K2’s Ripped From The Headlines – Outrageous Tales Of Cybercrimes

Session Description

Remote work environments have created many new opportunities for cybercriminals and other fraudsters to exploit, and accounting professionals are some of the most commonly targeted individuals. This session is a series of case studies that examine actual criminal filings and news accounts and use them to highlight some of the actions you can take to limit your exposure to similar schemes. Attend this session and learn more about how high-profile control failures occurred so you can be more effective at preventing crimes in your organization.

Major Topics

- Common security weaknesses which occur with hardware and software at home and in the office
- Malware, ransomware, data breach, and incident response tips
- Internal control failures that resulted in the theft of assets or unauthorized manipulation of data
- User authentication and security awareness training

Learning Objectives

- List at least three major security incidents reported in the headlines in the last year, and explain at least one primary internal control design or operation flaws that allowed the hack to occur
- Select the correct definitions for security terms such as attack surface, vulnerability, exploit, social engineering, phishing, malware, heuristics, biometrics, and multi-factor authentication (MFA)
- List at least three best practices learned by reviewing the control failures cited in the case studies

What We Didn’t Cover This Year

- **USA vs. Sam Bankman-Fried and FTX (Crypto)** – We didn’t cover this because, upon further exploration of the court pleadings, we discovered that the allegations describe a failure of basic custody controls in the company as opposed to some kind of weakness in security procedures and practices

Overview Of Topics

- Tech Support Scams Target the Elderly
- Deepfakes and Cybercrime: A Growing Threat
- Browser Fingerprint Impersonation
- Ransomware Attacks Many Old Bugs
- Incident Response Basics

ZD
NET

my central jersey
PART OF THE USA TODAY NETWORK

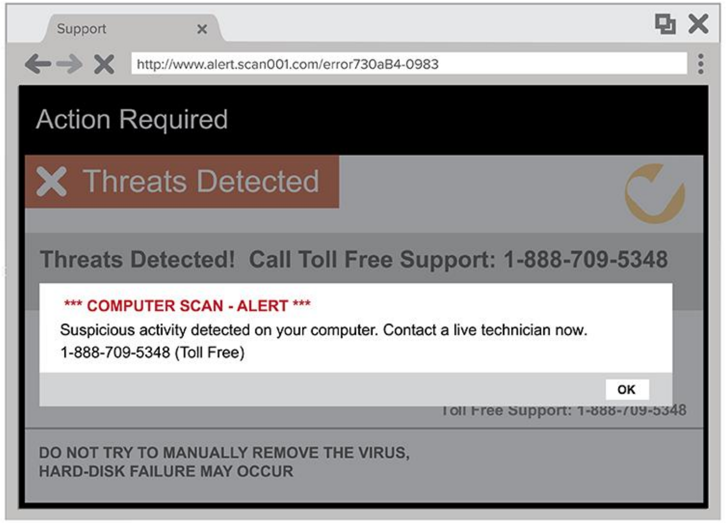
"FBI Warning: PC and Tech Support Scams Are Back", ZDNet 11/16/2022

"Edison Woman Pleads Guilty in Multimillion Dollar Computer Tech Support Scam", MyCentralJersey.com, 12/22/2022

TECH SUPPORT SCAMS TARGET THE ELDERLY

What Happened?

- Scammers caused popups to appear at websites frequented by senior citizens which told them that there were errors or even viruses on their device
- The popups used alarming phrases like:
  - *"Suspicious activity detected on your computer, Contact a live technician now at (toll free number)"*
  - *"WARNING YOUR DEVICE IS INFECTED WITH MANY TROJANS. FIREWALL IS AT 5 PERCENT. CALL CERTIFIED TECHNICIANS (Toll free number) IMMEDIATELY TO PREVENT DATA LOSS"*



Action Required

Threats Detected

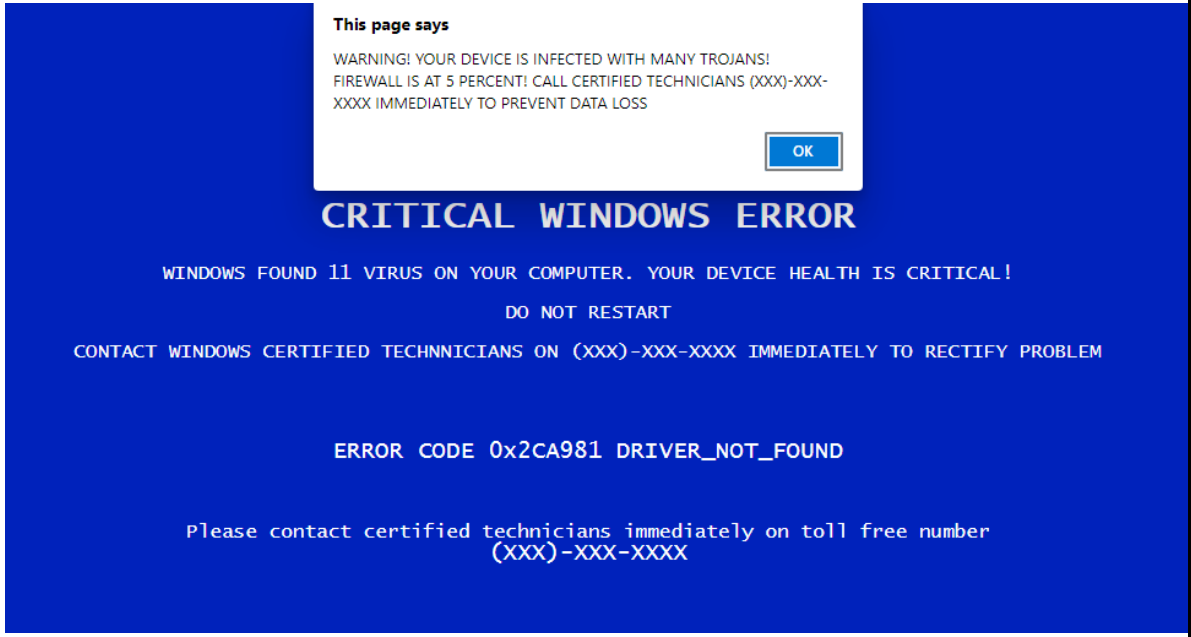
Threats Detected! Call Toll Free Support: 1-888-709-5348

*** COMPUTER SCAN - ALERT ***

Suspicious activity detected on your computer. Contact a live technician now.
1-888-709-5348 (Toll Free)

Toll Free Support: 1-888-709-5348

DO NOT TRY TO MANUALLY REMOVE THE VIRUS,
HARD-DISK FAILURE MAY OCCUR


This page says

WARNING! YOUR DEVICE IS INFECTED WITH MANY TROJANS! FIREWALL IS AT 5 PERCENT! CALL CERTIFIED TECHNICIANS (XXX)-XXX-XXXX IMMEDIATELY TO PREVENT DATA LOSS

CRITICAL WINDOWS ERROR

WINDOWS FOUND 11 VIRUS ON YOUR COMPUTER. YOUR DEVICE HEALTH IS CRITICAL!

DO NOT RESTART

CONTACT WINDOWS CERTIFIED TECHNICIANS ON (XXX)-XXX-XXXX IMMEDIATELY TO RECTIFY PROBLEM

ERROR CODE 0x2CA981 DRIVER_NOT_FOUND

Please contact certified technicians immediately on toll free number
(XXX)-XXX-XXXX

Sources: US FTC (link), Wikipedia (link)

What Happened?

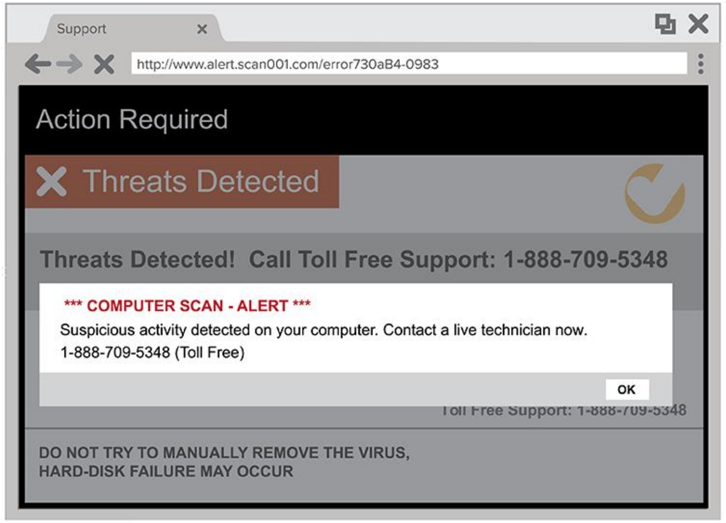
- Once the victims called the “help line”, the victims were immediately told that there is a severe problem with their computer
- In many cases, the perpetrators identified themselves as employees of software companies like Microsoft or Apple, or as employees of Dell, Lenovo, or other computer companies

Recorded FTC Undercover Investigator Call
Tech Support Scam

Source: US FTC

What Happened?

- Scammers then ask you to give them remote access to your computer and pretend to run a diagnostic test
- They then ask you to pay them to fix a nonexistent problem on your computer which requires you to install an application – which is often said to be “antivirus” – and often is a backdoor, ransomware, or other malware – which often also pops up scary warning messages, requiring additional calls for more paid “fixes”



Action Required

Threats Detected

Threats Detected! Call Toll Free Support: 1-888-709-5348

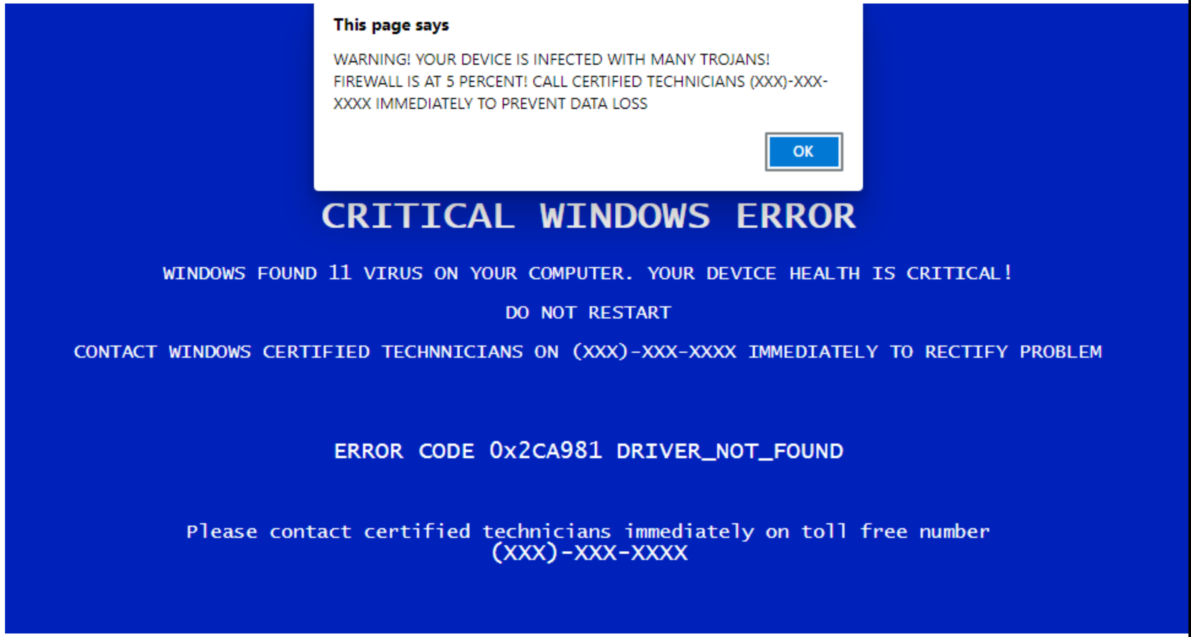
*** COMPUTER SCAN - ALERT ***

Suspicious activity detected on your computer. Contact a live technician now.
1-888-709-5348 (Toll Free)

OK

Toll Free Support: 1-888-709-5348

DO NOT TRY TO MANUALLY REMOVE THE VIRUS,
HARD-DISK FAILURE MAY OCCUR



This page says

WARNING! YOUR DEVICE IS INFECTED WITH MANY TROJANS! FIREWALL IS AT 5 PERCENT! CALL CERTIFIED TECHNICIANS (XXX)-XXX-XXXX IMMEDIATELY TO PREVENT DATA LOSS

OK

CRITICAL WINDOWS ERROR

WINDOWS FOUND 11 VIRUS ON YOUR COMPUTER. YOUR DEVICE HEALTH IS CRITICAL!

