How to Recognize and Stop Financial Fraudsters

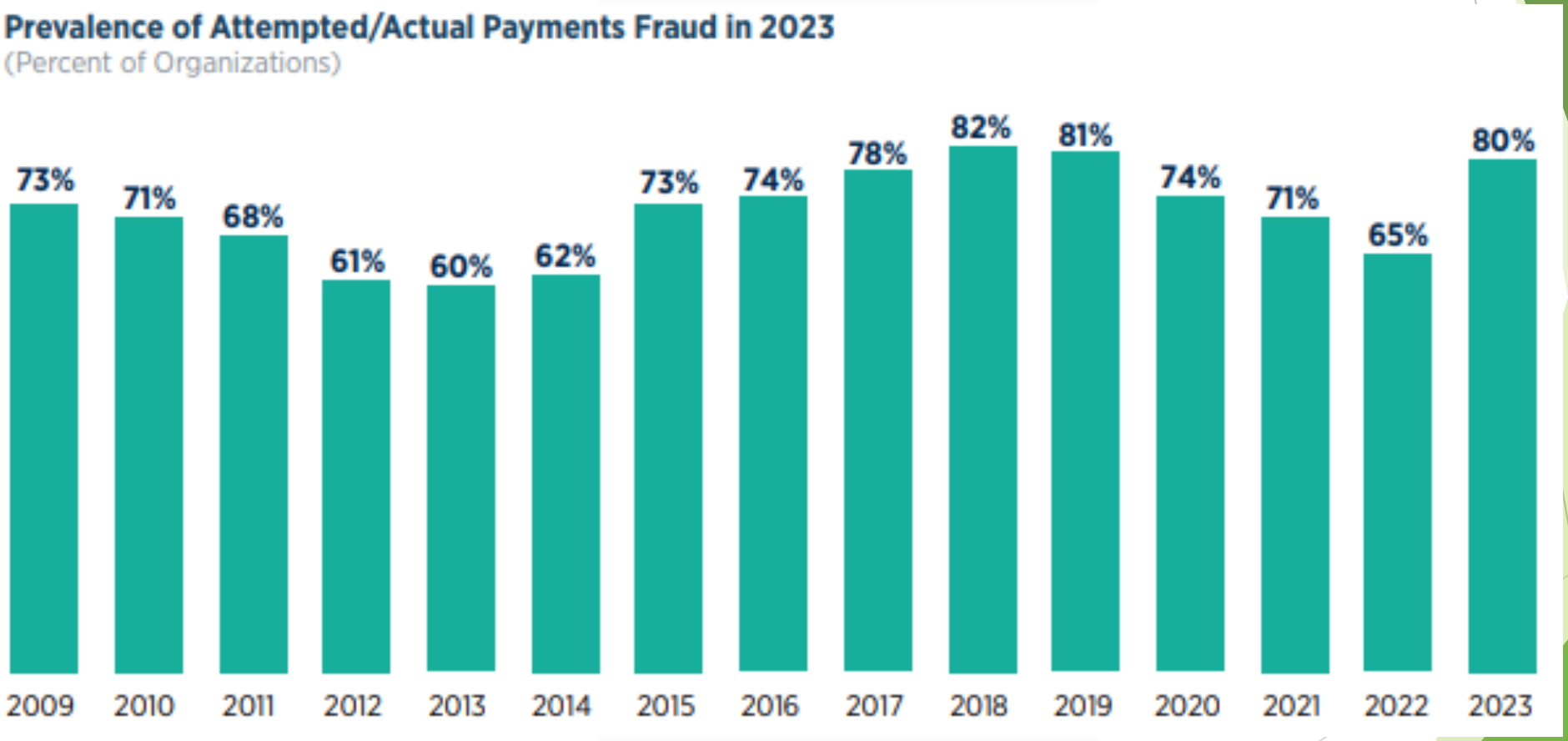
Presenters

- John Callahan
  - Senior Vice President
  - M&T Bank - Government Banking

- Jesse Adams
  - Cyber Security
  - Center for Internet Security

Agenda

- Trends in Fraud
- Recognizing Financial Crimes
- Practical Strategies to Prevent and Protect
- Steps if you are attacked by fraud
- Know Your Partners
- Question and Answer Discussion



Source: 2023 AFP Payments Fraud and Control Report | www.AFPonline.org

Payment Methods Subject to Attempted/Actual Payments Fraud

Account and Employee/Volunteer Fraud

Source: 2023 AFP Payments Fraud and Control Report | www.AFPonline.org

What is the percentage of data breach incidents caused by employee Mistakes?

95%

Payment Methods Subject to Attempted/Actual Payments Fraud

68% of companies experienced business email compromise –

Business email compromise (BEC):

- A type of phishing scam where attacker impersonates or compromises an executive's email account to manipulate the target into initiating a wire transfer or to giving away sensitive information.

