# 2024 UMRA Bryce Canyon Summer Conference

July 31, 2024

Sergeant Jeff Plank
Agent Scott Pugmire

# 2024 UMRA Bryce Canyon Summer Conference

July 31, 2024

Sergeant Jeff Plank
Agent Scott Pugmire

# Cyber Task Force (CTF) Utah Model

- Established in July 2013
- Is a collaboration between FBI Special Agents and Agents from the Department of Public Safety/State Bureau of Investigation.
- Agents are housed at the FBI.
- Agents investigate various kinds of Internet fraud and computer intrusions which are reported through IC3.gov and other sources.
- Utah was the first in the nation to do this with cyber

# Benefits to Utah From the CTF


- Access to Federal Databases
- FBI provided training and funding for training
- Standardized assistance around the U.S. and world
- LEGAT program
- Access to other Federal agencies
- Equipment
- Case are being investigated that previously were not

FEDERAL BUREAU of INVESTIGATION

# Internet Crime Report

2023

INTERNET CRIME COMPLAINT CENTER

# IC3 BY THE NUMBERS[12]

**$12.5 Billion**

Losses in 2023

**2,412**

Average complaints received daily

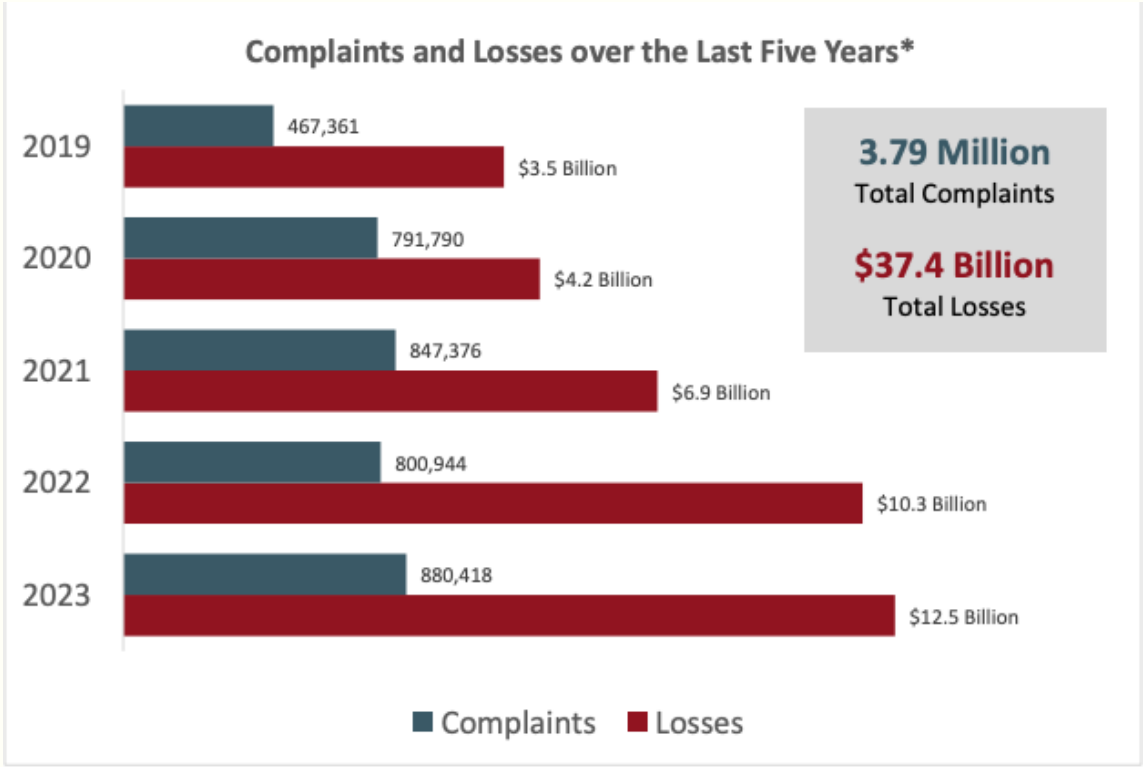

**758,000+**

Average complaints received per year (last 5 years)