DO NOT RESTART

CONTACT WINDOWS CERTIFIED TECHNICIANS ON (XXX)-XXX-XXXX IMMEDIATELY TO RECTIFY PROBLEM

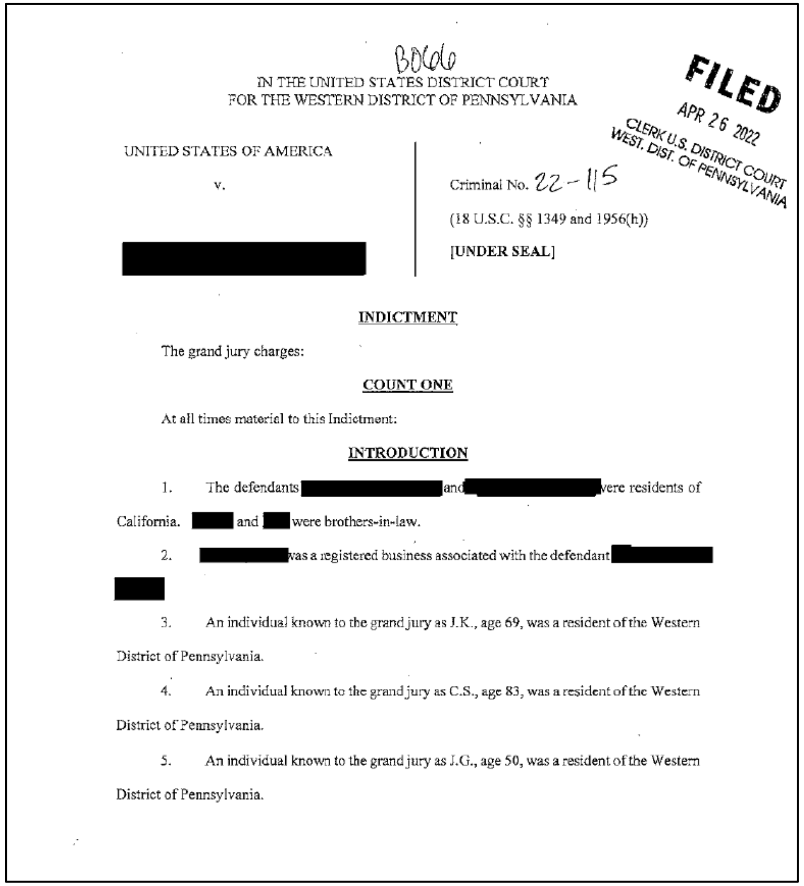
ERROR CODE 0x2CA981 DRIVER_NOT_FOUND

Please contact certified technicians immediately on toll free number
(XXX)-XXX-XXXX

Sources: US FTC (link), Wikipedia (link)

Actions Alleged In A Current Case

- Victims contacted via telephone, e-mail, or pop-up message with a toll-free number
- Once victims called the toll-free number, they were convinced by perp that their bank and financial accounts were compromised
- The perps then
  - Convinced victims to install remote access software on their computer
  - Extracted any personal identifying information available and set up new e-mail accounts and bank accounts in the name of the victim but controlled by the perps
  - Transferred funds from existing bank accounts to new bank accounts controlled by the perps without the victim's knowledge



BD66

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

FILED
APR 26 2022
CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

UNITED STATES OF AMERICA

v.

[redacted]

Criminal No. 22-115

(18 U.S.C. §§ 1349 and 1956(h))

[UNDER SEAL]

INDICTMENT

The grand jury charges:

COUNT ONE

At all times material to this Indictment:

INTRODUCTION

1. The defendants [redacted] and [redacted] were residents of California. [redacted] and [redacted] were brothers-in-law.

2. [redacted] was a registered business associated with the defendant [redacted]

3. An individual known to the grand jury as J.K., age 69, was a resident of the Western District of Pennsylvania.

4. An individual known to the grand jury as C.S., age 83, was a resident of the Western District of Pennsylvania.

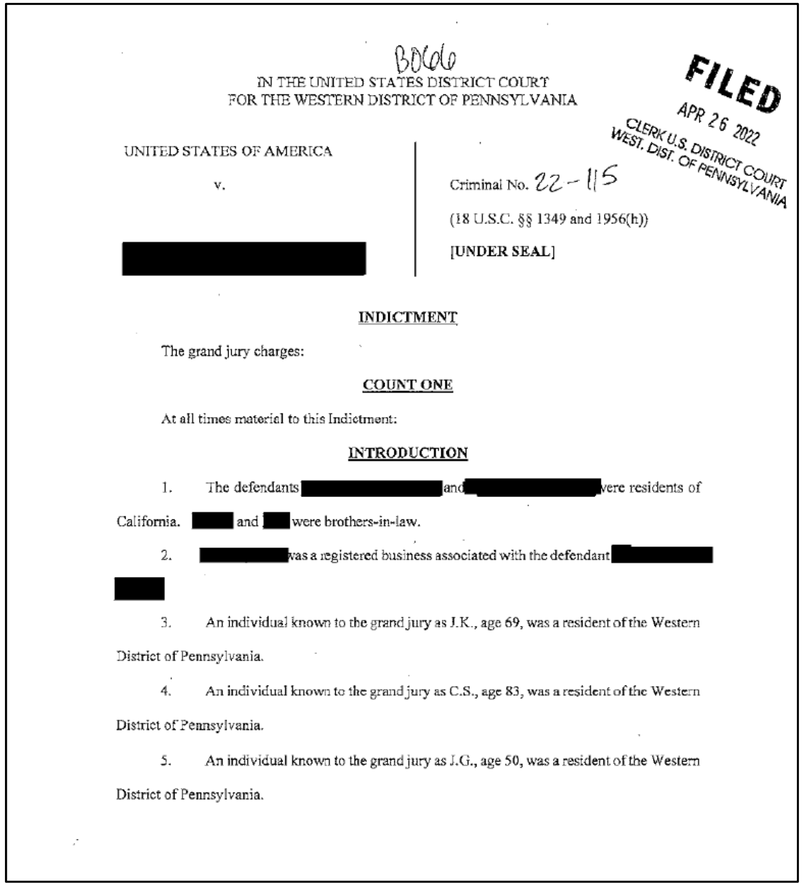
5. An individual known to the grand jury as J.G., age 50, was a resident of the Western District of Pennsylvania.

Source: Indictment in USDC W-PA in case 2:22-cr-00115-NR from pacer.gov

Names are redacted here since case is pending

Actions Alleged In A Current Case

- Victims were instructed to
  - Send funds to cryptocurrency wallets controlled by the perps
  - Purchase commercially available debit cards including Green Dot cards
  - Pay perp’s personal bills and mortgage
- The crew executing this scam was global, with operations in US, India, and Vietnam



BDC66

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

FILED
APR 26 2022
CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

UNITED STATES OF AMERICA

v.

[redacted]

Criminal No. 22-115

(18 U.S.C. §§ 1349 and 1956(h))

[UNDER SEAL]

INDICTMENT

The grand jury charges:

COUNT ONE

At all times material to this Indictment:

INTRODUCTION

1. The defendants [redacted] and [redacted] were residents of California. [redacted] and [redacted] were brothers-in-law.

2. [redacted] was a registered business associated with the defendant [redacted]

3. An individual known to the grand jury as J.K., age 69, was a resident of the Western District of Pennsylvania.

4. An individual known to the grand jury as C.S., age 83, was a resident of the Western District of Pennsylvania.

5. An individual known to the grand jury as J.G., age 50, was a resident of the Western District of Pennsylvania.

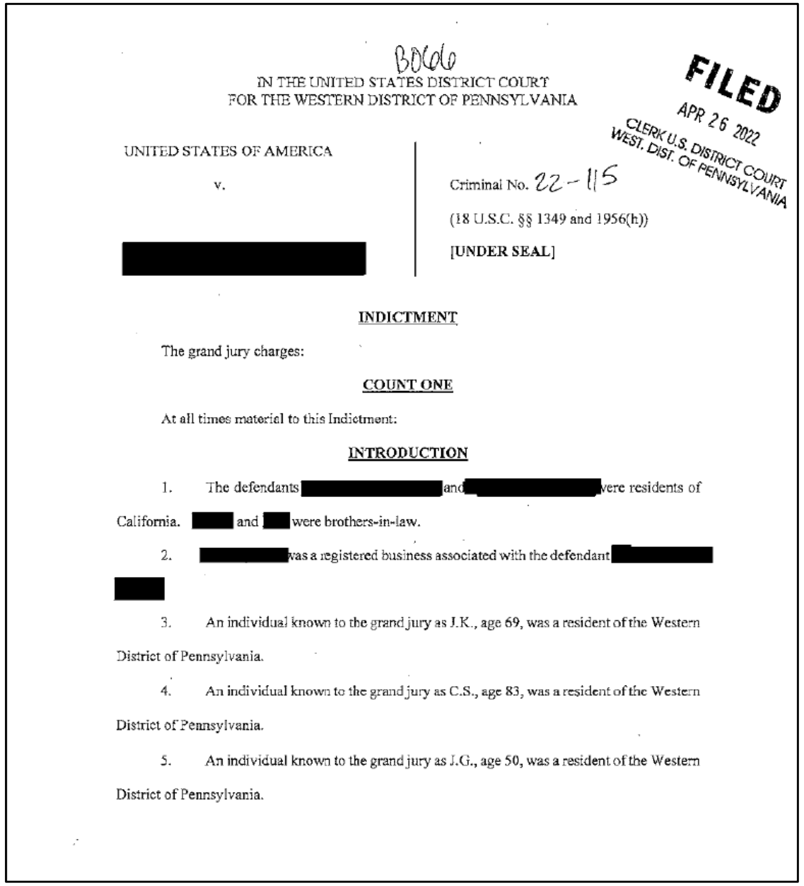
Source: Indictment in USDC W-PA in case 2:22-cr-00115-NR from pacer.gov

Names are redacted here since case is pending

Actions Alleged In A Current Case

The Story of "CS"

- Victim "CS" receives a popup message on his computer and calls the number
- Perp convinces CS that his computer is infected and transfers to "Alan Maxwell"
- "Maxwell" explains that CS's identity has been compromised and they needed to IMMEDIATELY move money out of retirement accounts into CS's bank account
- Maxwell then convinces CS to install remote access software on his computer
- On October 21, 2021, Maxwell directed CS to photograph CS's PA drivers license and create a new Gmail account in CS's name



BDCdo

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

FILED
APR 26 2022
CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

UNITED STATES OF AMERICA

v.

[redacted]

Criminal No. 22-115
(18 U.S.C. §§ 1349 and 1956(h))
[UNDER SEAL]

INDICTMENT

The grand jury charges:

COUNT ONE

At all times material to this Indictment:

INTRODUCTION

1. The defendants [redacted] and [redacted] vere residents of California. [redacted] and [redacted] were brothers-in-law.