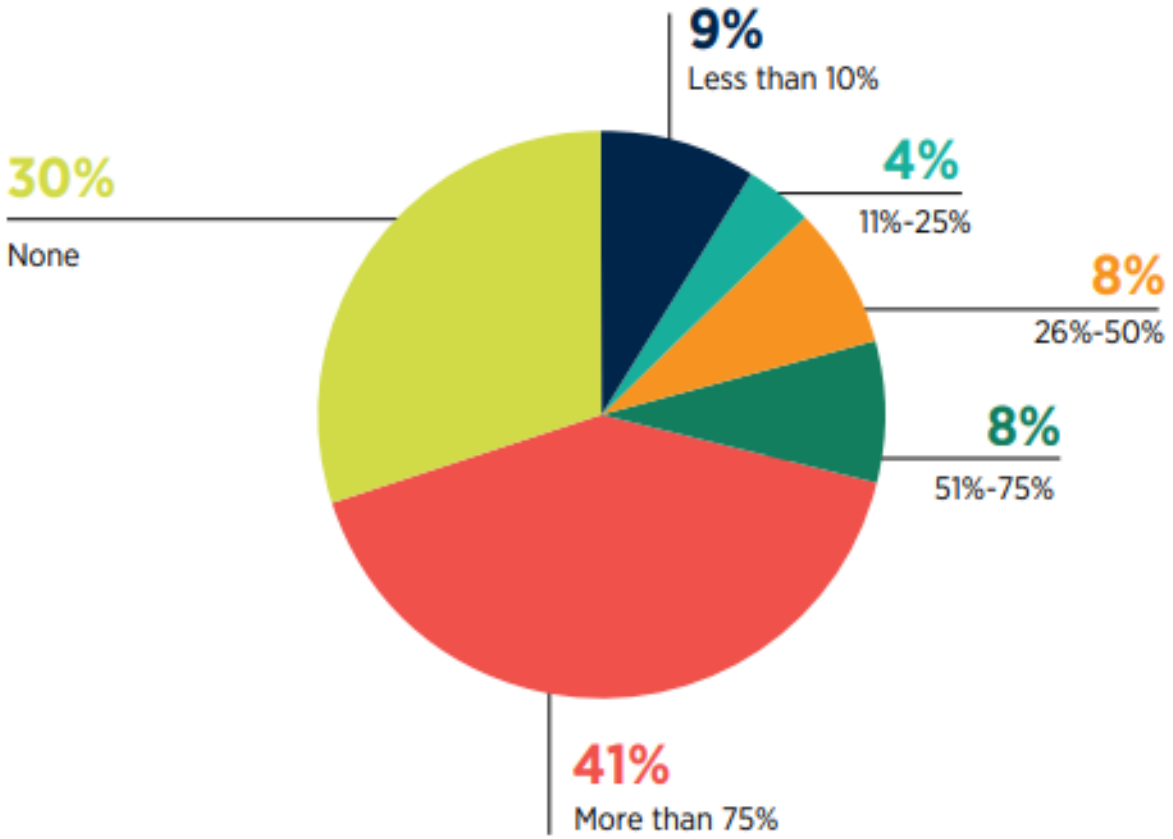
FBI: Biggest cause of cybercrime financial losses for U.S. organizations

High ROI of social engineering attacks, compared to time and cost of deploying sophisticated malware

Source: 2023 AFP Payments Fraud and Control Report | www.AFPonline.org

Recovering Lost Funds:

Percentage of Lost Funds Recovered
(Percentage Distribution of Organizations Experiencing Payments Fraud)



Source: 2022 AFP Payments Fraud and Control Report | www.AFPonline.org

Recognizing Financial Crimes

See if you can catch these agents of KAOS (Chaos)

Suspect #1 Email Impersonation -

This is how it plays out: You receive an email that appears genuine, seemingly originating from a credible source...

What it looks like: Change Signers

From: Joseph Porchetta (company email)
Sent: Thursday, April 18, 2024 12:17 PM
To: Bank
Subject: Addition of new signer

Hi Joe,

I would like to add our chief operating officer (Alan Myers) to all our accounts as an admin to our Treasury Cash Management – online banking services.

In addition to that, I would also like to add Alan as a signer on our accounts.

Alan should have complete access to all accounts, set up, approve and release domestic and international wires.

Alan will be the new Admin to our Treasury cash management online banking services.

Can you please forward the necessary forms needed to sign? Or have someone email me to assist with this request.

I would appreciate if this is done at your end as soon as possible.

Thanks,

- Email impersonation does not just happen to customers- the fraudsters are trying to get through your bank! Your financial institution has dual authorization and layers of approval that should defend you.
- In this case You will be contacted via the phone for signer changes as well as via your online system. (* the bank may call you??? ….. Politely hang up and call them back at the number you have on your phone or call a branch)

Suspect #2 Email Impersonation

Here's how it unfolds: the fraudster contacts your financial institution and attempts to gain access

What it looks like: Payroll Diversion & Supplier impersonation

From: supretendert@gmail.com
Sent: Thursday, April 18, 2024 12:17 PM
To: employer
Subject: Direct Deposit Updates Info

Jodie, I need to update my pay check direct deposit information for my next payroll. Please can you update this asap?

