep your license.

You can pay at:

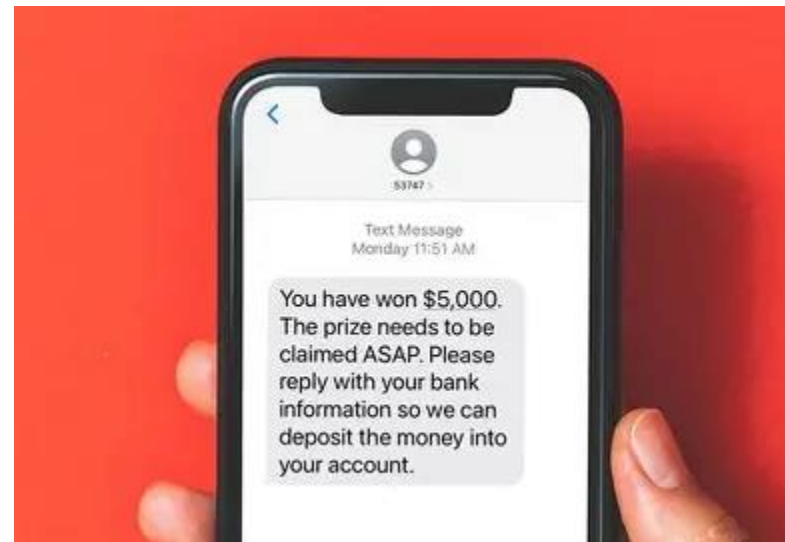
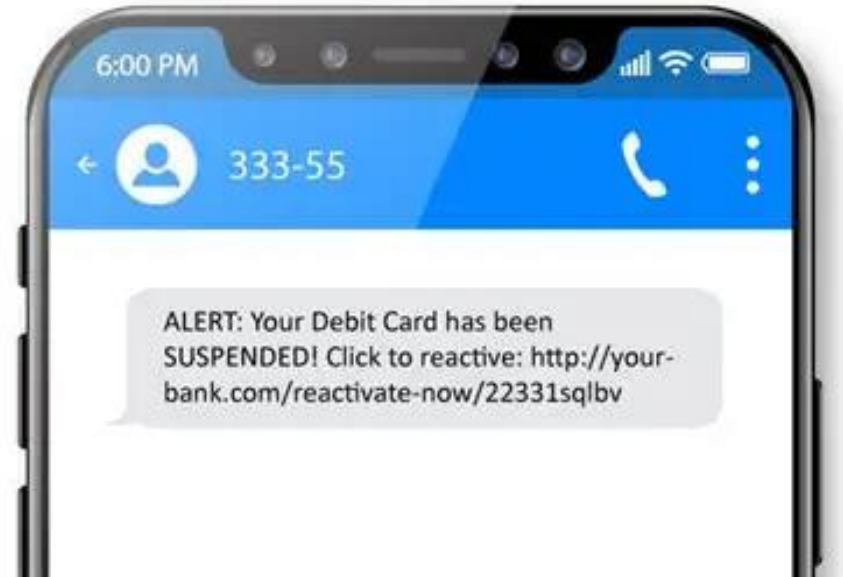
<https://www.fastracktoll.biz/tollpayment>

Your Bluestone account has been locked for suspicious activity. Please call [201-867-5309](tel:201-867-5309) to verify your identity and unlock your account.

Your USPS package arrived at the warehouse but could not be delivered due to incomplete address information. Please confirm your address in the link.