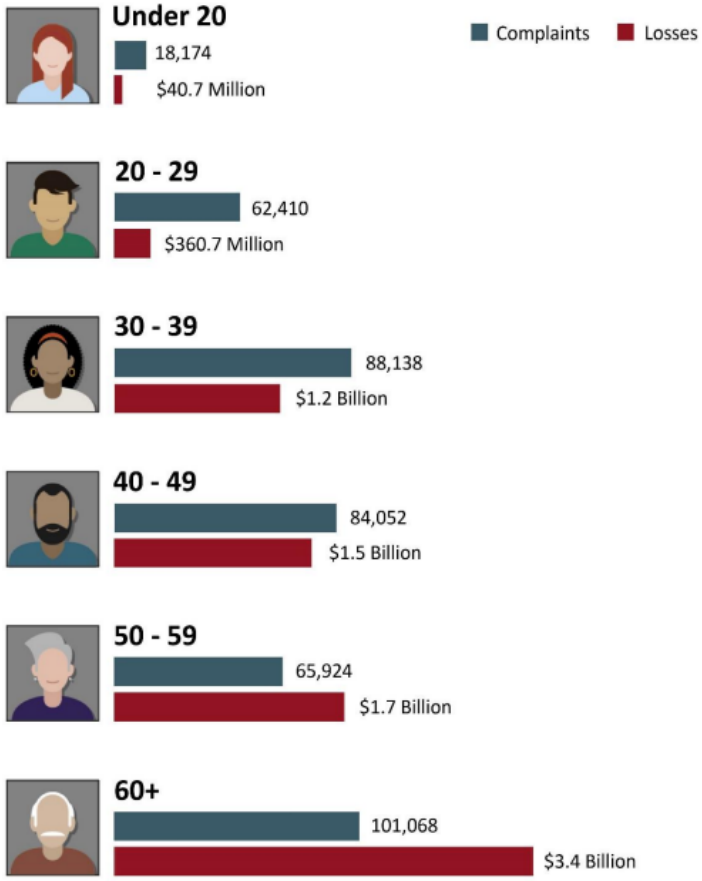
**Over 8 Million**

Complaints reported since inception

# IC3 Complaint Statistics



# 2023 - COMPLAINANTS BY AGE GROUP [13]



## OVERALL STATE STATISTICS

**Complaints per State***

| Rank | State | Complaints | Rank | State | Complaints |
|---|---|---|---|---|---|
| 1 | California | 77,271 | 30 | Louisiana | 4,890 |
| 2 | Texas | 47,305 | 31 | Kentucky | 4,641 |
| 3 | Florida | 41,061 | 32 | District of Columbia | 3,769 |
| 4 | New York | 26,948 | 33 | Iowa | 3,723 |
| 5 | Ohio | 17,864 | 34 | Arkansas | 3,220 |
| 6 | Arizona | 16,584 | 35 | Mississippi | 2,983 |
| 7 | Pennsylvania | 16,407 | 36 | New Mexico | 2,944 |
| 8 | Illinois | 15,783 | 37 | Kansas | 2,894 |
| 9 | Michigan | 14,784 | 38 | Delaware | 2,687 |
| 10 | Washington | 14,600 | 39 | Puerto Rico | 2,678 |
| 11 | Georgia | 13,917 | 40 | West Virginia | 2,365 |
| 12 | Virginia | 12,711 | 41 | Alaska | 2,338 |
| 13 | North Carolina | 12,282 | 42 | Idaho | 2,240 |
| 14 | New Jersey | 12,253 | 43 | Nebraska | 2,195 |
| 15 | Colorado | 11,475 | 44 | Hawaii | 1,954 |
| 16 | Indiana | 11,097 | 45 | South Dakota | 1,688 |
| 17 | Massachusetts | 9,915 | 46 | New Hampshire | 1,650 |
| 18 | Nevada | 9,893 | 47 | Maine | 1,626 |
| 19 | South Carolina | 9,736 | 48 | Montana | 1,571 |
| 20 | Maryland | 9,717 | 49 | Rhode Island | 1,425 |
| 21 | Tennessee | 8,484 | 50 | Wyoming | 828 |
| 22 | Missouri | 8,108 | 51 | North Dakota | 764 |
| 23 | Wisconsin | 7,683 | 52 | Vermont | 698 |
| 24 | Minnesota | 7,049 | 53 | U.S. Minor Outlying Islands | 145 |
| 25 | Oregon | 6,724 | 54 | Virgin Islands, U.S. | 126 |
| 26 | Alabama | 5,763 | 55 | Guam | 90 |
| 27 | Connecticut | 5,216 | 56 | American Samoa | 33 |
| 28 | Utah | 5,061 | 57 | Northern Mariana Islands | 16 |
| 29 | Oklahoma | 4,987 | | | |