DIRECT DEPOSIT INFO

- Employ detailed payroll procedures that require employee or Vendor verification and approved by a secondary personal other than one processing the change.
- Call the employee or vendor – you should have their number. Do not rely on email as it could contain fraudulent contact information.
- Utilize Vendor Match Service – verify account # / Name

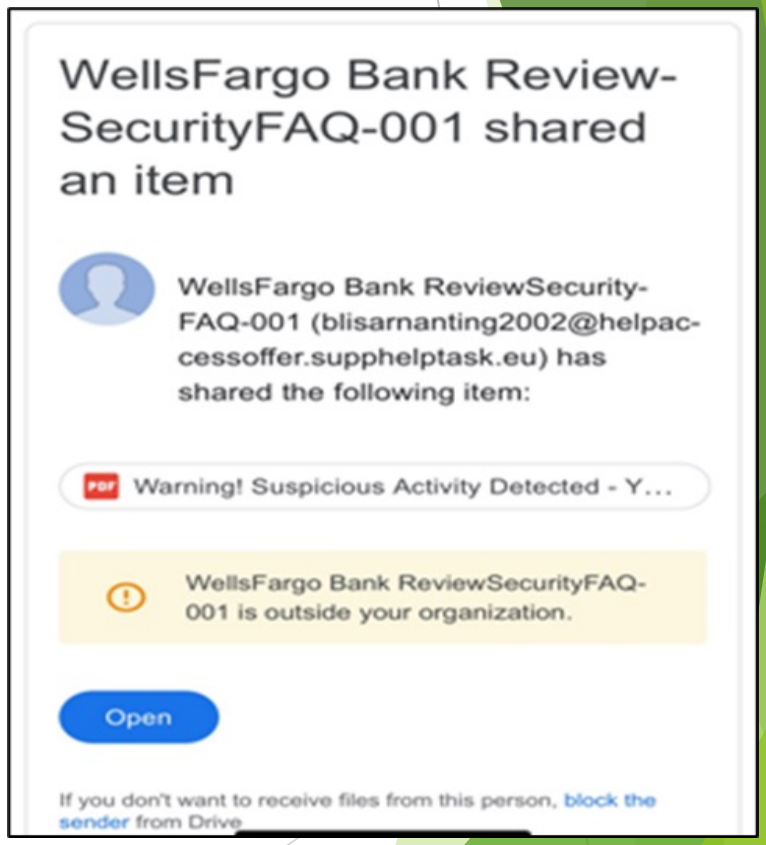
Suspect #3 Phishing-

This is how it plays out: You receive an email ; text or even a phone call that urges you to take action…..