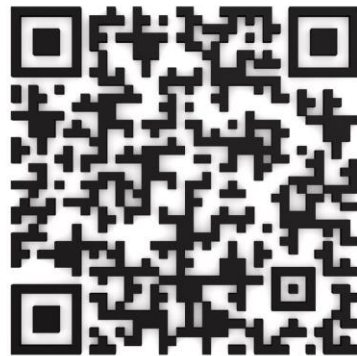
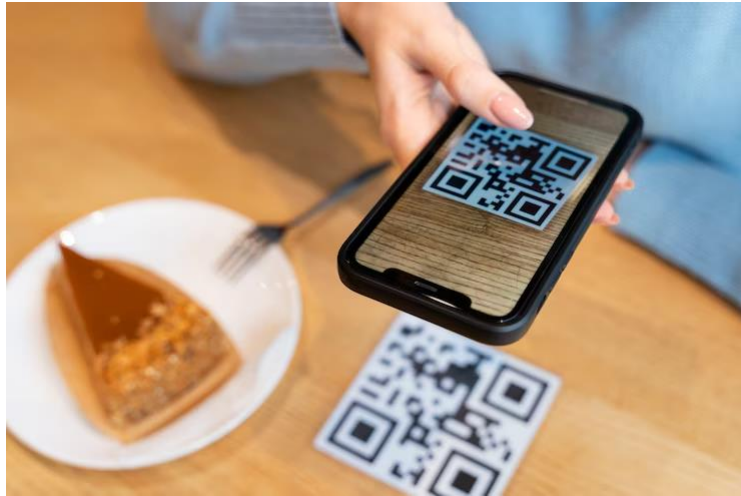
<https://usps.rpostei.com>

We will attempt delivery again within 24 hours after updating.



Quishing

- Quishing is a type of phishing attack that uses QR codes to deceive individuals into visiting malicious websites or downloading harmful content. They are distributed via phishing emails, social media, printed flyers, or other physical objects.





AI Powered Scams



Impostor uses AI to impersonate Rubio and contact foreign and US officials



AI FINANCIAL FRAUD

Sam Altman says financial industry faces a massive 'fraud crisis' as AI impersonates people's voices to trick security

BY THE ASSOCIATED PRESS

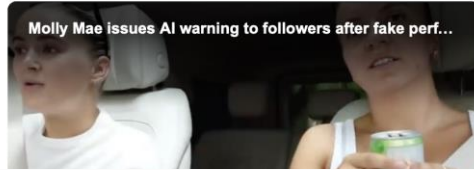
July 23, 2025 at 5:22 AM EDT



The "pro-Trump messaging" TV spot in the latest "South Park" episode features an AI deepfake of the president walking in the desert. YouTube/South Park Studios

Molly Mae issues AI warning to followers after fake perfume endorsement

The Independent
Tue, July 22, 2025 at 5:25 AM CDT



OpenAI CEO Sam Altman speaks during a discussion at the Federal Reserve Integrated Review of the Capital Framework for Large Banks Conference at the Federal Reserve in Washington, on July 22, 2025. MARK SCHIEFFELBEIN—AP

Trump Posts Fake Video Showing Obama Arrest

President Trump shared what appeared to be an A.I.-generated video of former President Barack Obama being detained in the Oval Office.

Listen to this article · 3:44 min [Learn more](#) [Share full article](#)



Fake video appears to be manipulated footage of an Oval Office meeting in November 2016 between then President Obama and Mr. Trump. Stephen Crowley/The New York Times

Spanish teenager investigated over AI naked images of classmates

By Reuters

July 27, 2025 11:40 AM CDT · Updated July 27, 2025



MADRID, July 27 (Reuters) - Spanish police said on Sunday they were investigating a 17-year-old on suspicion of using artificial intelligence to deepfake nude images of female classmates for sale.

Sixteen young women at an educational institute in Valencia, in southeastern Spain, complained about the AI-generated images of them which were circulating on social media and online.

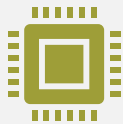
■ Deepfake Scams

- [OpenAI CEO Sam Altman warns of AI fraud crisis 'very soon'](#)
- [Finance worker pays out \\$25 million after video call with deepfake 'chief financial officer' | CNN](#)
- [Deepfake romance scam raked in \\$46 million from men across Asia, police say | CNN](#)
- [Pindrop: Deepfake Fraud Surges 1300% in 2025 Report](#)
- [How deepfake AI job applicants are stealing remote work](#)
- [Real-time deepfake fraud in 2025: AI-driven scams | Veriff.com](#)



Face & Voice Mapping

AI models analyze thousands of images and audio clips to learn how someone looks, talks, and moves—then replicate those patterns in new media.