## OVERALL STATE STATISTICS *continued*

**Losses by State***

| Rank | State | Loss | Rank | State | Loss |
|---|---|---|---|---|---|
| 1 | California | $2,159,454,513 | 30 | Louisiana | $78,286,085 |
| 2 | Texas | $1,021,547,286 | 31 | Oklahoma | $66,967,060 |
| 3 | Florida | $874,725,493 | 32 | Iowa | $59,829,482 |
| 4 | New York | $749,955,480 | 33 | Hawaii | $51,722,052 |
| 5 | New Jersey | $441,151,263 | 34 | Idaho | $50,631,580 |
| 6 | Pennsylvania | $360,334,651 | 35 | Kentucky | $48,746,051 |
| 7 | Illinois | $335,764,223 | 36 | Arkansas | $46,585,087 |
| 8 | Arizona | $324,352,644 | 37 | District of Columbia | $46,142,350 |
| 9 | Georgia | $301,001,997 | 38 | Montana | $45,554,368 |
| 10 | Washington | $288,691,091 | 39 | New Mexico | $45,127,386 |
| 11 | Virginia | $265,073,590 | 40 | Nebraska | $40,581,244 |
| 12 | Massachusetts | $235,890,173 | 41 | South Dakota | $35,855,494 |
| 13 | North Carolina | $234,972,238 | 42 | Delaware | $35,376,770 |
| 14 | Maryland | $221,520,527 | 43 | Mississippi | $32,144,078 |
| 15 | Michigan | $203,445,988 | 44 | Alaska | $31,771,278 |
| 16 | Nevada | $200,995,121 | 45 | Rhode Island | $31,586,831 |
| 17 | Ohio | $197,365,326 | 46 | Puerto Rico | $30,102,231 |
| 18 | Minnesota | $193,949,414 | 47 | New Hampshire | $27,178,268 |
| 19 | Colorado | $187,621,731 | 48 | West Virginia | $21,445,942 |
| 20 | Indiana | $162,259,036 | 49 | Maine | $18,968,567 |
| 21 | Tennessee | $161,195,036 | 50 | Wyoming | $13,746,109 |
| 22 | Oregon | $136,052,036 | 51 | North Dakota | $13,532,443 |
| 23 | Utah | $132,257,035 | 52 | Vermont | $ 8,818,181 |
| 24 | Missouri | $123,405,404 | 53 | U.S. Minor Outlying Islands | $3,588,797 |
| 25 | Connecticut | $120,767,349 | 54 | Virgin Islands, U.S. | $2,637,004 |
| 26 | South Carolina | $119,950,630 | 55 | Guam | $747,876 |
| 27 | Alabama | $96,479,649 | 56 | American Samoa | $327,467 |
| 28 | Kansas | $94,158,337 | 57 | Northern Mariana Islands | $25,917 |
| 29 | Wisconsin | $92,084,459 | | | |