Phishing

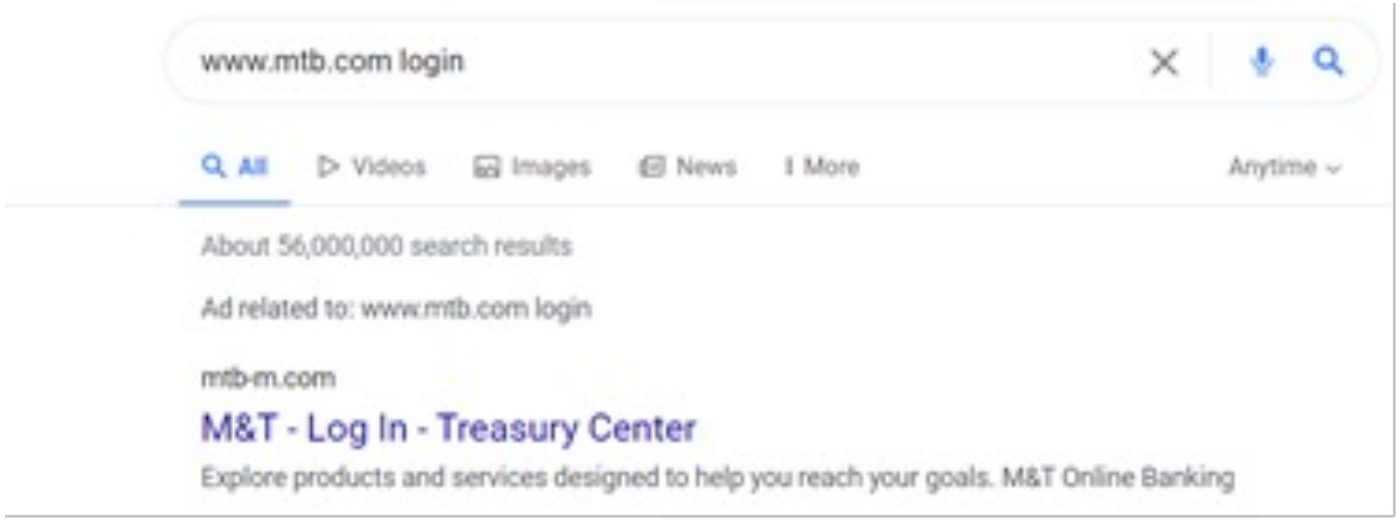
Exploiting the End User

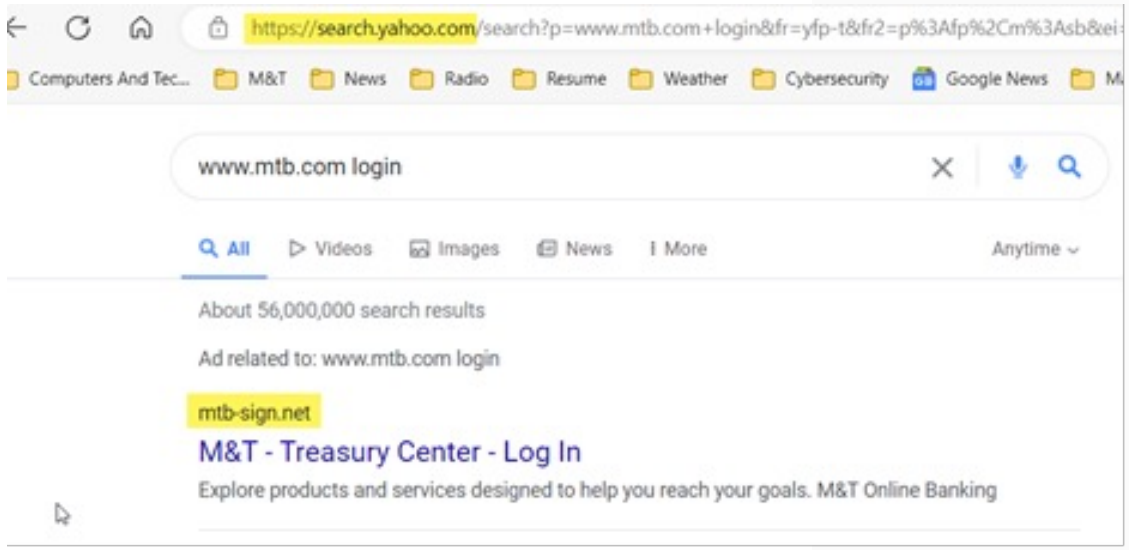
- Phishing: Cyber threat actors (CTAs) masquerade as legitimate entities to trick users into opening attachments, clicking links, or providing sensitive information.
- Often meant to provoke sense of urgency
- Phishing themes and lures include ongoing crises (e.g. hurricanes, COVID-19, etc..) or seasonal events (e.g. Tax Season)
- Types:
  - Spear Phishing
  - Business email compromise (BEC)
  - Threat High-jacking
  - Callback phishing