2. [redacted] was a registered business associated with the defendant [redacted] [redacted]

3. An individual known to the grand jury as J.K., age 69, was a resident of the Western District of Pennsylvania.

4. An individual known to the grand jury as C.S., age 83, was a resident of the Western District of Pennsylvania.

5. An individual known to the grand jury as J.G., age 50, was a resident of the Western District of Pennsylvania.

Source: Indictment in USDC W-PA in case 2:22-cr-00115-NR from pacer.gov

Names are redacted here since case is pending

Actions Alleged In A Current Case

The Story of “CS”, continued

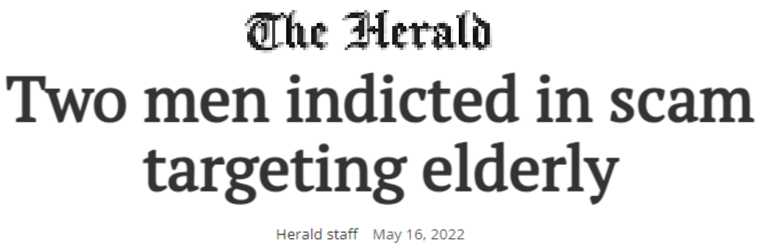
- Between 10/12/2021 and 11/19/2021, perps allegedly caused CS to liquidate $1.28 million which was transferred to accounts that were controlled by the perp and their co-conspirators

Date	Wire Amount	Beneficiary Account
10/21/2021	$63,000	PMDC, LLC
10/22/2021	$98,000	Payward Ventures
10/28/2021	$125,000	Prime Trust, LLC
10/30/2021	$278,000	Prime Trust, LLC
11/10/2021	$293,680	Prime Trust, LLC
11/17/2021	$274,500	Bittrex, Inc.
11/19/2021	$155,893	Bitstamp USA

Source: Indictment in USDC W-PA in case 2:22-cr-00115-NR from pacer.gov

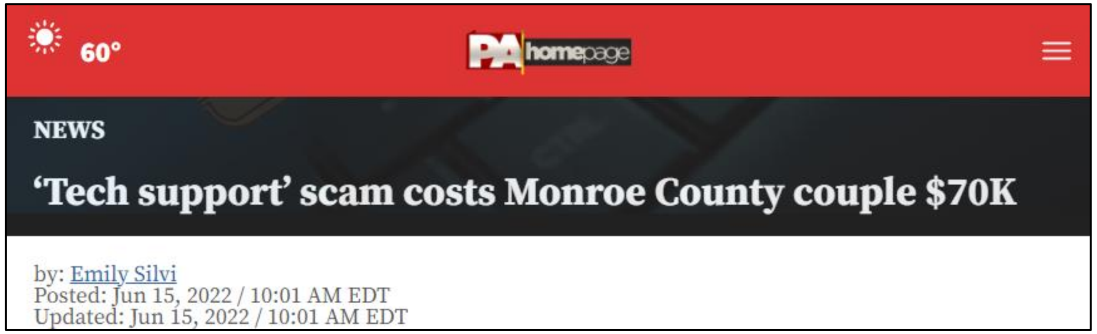
What Happened?

- Many senior citizens across North America have fallen victim to similar scams
- Many of you may know someone (as I do) who has fallen victim to such a scam and has been financially wiped out at the time their life savings is needed the most


The Herald

Two men indicted in scam targeting elderly

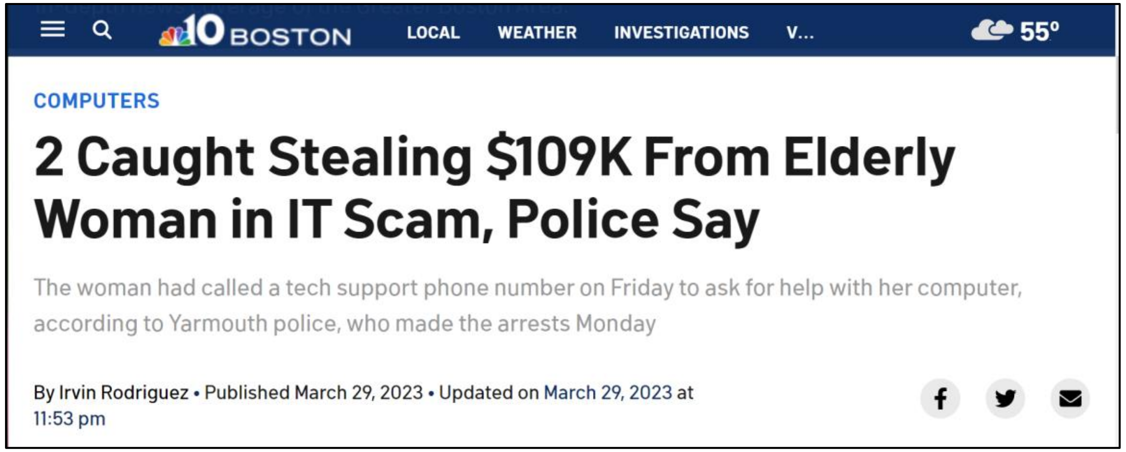
Herald staff May 16, 2022



NEWS

'Tech support' scam costs Monroe County couple $70K

by: Emily Silvi
Posted: Jun 15, 2022 / 10:01 AM EDT
Updated: Jun 15, 2022 / 10:01 AM EDT



COMPUTERS

2 Caught Stealing $109K From Elderly Woman in IT Scam, Police Say

The woman had called a tech support phone number on Friday to ask for help with her computer, according to Yarmouth police, who made the arrests Monday

By Irvin Rodriguez • Published March 29, 2023 • Updated on March 29, 2023 at 11:53 pm

Six Common Scams Affecting Senior Citizens

- **Tech Support:** Scammers pose as tech support and offer to fix computer problems that are not real. They ask targets to give them access to their computer and steal their personal information.
- **Posing as Utility Companies**: The scammer threatens to shut off utility service if a payment is not made immediately.
- **Online Shopping:** Scammers pretend to be a real business but have a fake website or a fake ad on a genuine retailer's site.
- **Business Imposters**: Scammers send emails or text messages pretending to be a major retailer to get your money or personal information.

Source: *Press Release, "Two Californians Indicted in Multi-Million Dollar Tech-Support Scam Targeting Elderly Victim"*, **US Atty, Western District of PA, 5/12/2022**

Six Common Scams Affecting Senior Citizens

- **Government Impersonation**: Scammers pose as government employees and threaten to arrest or prosecute targets unless they agree to pay an amount claimed to be owed to the government.
- **Romance Scams**: Scammers pose as interested romantic partners and convince targets to give them money for various fictitious reasons.

*US Victims of financial fraud are encouraged to call the **US Department of Justice's Elder Fraud Hotline** at **(833)372-8311**.*

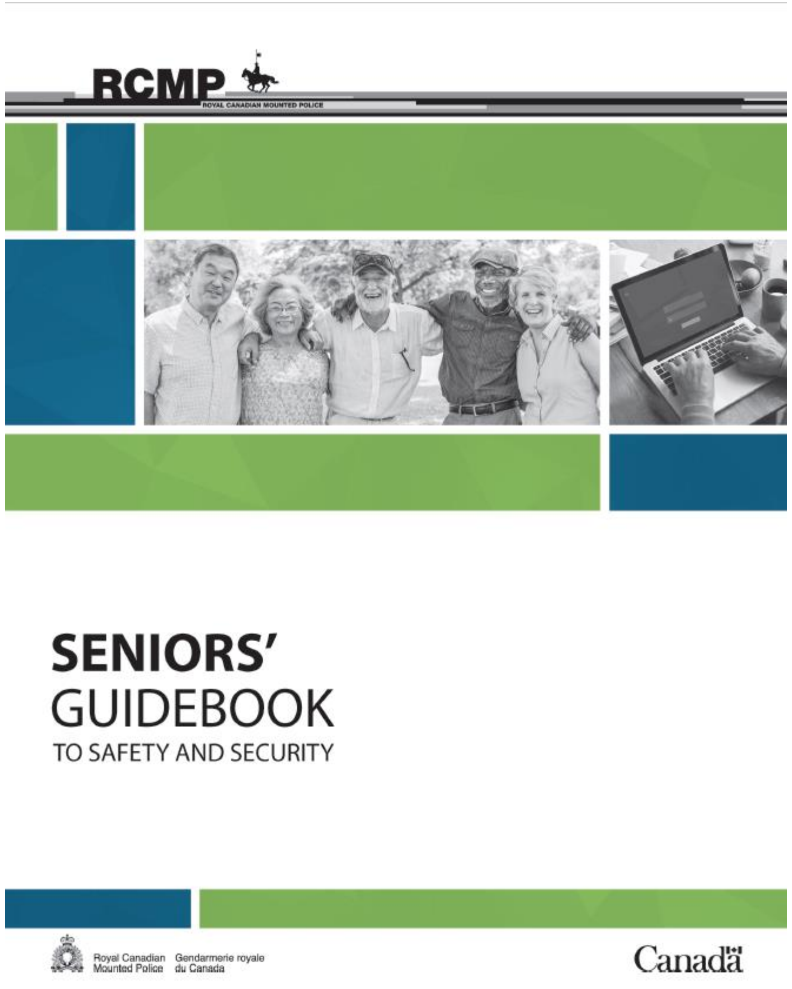
*Canadian victims of fraud are encouraged to contact the **Canadian Anti-Fraud Centre** at **(888)495-8501**.*

RCMP has created a guidebook for seniors on safety and security which can be downloaded as a PDF for free

Source: *Press Release, "Two Californians Indicted in Multi-Million Dollar Tech-Support Scam Targeting Elderly Victim"*, **US Atty, Western District of PA, 5/12/2022**

Help For Canadian Seniors

- Many senior citizens across North America have fallen victim to similar scams
- Many of you may know someone (as I do) who has fallen victim to such a scam and has been financially wiped out at the time their life savings is needed the most
- RCMP has a Senior’s Guidebook to Safety and Security for free (PDF) from their website – or a paper one can be purchased for your loved one by calling (888) 562-5561



RCMP

ROYAL CANADIAN MOUNTED POLICE

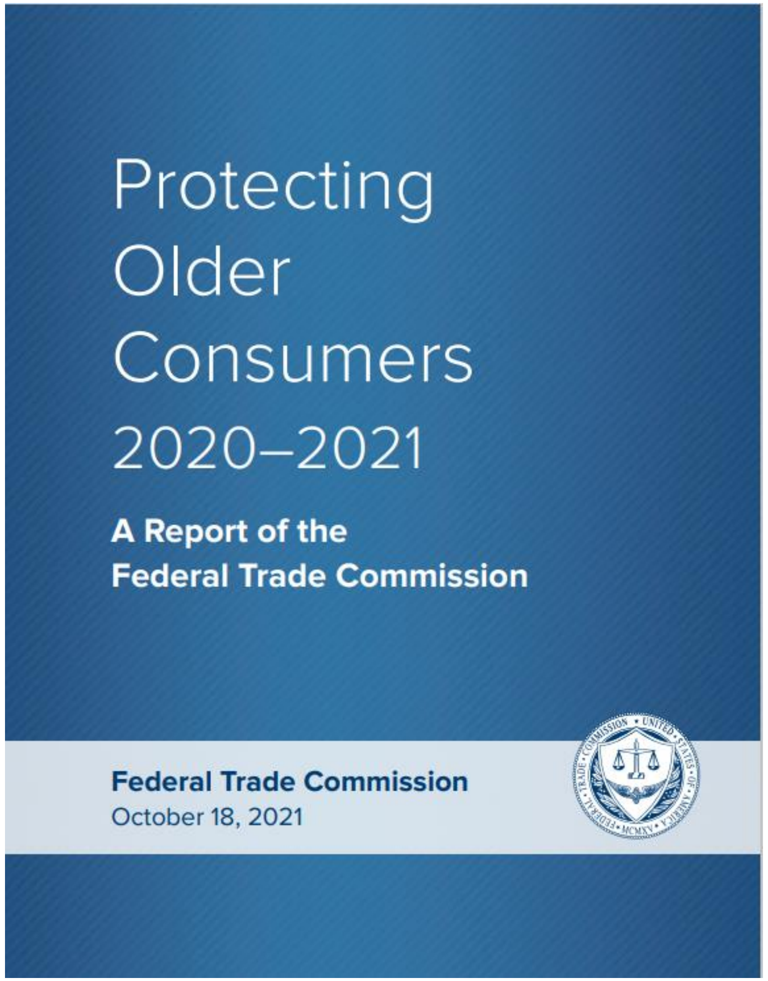
SENIORS’
GUIDEBOOK
TO SAFETY AND SECURITY

Royal Canadian Mounted Police Gendarmerie royale du Canada

Canadä

Help For US Seniors

- A US FTC report details some of the scams perpetrated on Seniors in 2020-2021. These included:
  - Fraudulent investments “guaranteed” to beat the market
  - Credit Card Stacking to pay for pricey training and coaching programs
  - Deceptive TV antenna marketing
  - Unsubstantiated COVID-19 health treatments
  - Fraudulent stem cell therapies for joint pain/arthritis
  - Fraudulent health claims about the benefits of using CBD products and other supplements