## OVERALL STATE STATISTICS *continued*

| Complaints per Capita* | | | | | per 100,000 citizens |
|---|---|---|---|---|---|
| *Rank* | *State* | *Subjects* | *Rank* | *State* | *Subjects* |
| 1 | District of Columbia | 555.1 | 27 | West Virginia | 133.6 |
| 2 | Alaska | 318.8 | 28 | New Jersey | 131.9 |
| 3 | Nevada | 309.7 | 29 | Missouri | 130.9 |
| 4 | Delaware | 260.4 | 30 | Rhode Island | 130.0 |
| 5 | Arizona | 223.2 | 31 | Wisconsin | 130.0 |
| 6 | California | 198.3 | 32 | Pennsylvania | 126.6 |
| 7 | Colorado | 195.2 | 33 | Georgia | 126.2 |
| 8 | Washington | 186.9 | 34 | Illinois | 125.8 |
| 9 | South Dakota | 183.6 | 35 | Oklahoma | 123.0 |
| 10 | Florida | 181.6 | 36 | Minnesota | 122.8 |
| 11 | South Carolina | 181.2 | 37 | Tennessee | 119.0 |
| 12 | Indiana | 161.7 | 38 | New Hampshire | 117.7 |
| 13 | Oregon | 158.8 | 39 | Maine | 116.5 |
| 14 | Maryland | 157.2 | 40 | Iowa | 116.1 |
| 15 | Texas | 155.1 | 41 | Idaho | 114.0 |
| 16 | Ohio | 151.6 | 42 | North Carolina | 113.3 |
| 17 | Utah | 148.1 | 43 | Alabama | 112.8 |
| 18 | Michigan | 147.3 | 44 | Nebraska | 110.9 |
| 19 | Virginia | 145.8 | 45 | Vermont | 107.8 |
| 20 | Connecticut | 144.2 | 46 | Louisiana | 106.9 |
| 21 | Wyoming | 141.8 | 47 | Arkansas | 105.0 |
| 22 | Massachusetts | 141.6 | 48 | Kentucky | 102.5 |
| 23 | New Mexico | 139.2 | 49 | Mississippi | 101.5 |
| 24 | Montana | 138.7 | 50 | Kansas | 98.4 |
| 25 | New York | 137.7 | 51 | North Dakota | 97.5 |
| 26 | Hawaii | 136.2 | 52 | Puerto Rico | 83.5 |

## OVERALL STATE STATISTICS *continued*

| Losses per Capita* | | | | | per 100,000 citizens |
|---|---|---|---|---|---|
| *Rank* | *State* | *Loss* | *Rank* | *State* | *Loss* |
| 1 | District of Columbia | $6,795,914 | 27 | Illinois | $2,675,478 |
| 2 | Nevada | $6,292,550 | 28 | Idaho | $2,577,030 |
| 3 | California | $5,542,009 | 29 | Indiana | $2,364,534 |
| 4 | New Jersey | $4,748,238 | 30 | Wyoming | $2,353,556 |
| 5 | Arizona | $4,364,657 | 31 | Tennessee | $2,261,914 |
| 6 | Alaska | $4,332,018 | 32 | South Carolina | $2,232,240 |
| 7 | Montana | $4,021,353 | 33 | North Carolina | $2,168,543 |
| 8 | South Dakota | $3,900,228 | 34 | New Mexico | $2,134,317 |
| 9 | Utah | $3,869,729 | 35 | Nebraska | $2,051,237 |
| 10 | Florida | $3,868,631 | 36 | Michigan | $2,026,907 |
| 11 | New York | $3,831,931 | 37 | Missouri | $1,991,645 |
| 12 | Washington | $3,695,066 | 38 | New Hampshire | $1,938,461 |
| 13 | Hawaii | $3,603,978 | 39 | Alabama | $1,888,622 |
| 14 | Maryland | $3,584,328 | 40 | Iowa | $1,865,588 |
| 15 | Delaware | $3,428,347 | 41 | North Dakota | $1,726,240 |
| 16 | Minnesota | $3,380,137 | 42 | Louisiana | $1,711,639 |
| 17 | Massachusetts | $3,369,186 | 43 | Ohio | $1,674,584 |
| 18 | Texas | $3,348,973 | 44 | Oklahoma | $1,651,948 |
| 19 | Connecticut | $3,338,719 | 45 | Wisconsin | $1,557,861 |
| 20 | Oregon | $3,213,809 | 46 | Arkansas | $1,518,551 |
| 21 | Kansas | $3,202,070 | 47 | Puerto Rico | $1,479,384 |
| 22 | Colorado | $3,192,143 | 48 | Vermont | $1,361,957 |
| 23 | Virginia | $3,041,335 | 49 | Maine | $1,359,051 |
| 24 | Rhode Island | $2,882,110 | 50 | West Virginia | $1,211,587 |
| 25 | Pennsylvania | $2,779,999 | 51 | Mississippi | $1,093,451 |
| 26 | Georgia | $2,729,130 | 52 | Kentucky | $1,076,986 |