Phishing

Malicious Links to Bank Websites



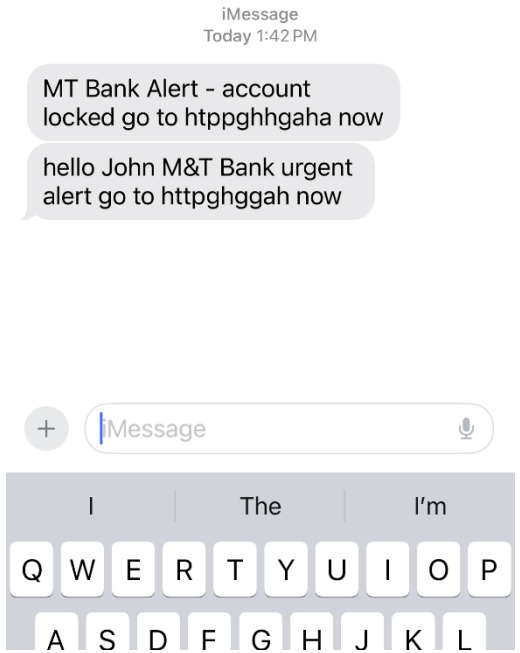


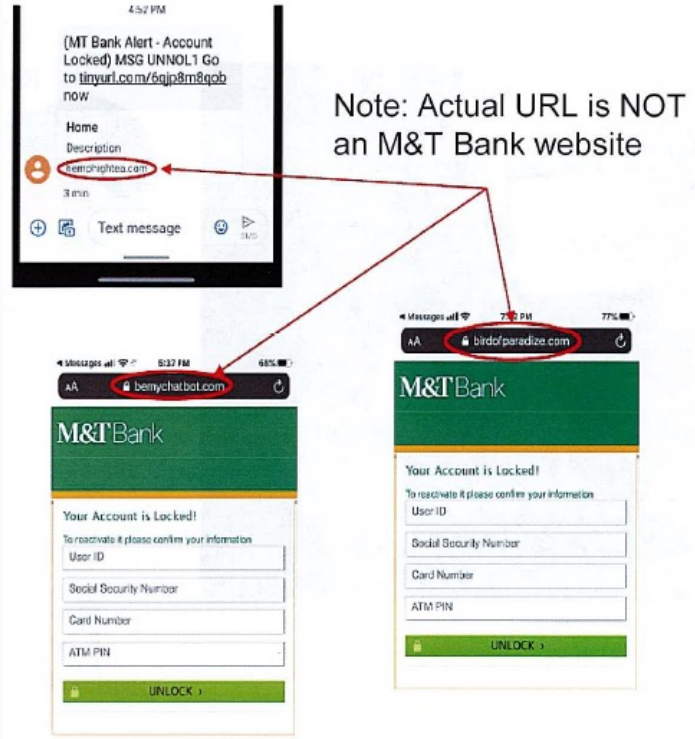
Suspect #4
Smishing

Here's how it unfolds: You receive a text from MT BANK…..

What it looks like: Smishing Schemes

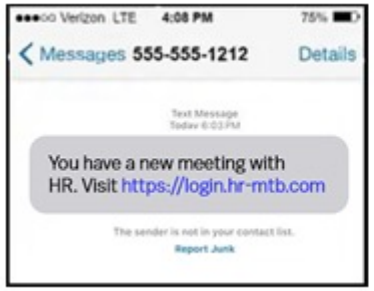
Note: “MT Bank” not “M&T Bank”





- Fraudsters continue to call, text and email from 1-800 bank numbers and emails
- Customers reveal account numbers – passcodes and PING ID numbers
- Always Call your bank at the number on their website; never share PING ID; passcodes or account numbers with someone who contacted you!

What it looks like: Smishing Schemes



Payment Methods Utilized in Business Email Compromise

(Percent of Organizations Experiencing Payments Fraud)

	2023	ANNUAL REVENUE LESS THAN $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION AND FEWER THAN 26 PAYMENT ACCOUNTS	ANNUAL REVENUE AT LEAST $1 BILLION AND MORE THAN 100 PAYMENT ACCOUNTS	2022
ACH credits	47%	57%	43%	50%	20%	34%
Wire transfers	39%	29%	43%	30%	80%	45%
ACH debits	20%	14%	23%	23%	27%	26%
Checks	18%	14%	19%	13%	20%	16%
Corporate/commercial credit cards (e.g., purchasing, T&E, fleet)	7%	5%	8%	3%	13%	8%
Gift cards	4%	--	6%	3%	7%	4%
Virtual cards	3%	--	4%	3%	7%	4%
Third-party pay-outs, e.g., Venmo, PayPal, Zelle etc.	3%	5%	2%	--	7%	5%
Real-time Payments (RTP, FedNow)	1%	5%	--	--	--	*