Protecting Older Consumers 2020–2021

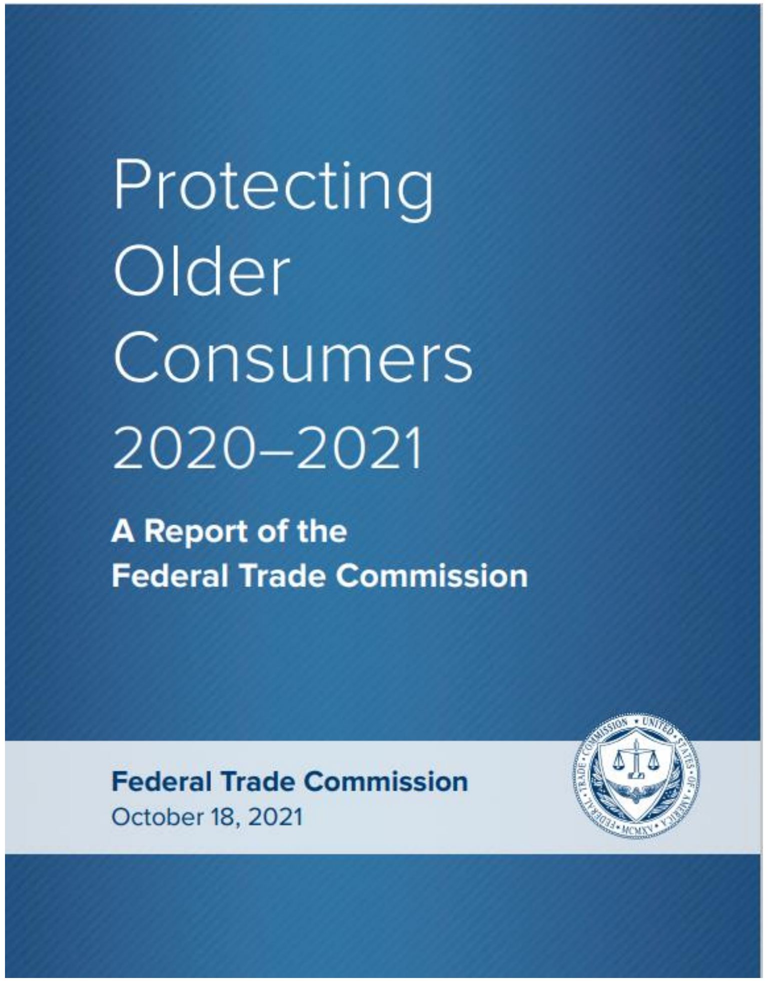
A Report of the Federal Trade Commission

Federal Trade Commission
October 18, 2021

Source: US Federal Trade Commission

Help For US Seniors

- FTC also works with criminal authorities on fraud cases affecting seniors, including:
  - Romance scams
  - Sweepstakes, prize, and lottery scams
  - Tech support scams
  - Impersonation of friends and family
- FTC requests that you report any suspicious activities to their fraud website, ReportFraud.FTC.gov.
- You can also register phone numbers to be on the FTC's "do not call" registry at www.DoNotCall.gov



Protecting Older Consumers 2020–2021

A Report of the Federal Trade Commission

Federal Trade Commission
October 18, 2021

Source: US Federal Trade Commission

TECH MONITOR

How-To Geek

“Scammers Created an AI Hologram of Me to Scam Unsuspecting Projects”, Binance Blog, 8/17/2022

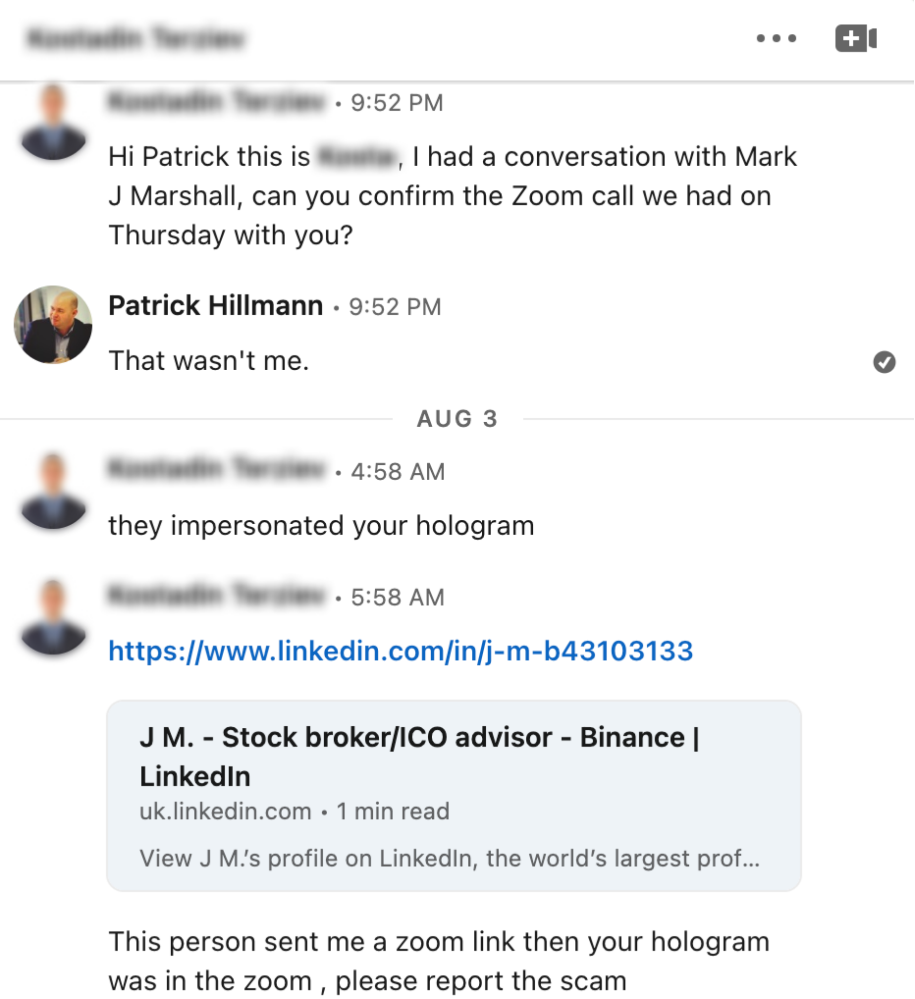
“Will Deepfake Cybercrime Ever Go Mainstream?”, Techmonitor.ai, 10/31/2022

“How Deepfakes Are Powering a New Type of Cyber Crime”, HowtoGeek.com, 7/23/2021

BINANCE CHIEF COMMUNICATIONS OFFICER: SCAMMERS CREATED AN AI HOLOGRAM OF ME TO SCAM UNSUSPECTING PROJECTS

What Happened?

- Binance Chief Communications Officer Patrick Hillman reports that he was thanked for taking a meeting he never attended
- He told the person thanking him that he never attended the meeting, and was informed that he had been impersonated – by AI
- Deepfakes are AI-generated photos, audio, and video which can be remarkably realistic, especially if there are many photos and videos around the web of a person
- Scammers created a “deepfake” of him from the audio and video captured in a Zoom video meeting



[redacted]

[redacted] • 9:52 PM

Hi Patrick this is [redacted], I had a conversation with Mark J Marshall, can you confirm the Zoom call we had on Thursday with you?

Patrick Hillmann • 9:52 PM

That wasn't me.

AUG 3

[redacted] • 4:58 AM

they impersonated your hologram

[redacted] • 5:58 AM

https://www.linkedin.com/in/j-m-b43103133

J M. - Stock broker/ICO advisor - Binance | LinkedIn
uk.linkedin.com • 1 min read
View J M.'s profile on LinkedIn, the world's largest prof...

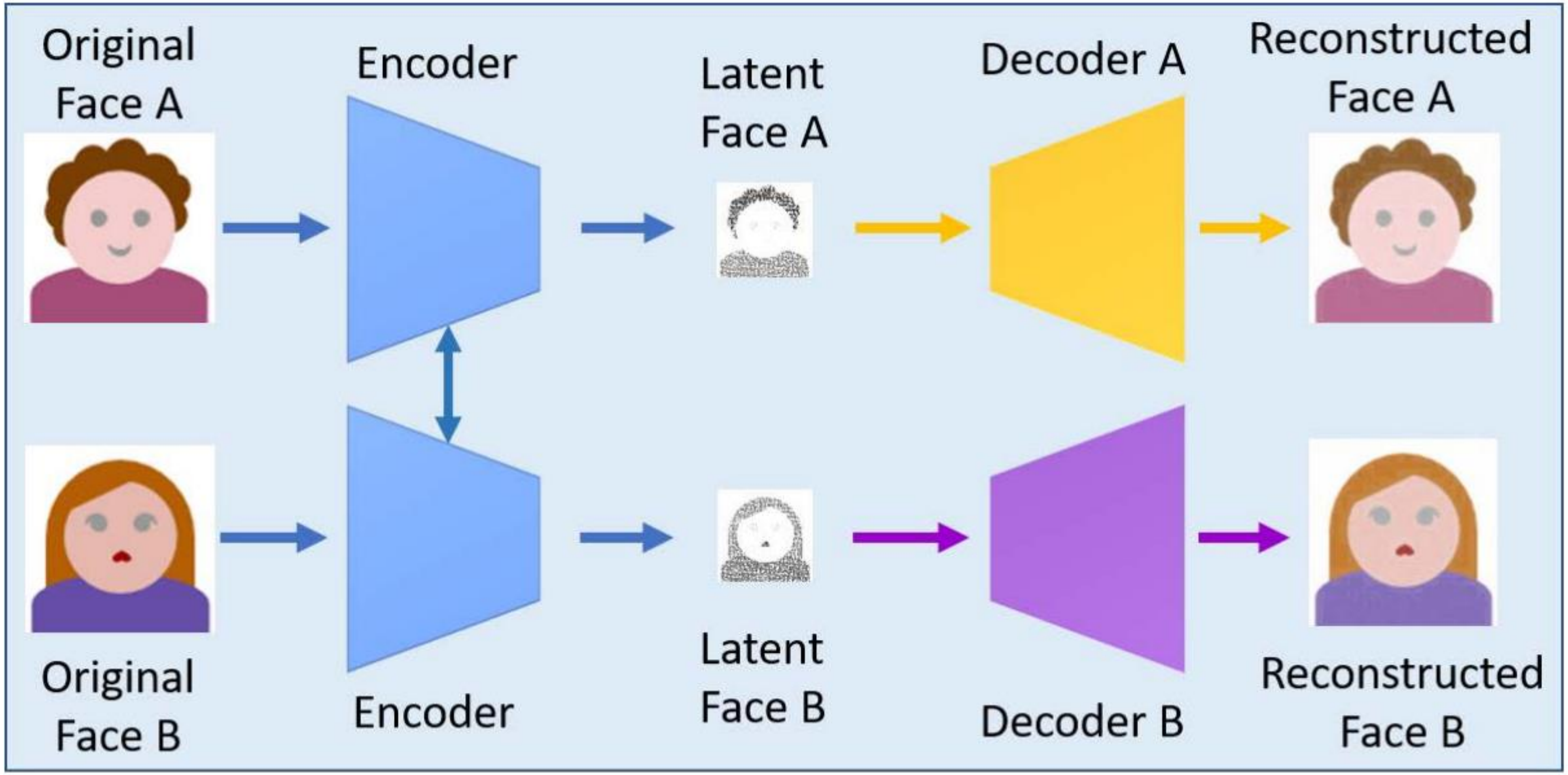
This person sent me a zoom link then your hologram was in the zoom , please report the scam

Source: Binance Blog (www.binance.com/blog)