Media Generation Models

Tools like image-to-video generators and voice cloning software create lifelike videos and sound from scratch, often using very little source material.



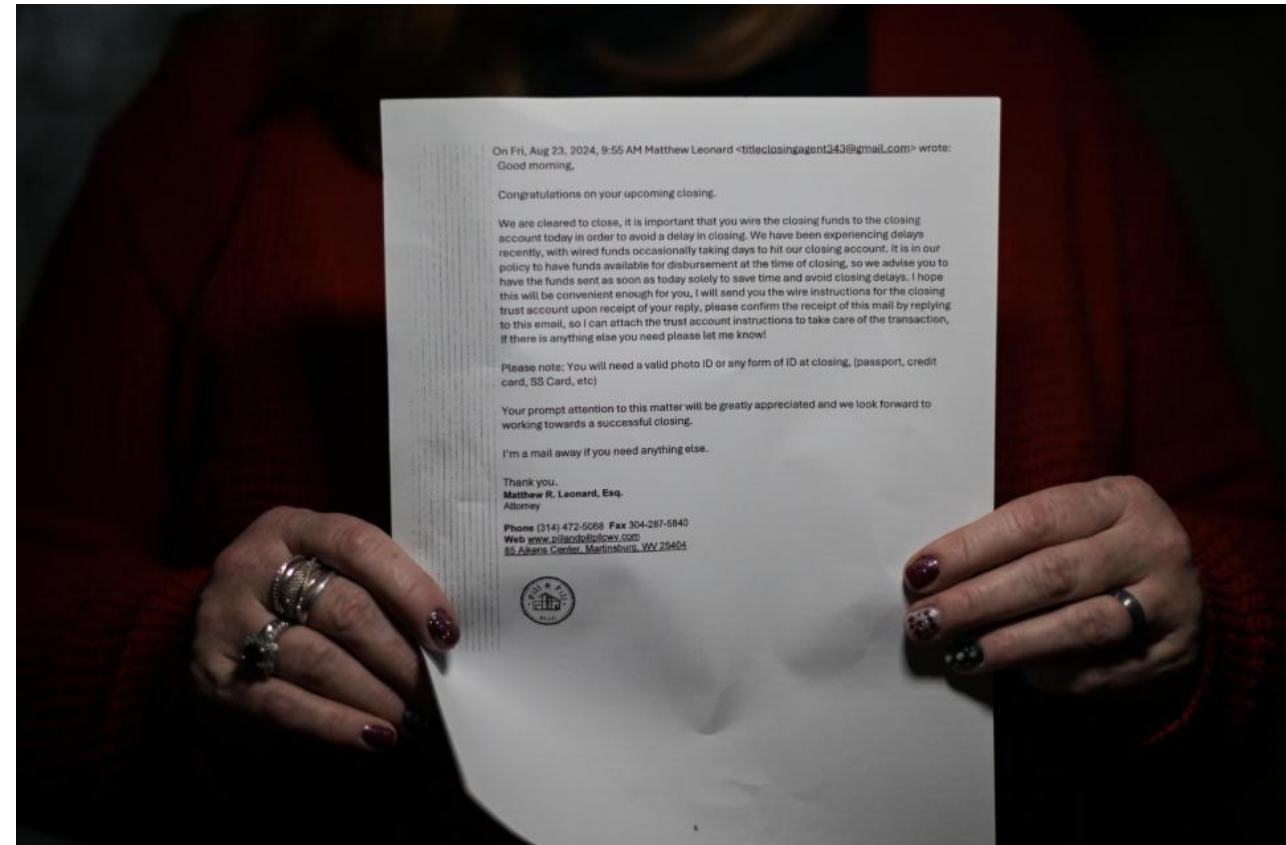
User-Friendly Deepfake Apps

Platforms like HeyGen, FaceSwap, DeepFaceLab, and ElevenLabs make it easy for non-experts to create convincing fake content with drag-and-drop interfaces.