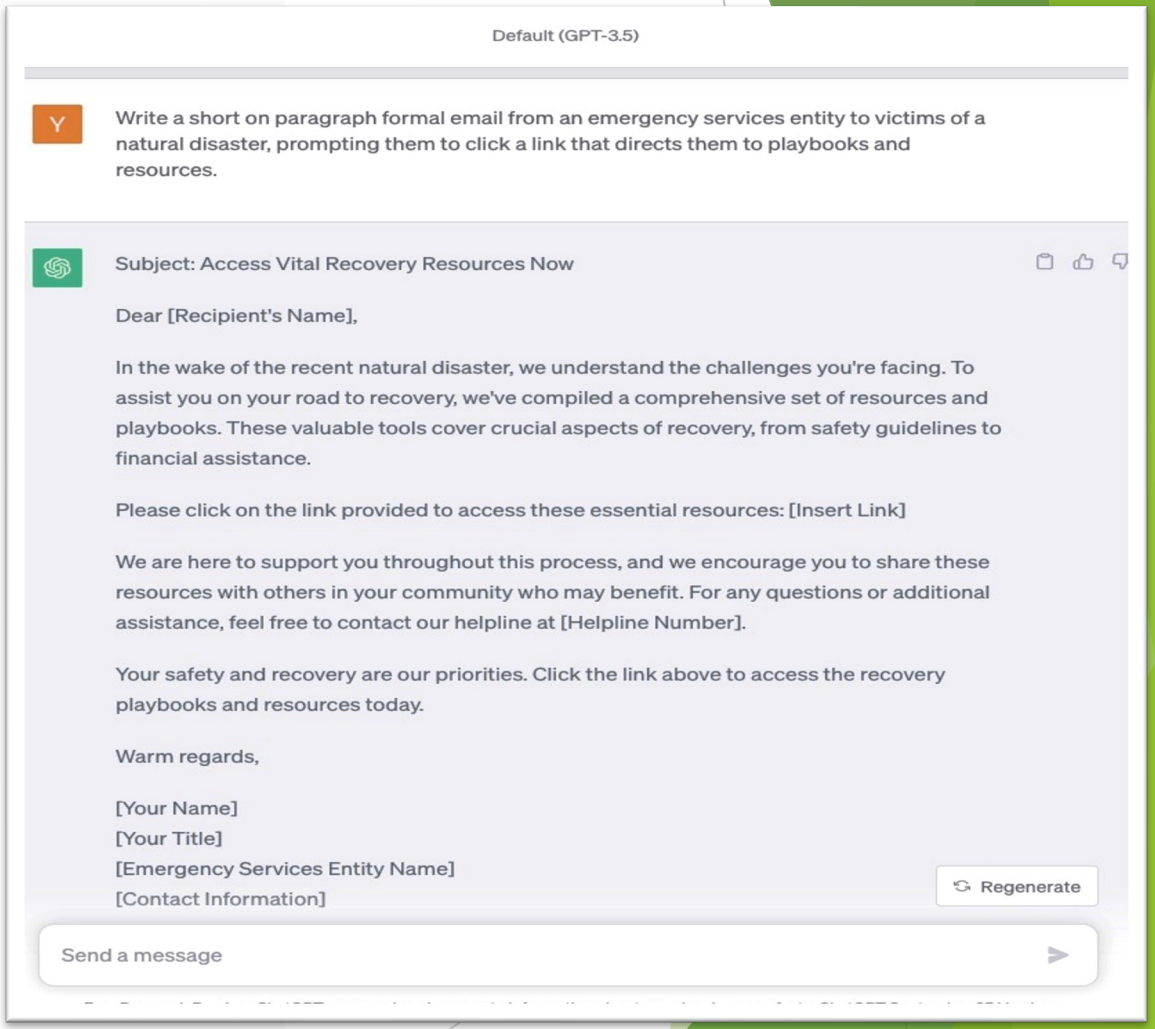
**not asked in 2022*


AI and Fraudsters - Agents of Kaos (Chaos)

Generative AI and Phishing

ChatGPT Used to Create Convincing Phishing Emails

- **Platforms can generate professional-sounding content**
  - Output represents a starting point for the user or threat actor
- **Cyber Threat Actors (CTAs) can leverage this**
  - Not as simple as “write a phishing email”
  - Changing prompts results in content
  - More details in the prompt = better content generation



Generative AI Meets The Internet

- Generative AI content going viral
  - Can spread quickly before people realize it isn't real

Generative AI-created video of the Eiffel Tower on fire
4.6 million views

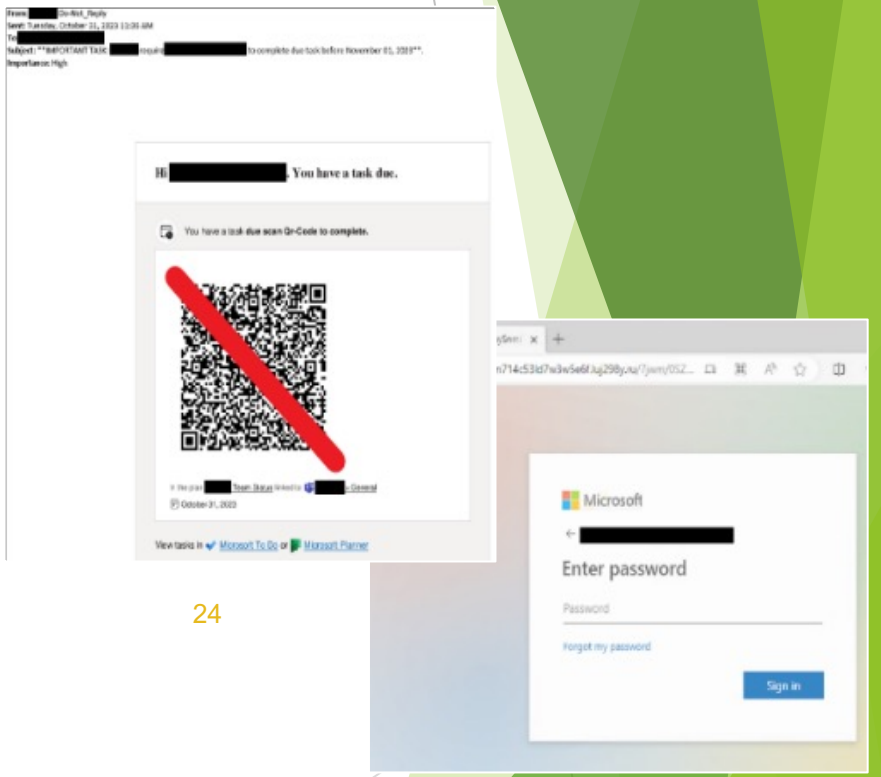
Generative AI-created image of an explosion at the Pentagon
Stock market dipped

Suspect #5 QR Code Phishing (Quishing)

Here's how it unfolds: You are prompted to use one of these

QR Code Phishing – new type: Quishing

- Quishing email has a sense of urgency
  - Victims are directed to complete a task
- Mobile scanning bypasses email phishing protections and email security tools
- Once scanned, victim is directed to a CTA phishing site
  - Used for credential harvesting



Source: CTI

The Big Boss: Data breach / data intrusion- Ransomware

Here's how it unfolds: You receive a text from your financial institution; a browser update; text; email….