## 2023 CRIME TYPES continued

### 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 |

## 2023 CRIME TYPES

### By Complaint Count

| Crime Type | Complaints | Crime Type | Complaints |
|---|---|---|---|
| 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 |

# Internet Crimes Complaint Center (IC3.gov)

- Powerful Investigative Tool
- Overlapping Complaint
- Suspect info (email, address, phone)
- Investigator sees bigger picture
- Map out criminal organization
- Identify unwitting participants


YOUR FILES ARE ENCRYPTED
Your photos, documents and other important files have been encrypted with unique key, generated for this computer.
NEXT

# Ransomware Basics


- Malware that infects computers, networks and services.
- The Malware encrypts victim's data making them unreadable.
- Actor demands payment to decrypt files.
- There are many variants of ransomware.

.CryptoHasYou., 777, 7ev3n, 7h9r, 8lock8, **Alfa Ransomware**, **Alma Ransomware**, Alpha Ransomware, AMBA, Apocalypse, ApocalypseVM, AutoLocky, BadBlock, BaksoCrypt, Bandarchor, Bart, BitCryptor, BitStak, BlackShades Crypter, Blocatto, Booyah, Brazilian, BrLock, Browlock, Bucbi, BuyUnlockCode, Cerber, Chimera, CoinVault, Coverton, Cryaki, Crybola, CryFile, CryLocker, **CrypMIC**, Crypren, Crypt38, Cryptear, **CryptFile2**, CryptInfinite, CryptoBit, CryptoDefense, CryptoFinancial, CryptoFortress, CryptoGraphic Locker, CryptoHost, CryptoJoker, **CryptoLocker**, Cryptolocker 2.0, CryptoMix, CryptoRoger, CryptoShocker, CryptoTorLocker2015, CryptoWall 1, CryptoWall 2, CryptoWall 3, CryptoWall 4, CryptXXX, CryptXXX 2.0, CryptXXX 3.0, **CryptXXX 3.1**, CTB-Faker, **CTB-Locker**, CTB-Locker WEB, CuteRansomware, DeCrypt Protect, DEDCryptor, DetoxCrypto, DirtyDecrypt, DMALocker, DMALocker 3.0, Domino, EDA2 / HiddenTear, EduCrypt, El-Polocker, Enigma, FairWare, Fakben, Fantom, Fonco, Fsociety, Fury, GhostCrypt, Globe, GNL Locker, Gomasom, Goopic, Gopher, Harasom, Herbst, Hi Buddy!, Hitler, HolyCrypt, HydraCrypt, iLock, iLockLight, International Police Association, JagerDecryptor, Jeiphoos, Jigsaw, Job Crypter, **KeRanger**, KeyBTC, KEYHolder, KimcilWare, Korean, Kozy.Jozy, KratosCrypt, KryptoLocker, LeChiffre, Linux.Encoder, Locker, **Locky**, Lortok, LowLevel04, Mabouia, Magic, MaktubLocker, MIRCOP, MireWare, Mischa, MM Locker, Mobef, NanoLocker, Nemucod, NoobCrypt, Nullbyte, ODCODC, Offline ransomware, OMG! Ransomware, Operation Global III, PadCrypt, Pclock, **Petya**, PizzaCrypts, PokemonGO, PowerWare, PowerWorm, PRISM, R980, RAA encryptor, Radamant, Rakhni,, Rannoh, Ransom32, RansomLock, Rector, RektLocker, RemindMe, Rokku, Samas-Samsam, Sanction, Satana, Scraper, Serpico, Shark, ShinoLocker, Shujin, Simple_Encoder, SkidLocker / Pompous, Smrss32, SNSLocker, Sport, Stampado, Strictor, Surprise, SynoLocker, SZFLocker, TeslaCrypt 0.x - 2.2.0, TeslaCrypt 3.0+, TeslaCrypt 4.1A, TeslaCrypt 4.2, Threat Finder, **TorrentLocker**, TowerWeb, Toxcrypt, Troldesh, TrueCrypter, Turkish Ransom, UmbreCrypt, Ungluk, Unlock92, VaultCrypt, VenusLocker, Virlock, Virus-Encoder, WildFire Locker, Xorist, XRTN, Zcrypt, **Zepto**, Zimbra, Zlader / Russian, Zyklon