Virtual Kidnapping/Deep Fake Voice



Fake Identity Creation



Detecting Deepfakes

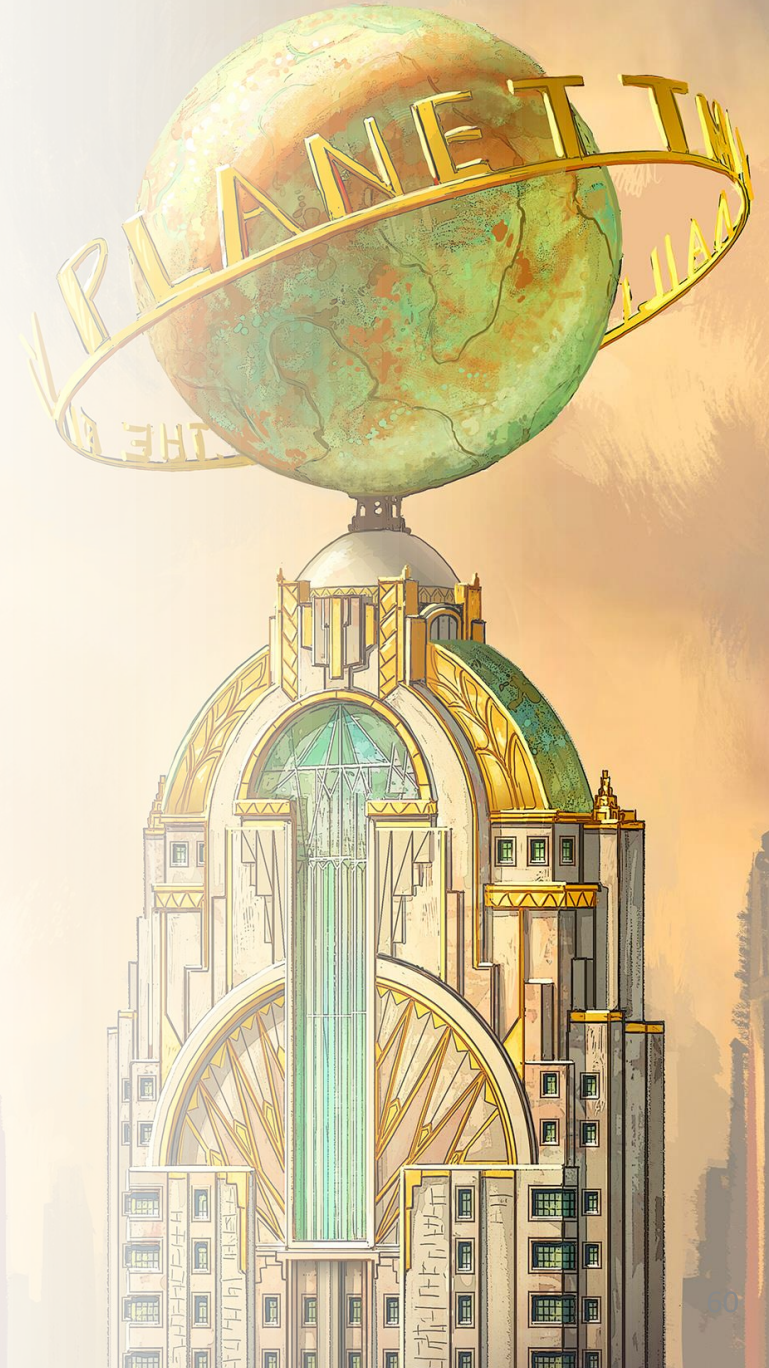
- Unsettling silences, distorted decibels, unnatural pauses
- Flat speaking tone
- Video inconsistencies or unnatural movement
- Facial profile images look distorted, blurred, or unsettling
- Poor video, lighting, and audio quality or odd background noise
- Deep fake detection technologies