Thread Hijacking

From: John Smith <wefoiunfcon2.23r2@spamemail[.]org>
Sent: Wednesday, January 4, 2023 1:09 AM
To: youremail@yourcompany[.]org
Subject: RE: Meeting tomorrow

Hello,
The signed document was uploaded here:
https://maliciouslink[.]org

From: John Smith <john.smith@yourcompany[.]org>
Sent: Wednesday June 7, 2022 3:09 PM
To: youremail@yourcompany[.]org
Subject: Meeting tomorrow
Hey Mike,

I'm sending the conference call information below. Pam will be joining us on the call and wants to go over what Stanley proposed during our meeting earlier this morning. Could you please send over any notes you took?

Thanks
-John

Name does not match email address. Email address does not match the original in the thread.

Email is responding to correspondence from several months ago. Does John usually email you at 1:00am?

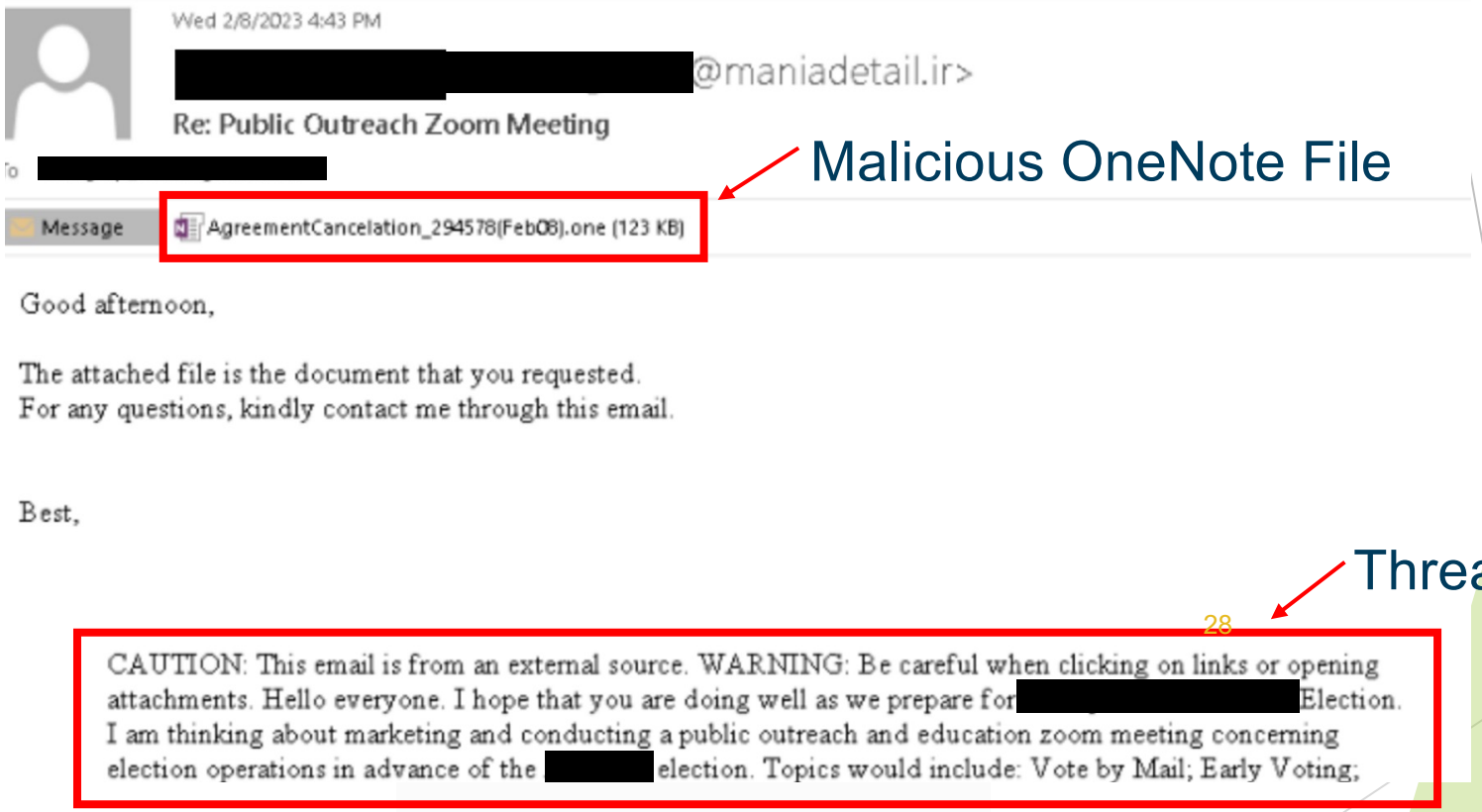
This content has nothing to do with the original message.