# State of Ransomware - Sophos



# Ransomware – Phases of Attack

**Step 01**

**Email**

Given the volume of email, even a small percent of evasion translates to malicious email getting through to users

**Step 02**

**User Clicks and Attack Begins**

Without URL filtering to prevent users going to malicious sites or proper endpoint protection to prevent malicious file detection and execution, an attack is unsuspectingly launched

**Step 03**

**Worms Network**

Without anomaly or heuristic detection and prevention, attack hunts for key data, folders and disables backup and recovery mechanisms

**Step 04**

**Command & Control and Encrypts**

When ready, establishes command and control to communicate back to the attacker and encrypts files

**Step 05**

**Lateral Movement**

Without segmentation in place to isolate systems, encryption spreads laterally and hunts for other connected networks


Your files have been encrypted.
Your computer has been hacked
and you will not be able to access your data.
If you pay $5 million to us within 48 hours,
you will be able to regain access to your data.
Decrypt
CNN

# Protect Against Ransomware

- **Immediate Actions You Can Take Now to Protect Against Ransomware:**
- Update your operating system and software.
- Implement user training and phishing exercises to raise awareness about the risks of suspicious links and attachments.
- If you use Remote Desktop Protocol (RDP), secure and monitor it.
- Make an offline backup of your data.
- Use multifactor authentication (MFA).

# Ransomware-as-a-Service

## Ransomware as a service is the new big problem for business

Easy-to-use ransomware as a service schemes are booming, accounting for almost two-thirds of ransomware campaigns during the past year, warn researchers.

By Danny Palmer | March 4, 2021 -- 12:31 GMT (04:31 PST) | Topic: Security


Ransomware as a service is proving effective for cyber criminals who want a piece of the cyber-extortion action but without necessarily having the skills to develop their own malware, with two out of three attacks using this model.

Ransomware attacks are still proving extremely lucrative, with the most well-organised gangs earning millions per victim, so many cyber criminals want to cash in – but don't have the ability to code and distribute their own campaigns.

MORE FROM DANNY PALMER

Security
Ransomware: A company paid millions to get their data back, but forgot to do one thing. So the hackers came back again

Security
VPNs, two-factor-authentication and more: Keeping your data safe from hackers while working from home

Security
Hacked companies had backup plans. But they didn't print them out before the attack.

# Purchase Order Fraud Basics


- University or corporate identities are impersonated to obtain merchandise on credit.
- Merchandise is shipped before the victim vendor discovers the fraud.
- Scammers operate primarily from Nigeria or outside of U.S. Jurisdiction. University or corporate identities are impersonated to obtain merchandise on credit.