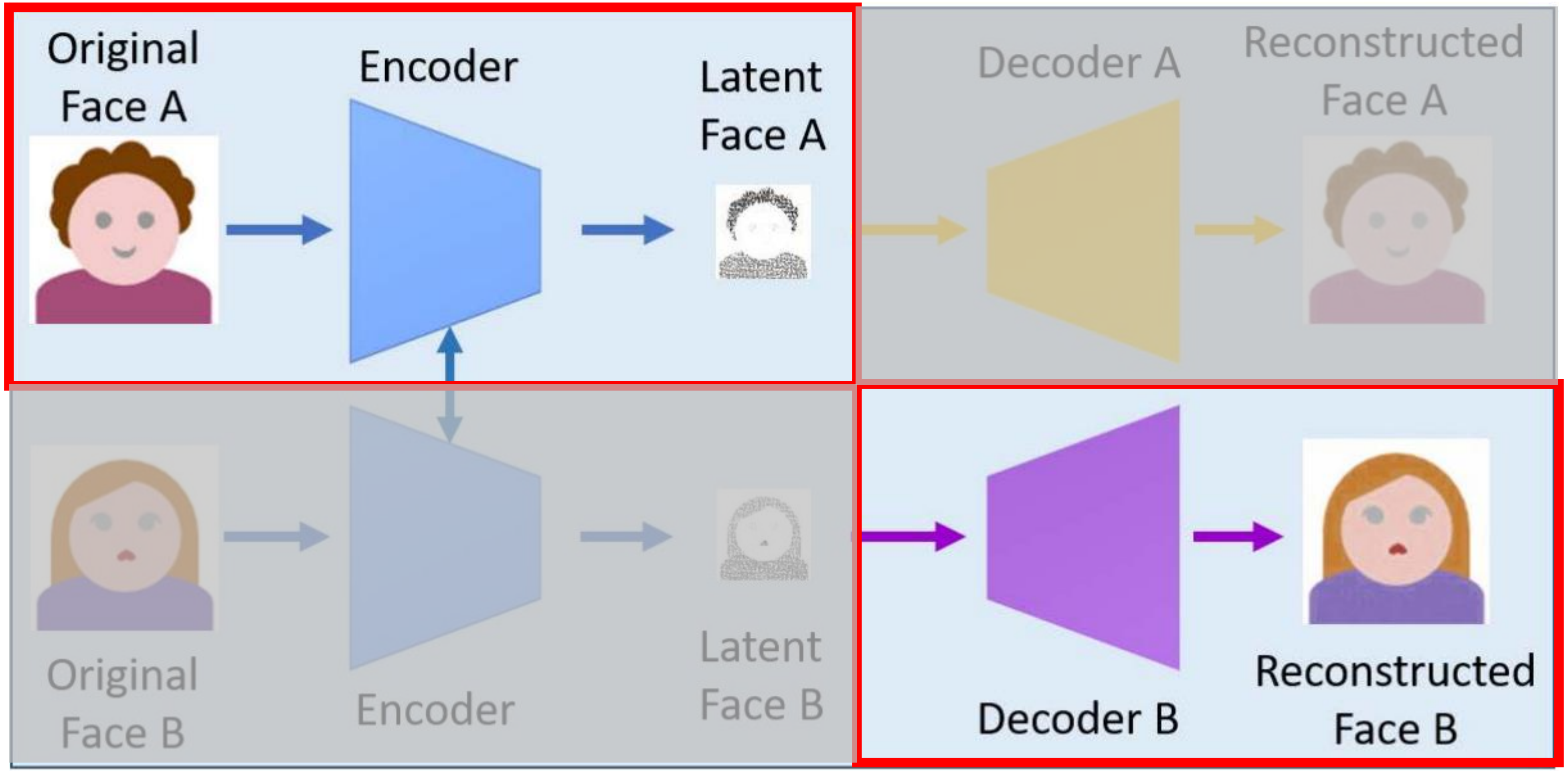
Another Deepfake Incident

- A CEO in the UK received a spear-phishing e-mail from someone posing as his parent company's CEO
- The request said that £243,000 ($302,000 USD, $407,000 CAD) must be wired in the next hour to a Hungarian supplier
- The e-mail was followed up with a phone call from the parent company's CEO, confirming the payment
- The victim said that he recognized "his boss' voice and slight German accent" as well as the "cadence and careful enunciation", so he happily made the payment to the scammers

How Deepfake Image Creation Works

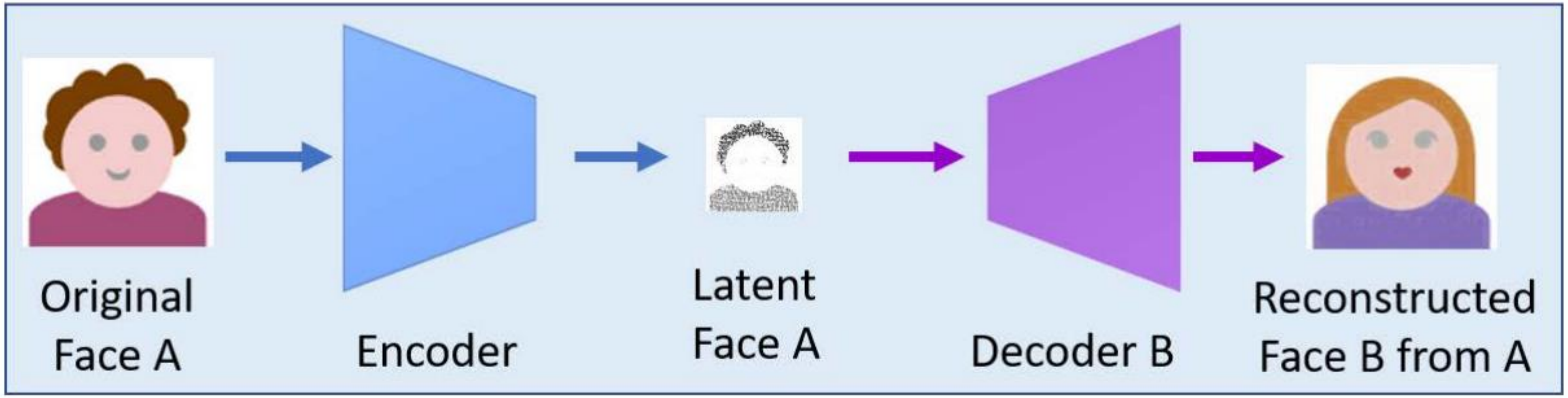


How Deepfake Image Creation Works



Source: Deep Learning for Deepfakes Creation and Detection: A Survey (arxiv.org)

How Deepfake Image Creation Works

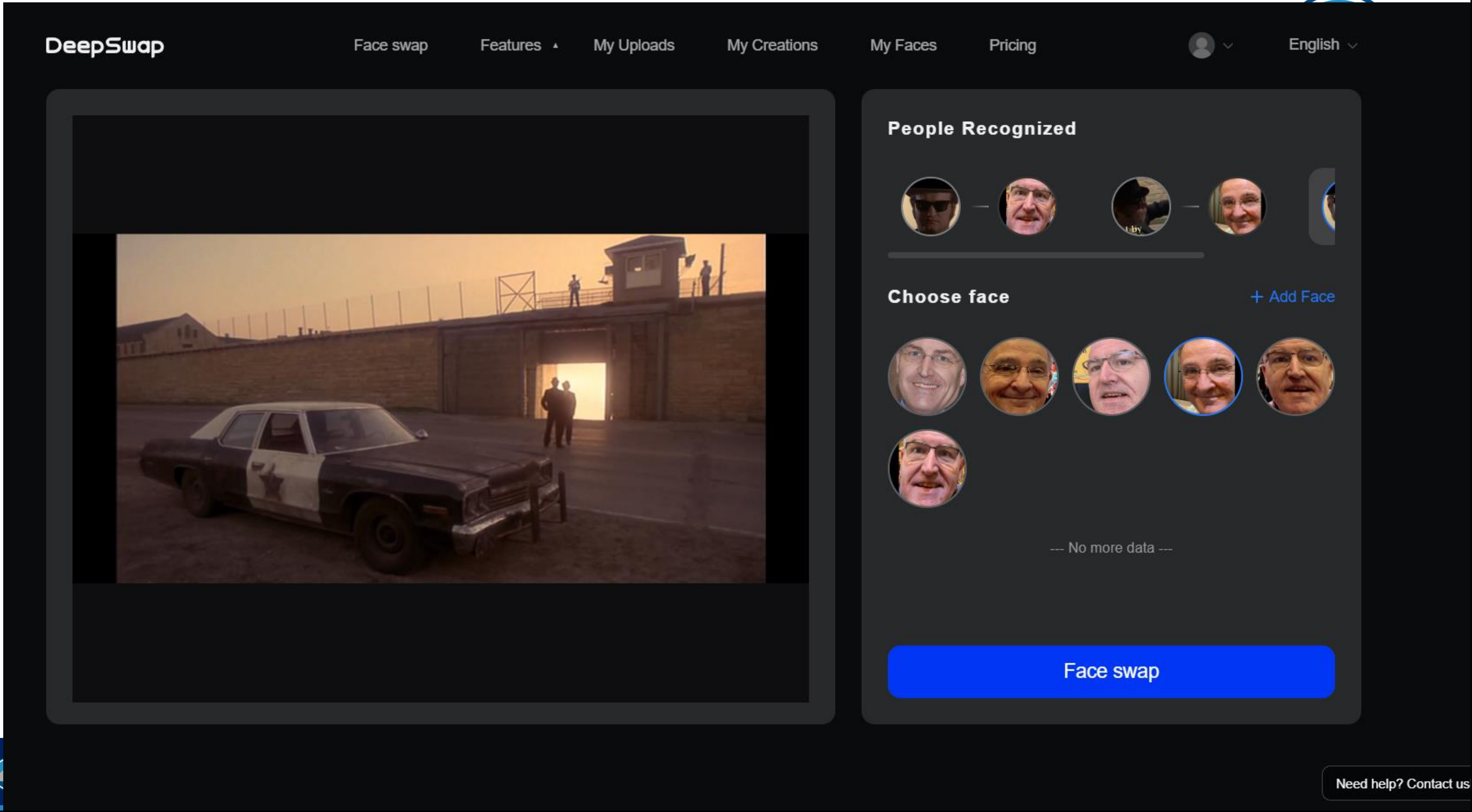


Soured: Deep Learning for Deepfakes Creation and Detection: A Survey (arxiv.org)

Creating A Deepfake: The Blues Brothers

- Created an account at DeepSwap.ai
- Uploaded photos of Brian Tankersley and Randy Johnston
- Cut the title sequence out of the Blues Brothers
- Selected faces to be replaced:
  - Jake's face (Belushi) with Brian's face
  - Elwood's face (Akroyd) with Randy's face
- What you see next is the process/result

Source: Deep Learning for Deepfakes Creation and Detection: A Survey (arxiv.org)


DeepSwap
Face swap
Features
My Uploads
My Creations
My Faces
Pricing
English
People Recognized
Choose face
+ Add Face
--- No more data ---
Face swap
Need help? Contact us