Apply “The Golden Rule”

- Treat all digital communication as if it is a possible attack.
- **Who?**
 - Can you verify that it is coming from the real person?
 - Out-of-band communication
- **What?**
 - What do they want you to do?
 - Have they ever asked you to do this?
 - Send money (Crypto is a big red flag)
 - Click on link or go to a website
- **Why?**
 - Why do they want you to take action?
 - This is always creating a sense of urgency

Continual Education

- Share articles and example threats
- Posters
- Computer desktop images or screensavers
- Online learning management system with quarter or monthly training
- Phish tank
- Continual employee contact
- October Security Awareness Month
- Social engineering tests
- Weekly or monthly phishing tests/training
- Cybersecurity Escape Rooms
- Peer Led Trainings



■ Cyber Pulse Memos

- Create executive memos of events that are happening (one page)
 - What happened
 - Impact on the members
 - How it happened
 - How it could happen to us
 - Current control or gaps in programs
 - Links to stories or resources



Regular Email Notifications



AI-Fueled Cybercrime May Outpace Traditional Defenses, Check Point Warns

The security firm said in a new report that defenders should begin using AI to counter cybercriminals' adoption of the technology.

[Read the full article at Cybersecurity Dive](#)

Reporting Lines: Could Separating from IT Help CISOs?

CISOs who report to the CFO find that the shift away from IT can improve their ability to translate risk into business terms, communicate more effectively with executives, and avoid conflicts of interest with IT.

[Read the full article at CSO Online](#)

The State of Intrusions: Stolen Credentials and Perimeter Exploits on the Rise, as Phishing Wanes

Cybercriminals also likely to leverage tools present within the targeted environment rather than to construct new malware or configure post-exploitation tools, according to Mandiant's incident observations.

[Read the full article at CSO Online](#)

Other Recommended Reads

- [Bleeping Computer: FBI shares massive list of 42,000 LabHost phishing domains](#)
- [Bleeping Computer: Google- 97 zero-days exploited in 2024, over 50% in spyware attacks](#)
- [Tripwire: Ransomware Attacks on Critical Infrastructure Surge, Reports FBI](#)
- [Cybersecurity Dive: Zero-day exploitation drops slightly from last year, Google report finds](#)
- [The Hacker News: 159 CVEs Exploited in Q1 2025 — 28.3% Within 24 Hours of Disclosure](#)
- [The Register: Infosec pros rally against Trump's attack on Chris Krebs](#)
- [inforRiskToday: JPMorgan Chase CISO Decries Poor SaaS Cybersecurity](#)
- [ars Technica: The end of an AI that shocked the world: OpenAI retires GPT-4](#)

Downloads & More!

- Head to our landing page and download some goodies!
- Including:
- Chance to win a **free SBS Institute webinar or membership!**
- This presentation's **slide deck!**
- Presentation survey – we love feedback! Tell us how we did!
- **Free download** – 34 ideas to build a Culture of Cybersecurity!
- Sign up for **in the wild!**
- <https://sbscyber.com/dakcu>



GAME OVER

10

CONTINUE?

> YES NO





Nick Podhradsky

Head of Business Development

nick@sbscyber.com | 605-770-3926

- Follow me on LinkedIn!

HACKER
 **HOUR**



 linkedin.com/company/sbs-cybersecurity

 facebook.com/trustSBS

 @SBSCyber

Consulting

Network Security

Solutions

IT Audit

Education



IN THE
WORLD

*Email Nick to receive our weekly top-secret
cybersecurity newsletter... or click here:*

**SIGN UP
TODAY**