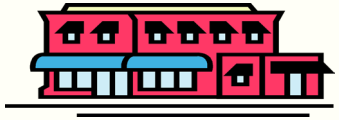
# How the Scam Works:


Imposter domain and VoIP phone numbers are established

Establish US address to receive and re-ship products


Email & fraudulent Purchase Orders sent to US vendors – net 30 day credit


Vendor bills impersonated company or university



Victim Vendor

US Business ships products to US address (re-shipper)

Merchandise received at US address (re-shipper)

US Freight Forwarder ships to Nigeria, often through the UK

# Victims are targeted after uploading resumes online

- Monster
- LinkedIn
- Indeed
- Career Builder
- Dice
- Zip Recruiter

# Jobs Offered by Scammers are…

- Reshipping Managers
- Package Processing
- Package compliance officer
- Logistics Coordinator

# Payment

- Western Union
- Money Gram
- Wire Transfer
- Crypto Currency

# Encouraged to…

- Find Office Space
- Find Storage Units
- Not tell others what they do

# What can be done?

Find out where packages were sent and get them returned.

Disrupt organization by preventing shipment.

Return hundreds of thousands of dollars to local victim business.

Even make arrests in Nigeria.

# Prince Oseph

# Business Email Compromise

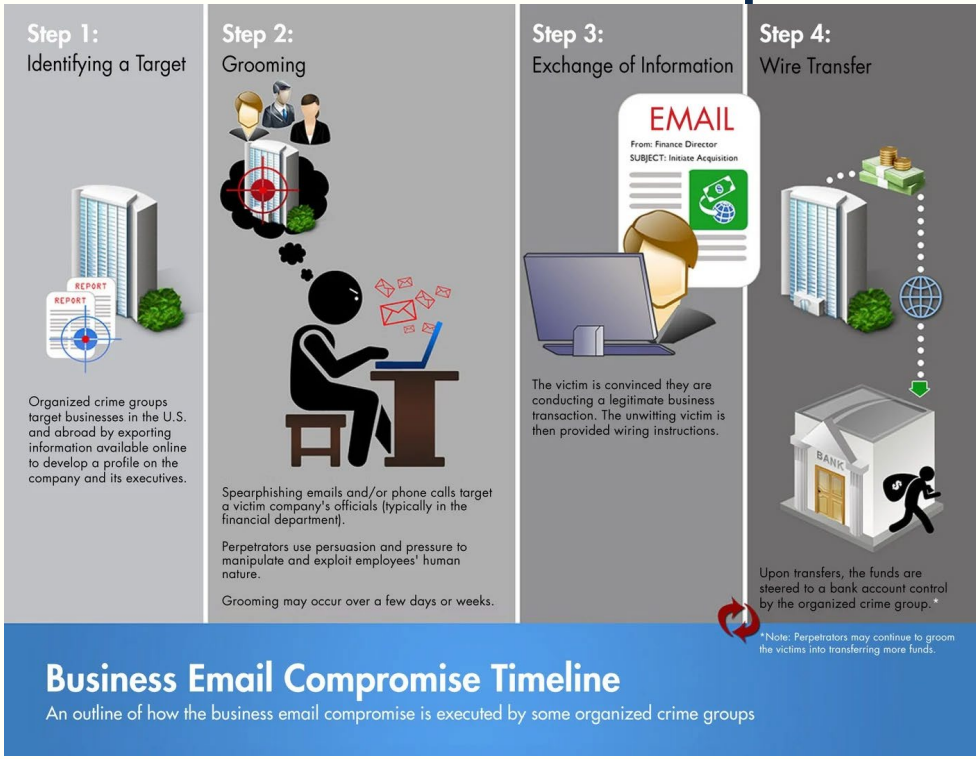

- Business email compromise (BEC) is an exploit in which an attacker obtains access to a business email account and imitates the owner's identity, in order to defraud the company and its employees, customers or partners.

  -Barracuda Networks

# Business Email Compromise


- **Spoof an email account or website.** Slight variations on legitimate addresses (john.kelly@examplecompany.com vs. john.kelley@examplecompany.com) fool victims into thinking fake accounts are authentic.
- **Send spearphishing emails.** These messages look like they're from a trusted sender to trick victims into revealing confidential information. That information lets criminals access company accounts, calendars, and data that gives them the details they need to carry out the BEC schemes.
- **Use malware.** Malicious software can infiltrate company networks and gain access to legitimate email threads about billing and invoices. That information is used to time requests or send messages so accountants or financial officers don't question payment requests. Malware also lets criminals gain undetected access to a victim's data, including passwords and financial account information. (FBI.gov)