The Resulting Video

JOHN BELUSHI

DAN AYKROYD

The Resulting Video

Preventing Deepfake Scams

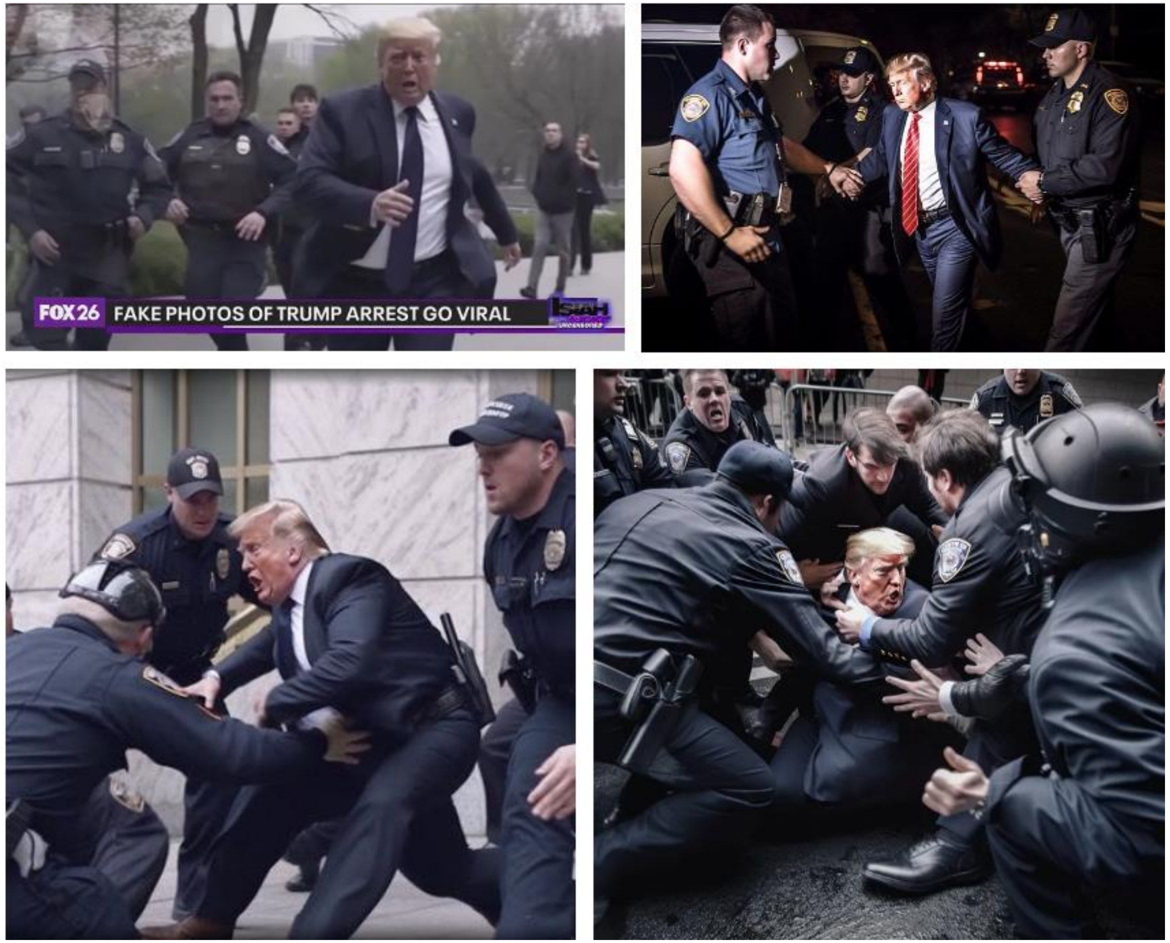
- No transfer of finances should be actioned solely on receipt of an email
- A follow-up phone call should be made from the recipient of the email to the sender, not from the sender to the recipient
- Challenge phrases can be incorporated that an outside attacker would not know
- Cross-reference and double-check everything that is out of the ordinary
- Urgent requests for immediate help should be questioned
- The authors of one paper suggest that future deep learning tools may help detect deepfakes, but they don't exist now

Source: HowToGeek, some items added

Deepfake Of Canadian PM Trudeau

- This is a piece of propaganda created by a group who opposes PM Trudeau, and is NOT REAL
- Learn more about this video at [The Post-Millennial]

Deepfake Of Former President Trump



- Immediately prior to the arrest of former US President Donald Trump in early 2023, the internet (and even some news outlets) were flooded with deepfake images of a fake attempt to escape custody
- Learn more about this propaganda at [Medium]

Observations On Deepfakes

- We have entered an era when seeing or hearing what you think is someone and trusting your eyes/ears is unwise
- Deepfakes are better than you think, and getting better daily
- If you are a public figure and a perpetrator has access to recorded video or audio of you, it is not difficult to train a new deepfake model to impersonate you
- The deepfake Blues Brothers video was created with only one picture of Brian and Randy – and the video of Trudeau and photos of Trump were more convincing

CYBERSCOOP

techradar.

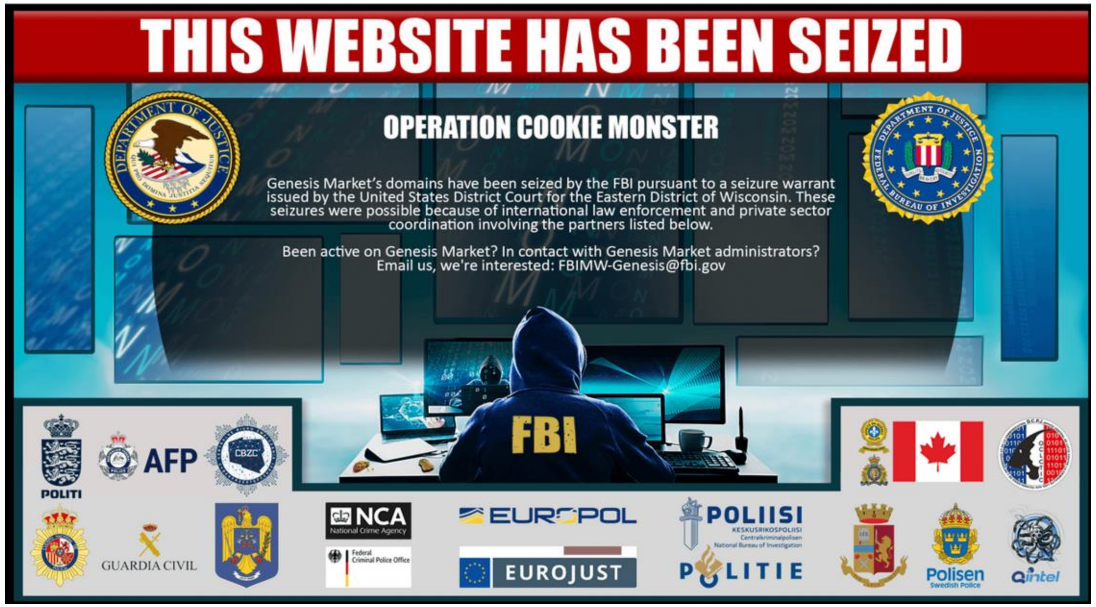
"Notorious Genesis Market cybercrime forum seized in international law enforcement operation" – Cyberscoop.com, 4/4/2023

"Browser fingerprinting: what it is and how to protect yourself" – Techradar.com, 6/14/2022

BROWSER FINGERPRINT IMPERSONATION

About Genesis Market

- Genesis was one of the top online criminal platforms globally before it was shut down on April 4, 2023
- There were versions of the Genesis Market site on both the public web and the "dark web"



THIS WEBSITE HAS BEEN SEIZED

OPERATION COOKIE MONSTER

Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.

Been active on Genesis Market? In contact with Genesis Market administrators? Email us, we're interested: FBIMW-Genesis@fbi.gov

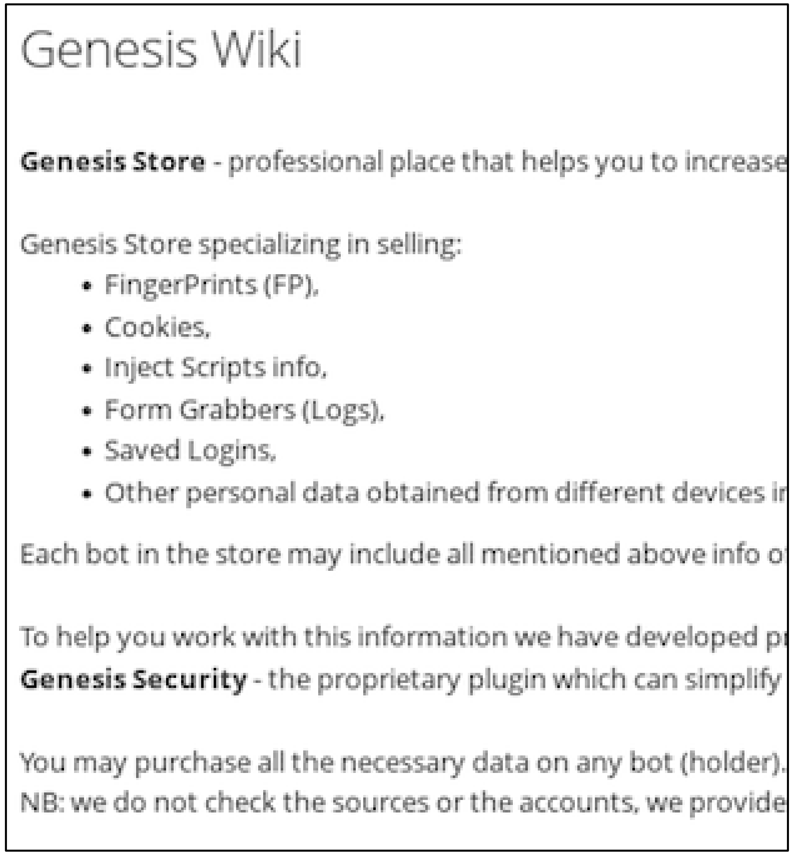
"Genesis … has been linked to millions of financial motivated cyber incidents globally, from frauds to ransomware attacks" – TheRecord.media

About Genesis Market

- Genesis sold confidential information like compromised credentials and biometric data like many other cybercrime websites
- Unlike its competitors, Genesis Market also offered criminals access to “bots” or “browser fingerprints” that allowed them to impersonate victims’ web browsers — including IP addresses, session cookies, operating system information, and plugins
- This “fingerprint” is used by many sites to determine whether or not you should have to use two-factor authentication (2FA) to confirm your identity – and are often used to bypass 2FA altogether

About Genesis Market

- The stolen fingerprints could be imported into a special “Genesis Security” browser plugin, which used the stolen details to impersonate the victim
- These fingerprints can be silently used to confirm the identity of a browser – and if spoofed by a criminal, they could take over your legitimate session with a site by impersonating the characteristics of your validated browser – and you would have no knowledge of the attack



Genesis Wiki

Genesis Store - professional place that helps you to increase

Genesis Store specializing in selling:

- FingerPrints (FP),
- Cookies,
- Inject Scripts info,
- Form Grabbers (Logs),
- Saved Logins,
- Other personal data obtained from different devices ir

Each bot in the store may include all mentioned above info o

To help you work with this information we have developed p
Genesis Security - the proprietary plugin which can simplify

You may purchase all the necessary data on any bot (holder).
NB: we do not check the sources or the accounts, we provide

Genesis Market’s Wiki explained the niche offerings from the now defunct website

(Source: TheRecord)

What Is Browser Fingerprinting?

- When you log into a website, that website usually sets a piece of data “cookie” in your browser and takes a snapshot of the identifying characteristics of the web browser you’re using
- That data is stored in a database on the web server for verifying identity
- When you return to that website, it may decide to make you authenticate again, prompting you for username/password/2FA
- BUT - if the browser fingerprint and cookies match EXACTLY, it may decide to just grant you access immediately

What Is Browser Fingerprinting?

Items commonly included in a browser fingerprint include things like:

- Operating system and exact version
- Browser and exact version
- Your time zone
- Your IP address
- Screen resolution
- Exact hardware details and versions of drivers used
- Font size
- Active background color
- The user ID used to log into Windows

…and many similar small details

How Do Sites Get All This Data?

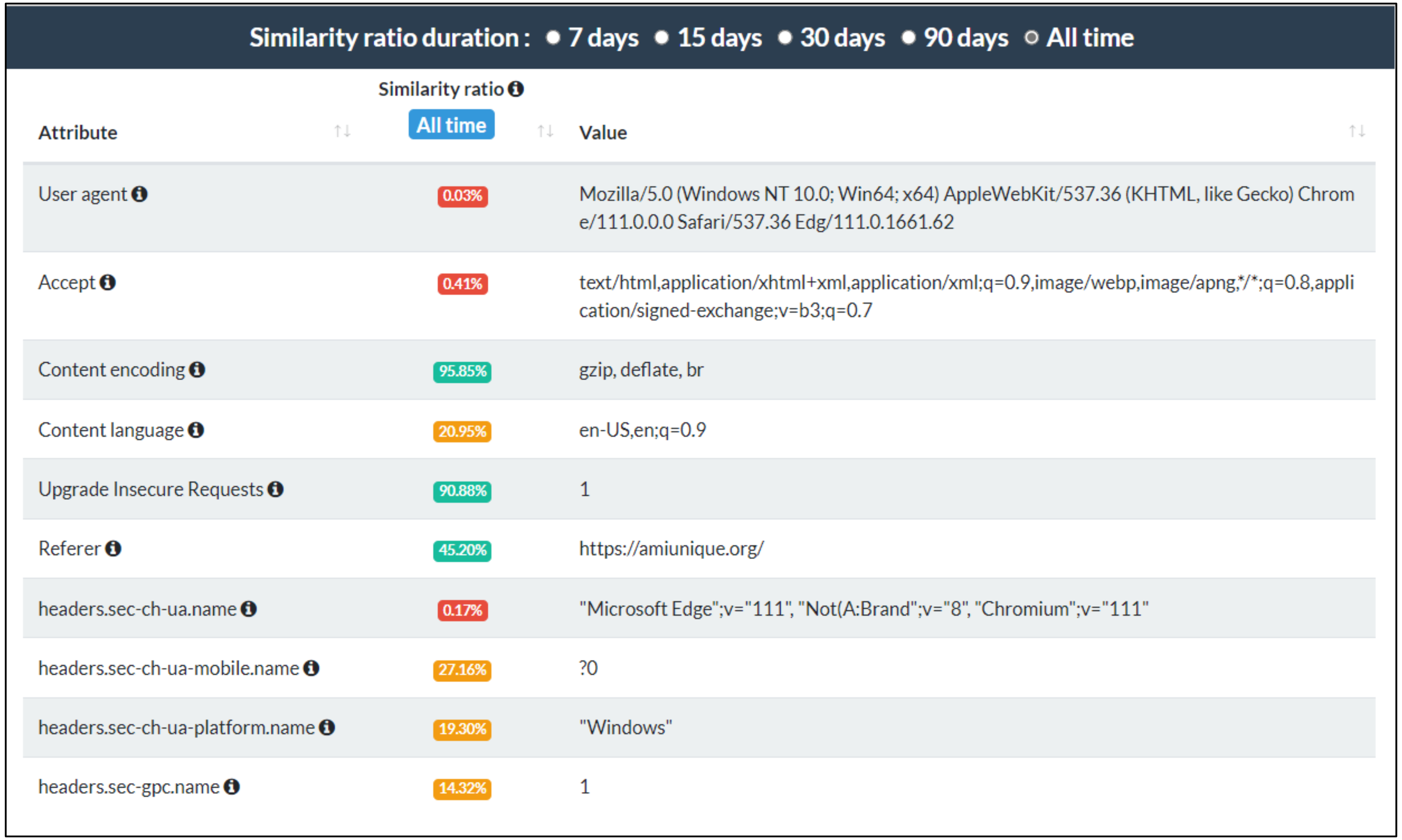
- Most sites use HTML5 to create their capabilities
- An element called "Canvas" can retrieve all kinds of information about your PC at the same time that it is rendering the content you requested – things like
  - Type of Browser (User Agent)
  - What kinds of headers you accept
  - Names of all browser plugins installed
  - Time zone
  - Names of all fonts on your PC

  …and much more

- *Want to see the details of your browser fingerprint? Go to coveryourtracks.eff.org, and click on "**Test Your Browser**"*
- *You can learn more about fingerprinting by visiting the Electronic Frontier Foundation*

What Does MY Fingerprint Show?

- Go to AmIUnique.org in your favorite browser
- Click on "**View My Browser Fingerprint**"
- The site will tell you what attributes are associated with your fingerprint and their relative frequency
- Each browser will create a different profile/signature



Similarity ratio duration : ● 7 days ● 15 days ● 30 days ● 90 days ○ All time

Attribute ↑↓	Similarity ratio 🛈 All time ↑↓	Value ↑↓
User agent 🛈	0.03%	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.1661.62
Accept 🛈	0.41%	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Content encoding 🛈	95.85%	gzip, deflate, br
Content language 🛈	20.95%	en-US,en;q=0.9
Upgrade Insecure Requests 🛈	90.88%	1
Referer 🛈	45.20%	https://amiunique.org/
headers.sec-ch-ua.name 🛈	0.17%	"Microsoft Edge";v="111", "Not(A:Brand";v="8", "Chromium";v="111"
headers.sec-ch-ua-mobile.name 🛈	27.16%	?0
headers.sec-ch-ua-platform.name 🛈	19.30%	"Windows"
headers.sec-gpc.name 🛈	14.32%	1

Observations On Browser Fingerprinting

- “Incognito” or “Private Browsing” mode may not protect you from being profiled/identified by websites
- You may want to protect yourself by using certain browsers and taking other actions to anonymize yourself
  - **Plugins**: AdBlock Plus, Privacy Badger, Disconnect, NoScript
  - **Browsers:** Firefox, TOR, Brave, AdsPower (Sun/Flower Browsers)
  - Other practices
    - Disabling Javascript and Flash
    - Changing browser settings from default
    - Turning on the “Do Not Track” setting
    - Using some antimalware apps can protect your browser fingerprint

DARKReading

SPOTLIGHT REPORT 2023

RANSOMWARE

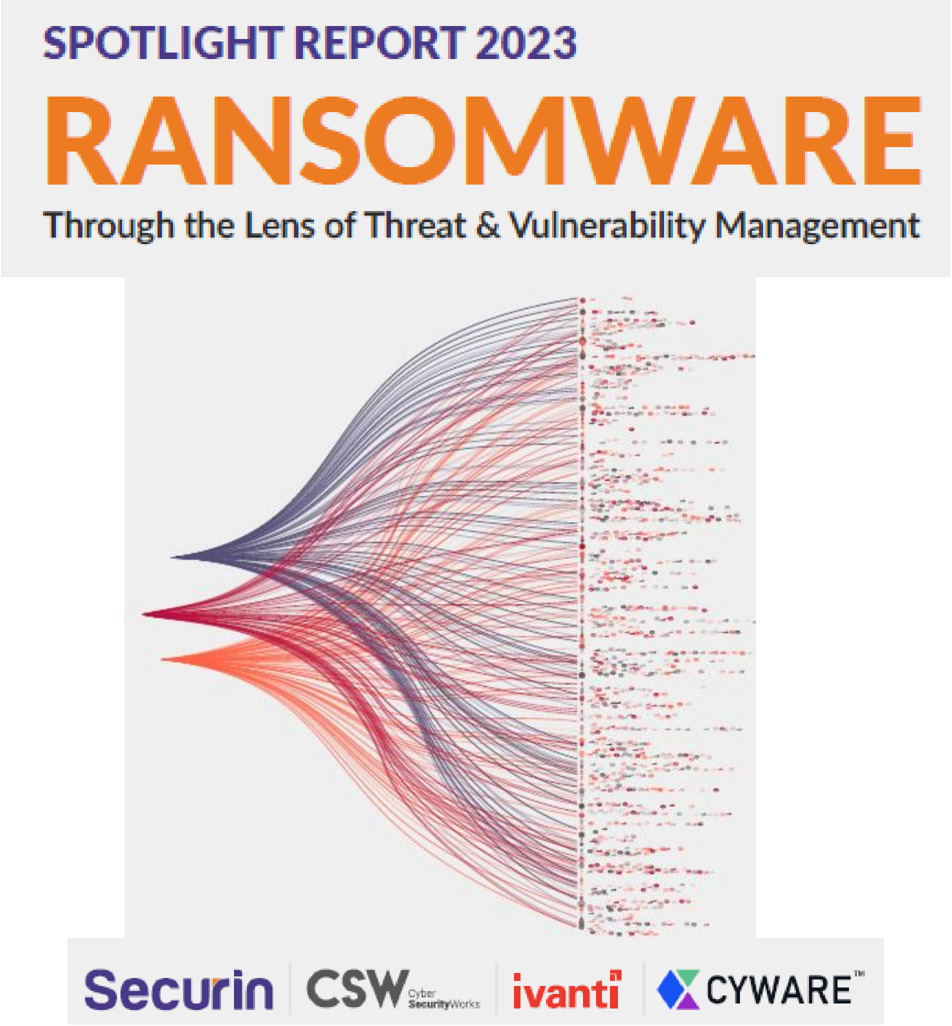
Through the Lens of Threat & Vulnerability Management

“Majority of Ransomware Attacks Last Year Exploited Old Bugs”, Dark Reading 3/29/2023

RANSOMWARE ATTACKS MANY OLD BUGS!

Avoiding Ransomware

- To avoid having systems infected with ransomware, it is essential to keep systems patched with the latest updates from the publisher or hardware manufacturer
- The authors of this survey identified that **76% of the ransomware-associated security vulnerabilities were discovered between 2010 and 2019** – so if you haven’t updated your computers and servers, it’s just a matter of time before you are affected by ransomware



SPOTLIGHT REPORT 2023

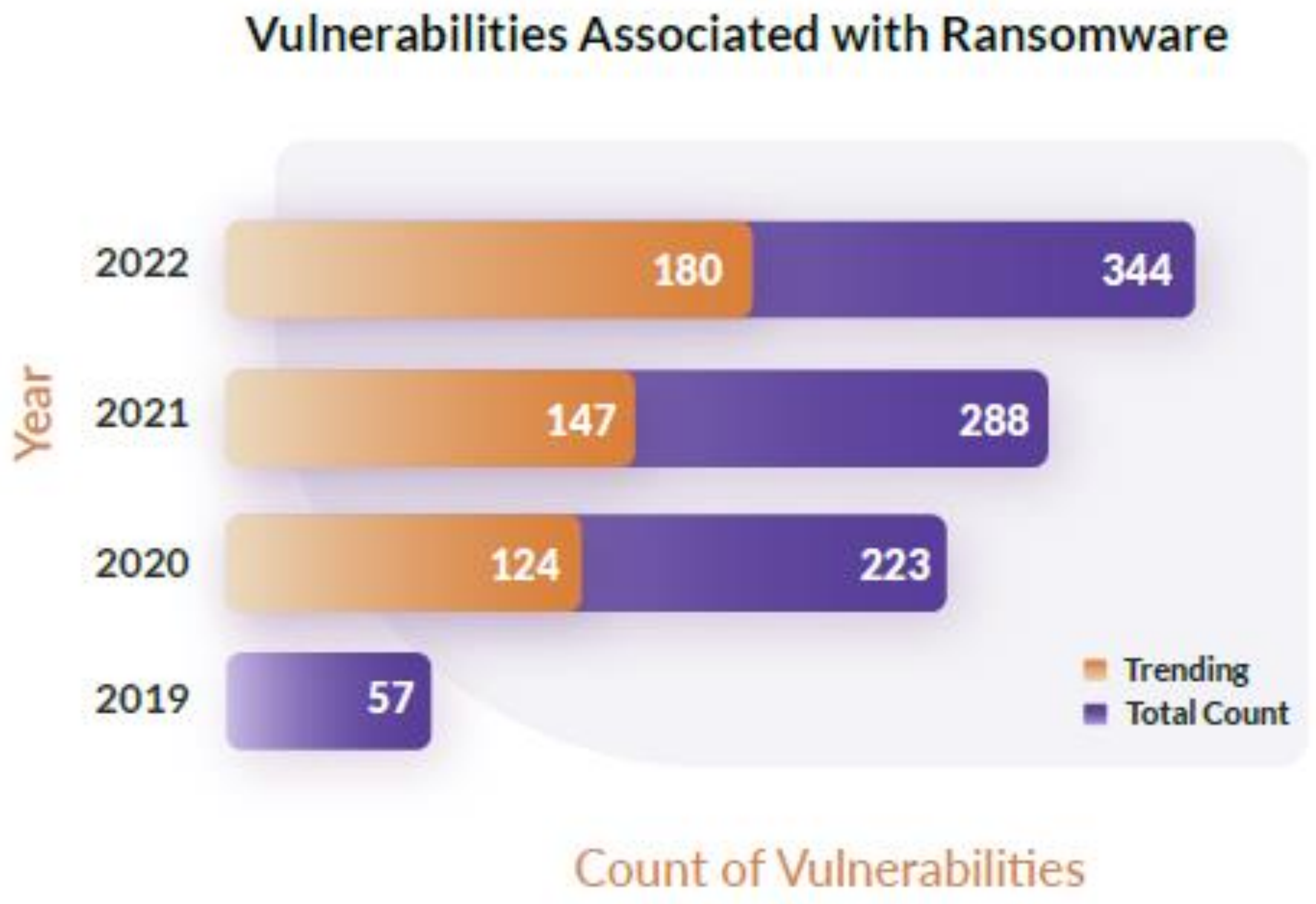
RANSOMWARE

Through the Lens of Threat & Vulnerability Management

Securin | CSW Cyber SecurityWorks | ivanti | CYWARE™

Avoiding Ransomware

- The survey's authors pooled their data on ransomware variants and the vulnerabilities which allow them to function, and noted that there are 56 more vulnerabilities associated with ransomware in 2022 as compared to 2021
- There are also 33 more vulnerabilities which are "trending" or are vulnerabilities under active exploitation by cybercriminals