# Business Email Compromise




(FBI.gov)

# Business Email Compromise

## How to Protect Yourself

- Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.
- Don’t click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company’s phone number on your own (don’t use the one a potential scammer is providing), and call the company to ask if the request is legitimate.
- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.
- Be careful what you download. Never open an email attachment from someone you don't know, and be wary of email attachments forwarded to you.
- Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.
- Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request.
- Be especially wary if the requestor is pressing you to act quickly. (FBI.gov)

# Financial Fraud Kill Chain (FFKC)

The FFKC can be initiated for international wires only.

- Normal bank procedure still apply to recovery
- Wire transfer is >$50,000
- International destination
- SWIFT recall notice has been initiated
- Wire transfer has been initiated with the last 72 hours

# FFKC Domestic

- Initiated through the FBI Recovery Asset Team at IC3
- Time is of the essence
- At least $50,000
- Less than 72 hours prior
- Transfer was sent between two US banking institutions

# Passwords


TWONKS
WHAT'S THE WI-FI PASSWORD AGAIN?
IT'S OUR ANNIVERSARY
SNEL.SE

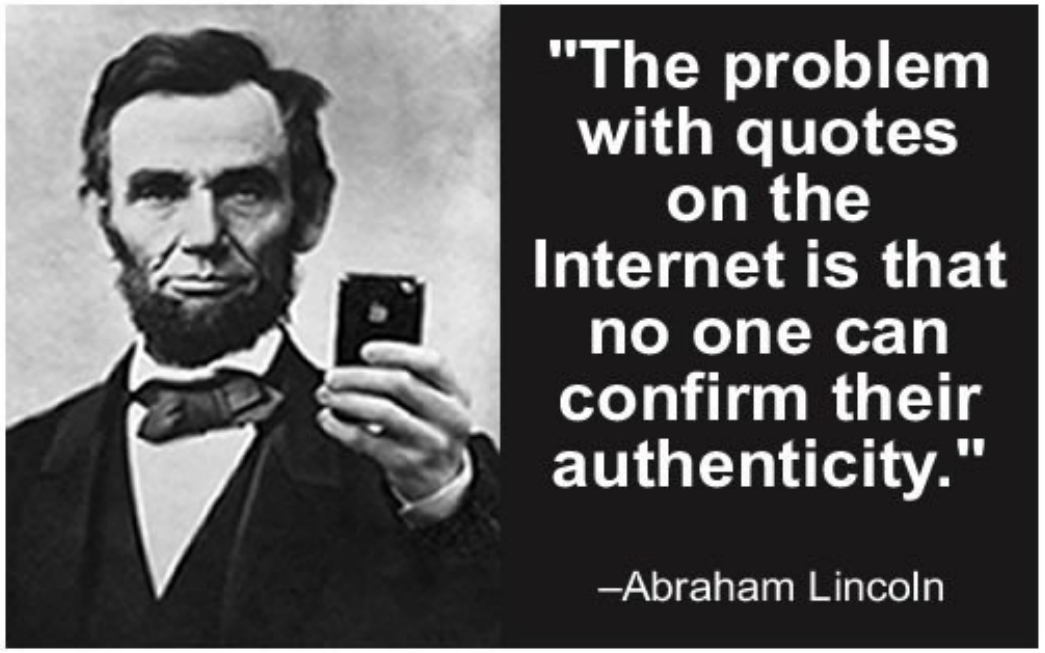
# Crypto Investment Scams

Cryptocurrency investment fraud, which the media commonly describes as "pig butchering," is one of the most prevalent and damaging fraud schemes today.

Scammers, through various means of manipulation, convince victims to deposit more and more money into financial “investments” using cryptocurrency. In truth, these investments are fake; all victim money is under the control of—and ultimately stolen by—criminal actors, usually overseas. As a result, victims typically lose all money they invested.

(FBI.gov)

# In Conclusion



# Questions?

Sgt. Jeff Plank - jplank@utah.gov

Agent Scott Pugmire - spugmire@utah.gov