Avoiding Ransomware

- Other observations include:
  - 16% of the vulnerabilities exploited by ransomware are considered low or medium risk by the security community
  - 118 of the vulnerabilities associated with ransomware strains are present in multiple products
  - Most problematic are the ongoing issues with Apache Log4J, a library used by many other applications
    - CVE-2021-45046 present in 93 products from 16 vendors
    - CVE-2021-45105 present in 128 products from 11 vendors
    - Both are exploited by the AvosLocker Ransomware

Avoiding Ransomware

- Other observations include:
  - 131 vulnerabilities associated with ransomware are excluded from the US CISA’s database of “Known Exploited Vulnerabilities” (KEVs), meaning that government systems are not required to patch for them
  - 20 vulnerabilities associated with ransomware are not detected by major enterprise scanners like Nessus, Nexpose, and Qualys, including two in the last quarter before the report was issued
    - CVE-2021-33558 (Boa)
    - CVE-2022-36537 (Zkoss)

Observations

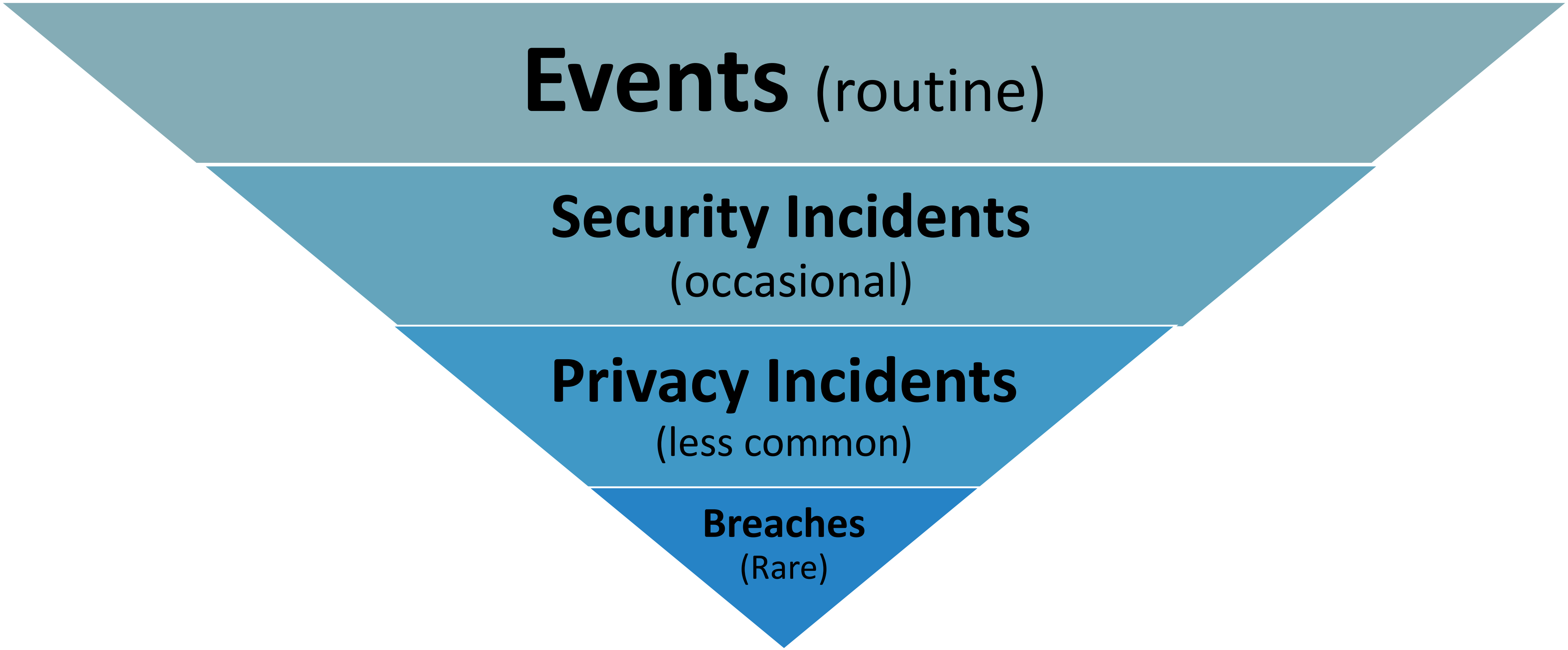
- While patching is not a panacea for ransomware, not patching makes it very likely that, if exposed, you would be infected
- Some vulnerabilities are hard to patch and will take years to make their way through the software supply chain – so look for ways to reduce your exposure to those problems
- The bad guys are getting better at an alarmingly fast rate – so remain vigilant and keep learning – because it's not getting easier anytime soon

INCIDENT RESPONSE

Incident Response Planning

- Understanding the incident response, compliance, legal and law enforcement aspects of responding to a breach before it happens is stressed by all experts
- Having documented procedures in place helps you make better decisions under duress. Not being prepared may cause mistakes when an event happens.
- The Poneman Institute's research indicates that the single best way to reduce the capital cost of a data breach is to have an incident response team and related strategy

Events, Incidents, And Breaches In Perspective



Events (routine)

Security Incidents
(occasional)

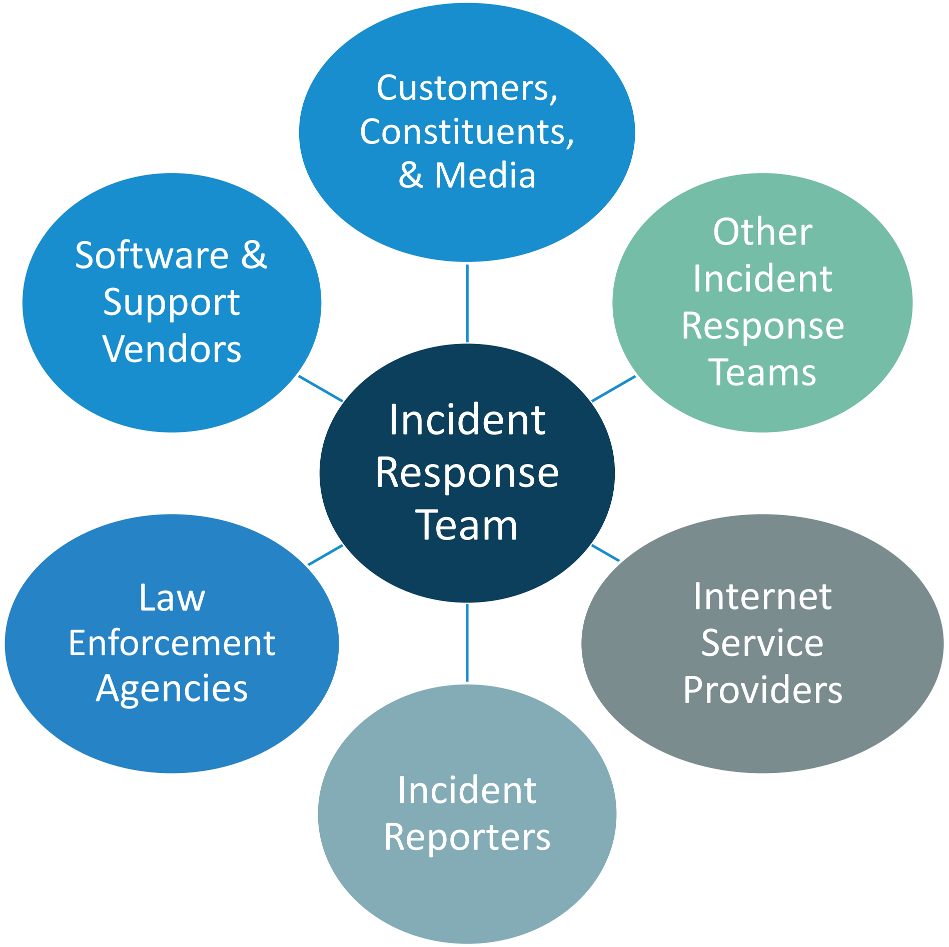
Privacy Incidents
(less common)

Breaches
(Rare)

Create Incident Response (IR) Team

- Incident Response Team brings together management, information security, physical security, IT, legal, HR, public relations, and financial audit personnel
- The IR Team's job is to detect, identify, contain, eradicate, and recover from information security incidents that arise
- Developing an IR plan before an incident is key to successful resolution
  - The steps to take when an incident is discovered (what to do)
  - The process used to implement the steps (how to do it)

Communication With Outside Parties


Customers, Constituents, & Media
Other Incident Response Teams
Internet Service Providers
Incident Reporters
Law Enforcement Agencies
Software & Support Vendors
Incident Response Team

- You will likely need to interact with outside parties regarding an incident
- Your Incident Response Team (IRT) should discuss information sharing with your media relations team, legal counsel, and management before an incident occurs to create policies and procedures on information sharing before they are needed

Incident Response Overview

- Assess the incident before taking action
- Be familiar with the law or retain an attorney
- Execute your prepared IR action plan
- Contact law enforcement
- Reassess and take the long view

"48 Hours," *InfoSecurity Professional*, July/August 2015

Assess The Incident Before Acting

- Incident may not be an isolated event but rather part of a larger intrusion
- Locking down the network may not always be the best response
- Capturing the experience of those involved with the incident is critical
- Make sure to work closely with your legal counsel and document any work product items properly

Be Familiar With The Law

- Distinguish an _*incident*_ from a _*data breach*_
- Rarely when you discover something do you have enough evidence to conclude that you have a legal breach
- Before evidence of a legal breach, the event is merely an incident
  - Stop the damage
  - Investigate what happened
  - Confidentiality is paramount

Benjamin Wright, Attorney and SANS Institute instructor

Execute Your IR Action Plan

- Preparation is key to minimizing the impact of a breach
- Make sure to verify that the controls that were implemented are working as expected
- Vulnerability scans and penetration tests help organizations expose the vulnerabilities that could allow criminals to steal information

Troy Leach, CTO of the PCI Security Standards Council

Contact Law Enforcement

- Your IR action plan should include the contact details of all appropriate law enforcement officials responsible for security breaches
  - Identify the appropriate law enforcement agency for your industry and geographic area
  - You can't just dial 911
- In some cases, you will call the FBI, but your local or state police may have the relevant expertise
- Other industries fall under Secret Service or Homeland Security

William C. Snyder, former federal prosecutor and
assistant professor, Syracuse College of Law

FBI Involvement

- Three scenarios that may require FBI involvement
  - When proprietary information or data is on a hosted server and the organization doesn't have the means to take it back
  - When an imminent and ongoing threat such as DDOS is so onerous that it's impeding the operations of the company
  - When your IT department has identified an insider threat
- Once you contact the appropriate local authorities, identify one or two key people in your organization who will be the primary contacts for law enforcement personnel

Joseph R. Bonavolonta, assistant special agent in charge, Boston Division of the FBI, overseeing the Cyber, Counterintelligence and Security Branch

Who Will Be Involved?

- FBI personnel
  - A cyber-trained case agent
  - A computer scientist
  - A forensic examiner
  - An intelligence analyst
- From your IT department, the FBI will expect to receive
  - Specific dates and times of the incident
  - IP origination, log files, domains, etc.
  - Specific intellectual property that was compromised

Incident Response Traps And Pitfalls

- Avoid a DIY response, especially if you don't have an IR Team or a prepared IR action plan
- Fix the problems you identify
- Don't let intruders know what you know
- Notify executive management in a timely manner
- Be aware of the sensitivity of data breaches
- Don't announce the breach publicly before a thorough evaluation is complete

Thank You For Attending

QUESTIONS?