Consumer Technology Adaptation

OneNote

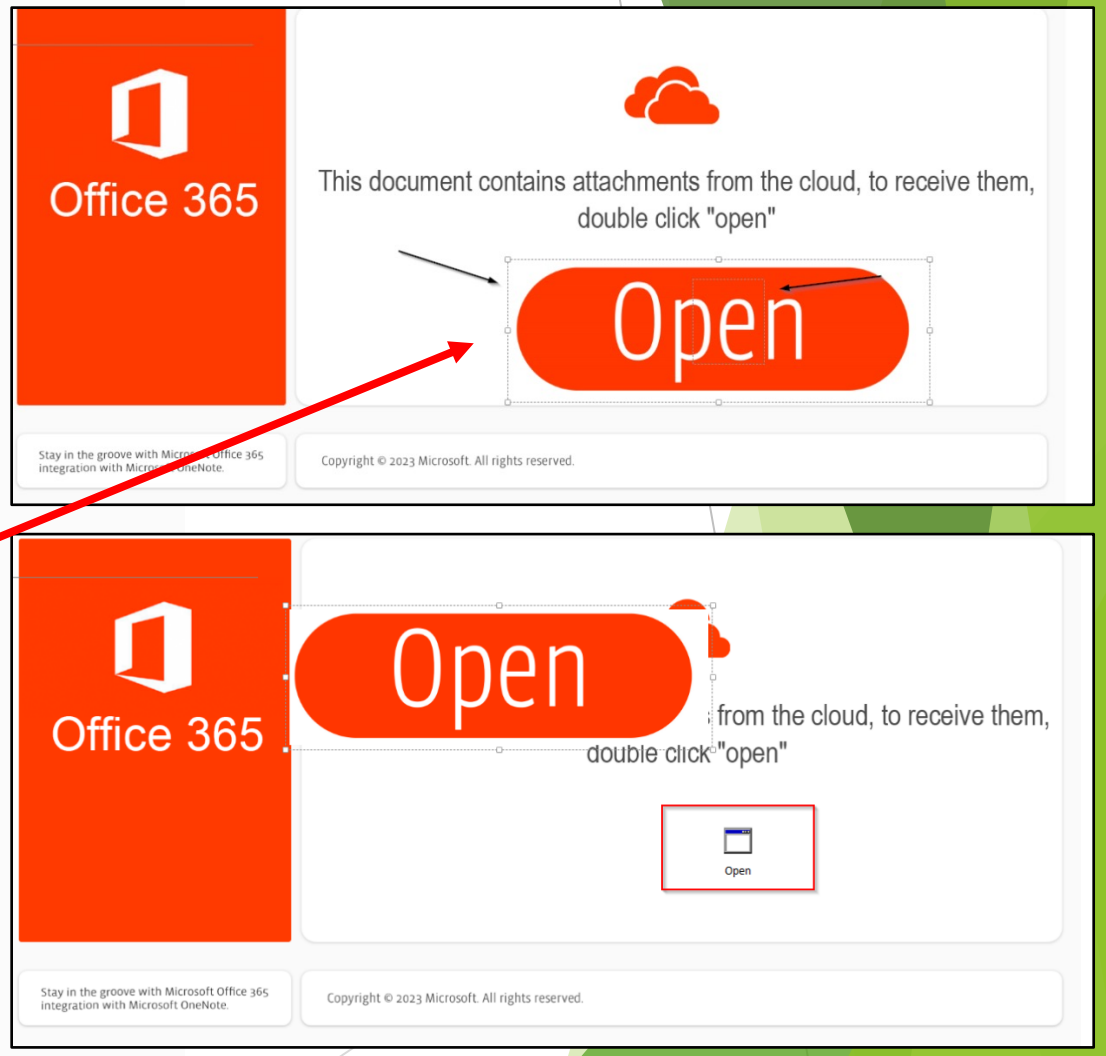
- Attackers used malicious OneNote files
  - Response to Microsoft's security measures limiting exploitation word/excel documents
- Based on open-source reporting and MS- and EI-ISAC data
  - 0 submissions to MCAP in 2022
  - 23 submissions to MCAP between January and February 2023
  - Submissions follow typical naming conventions of malspam
    - "Invoice," "Cancelation," "Complaint"

What does it look like:



OneNote Example

- File lures victims into opening
  - User interaction required
- Hidden malicious script
- Warning message often ignored

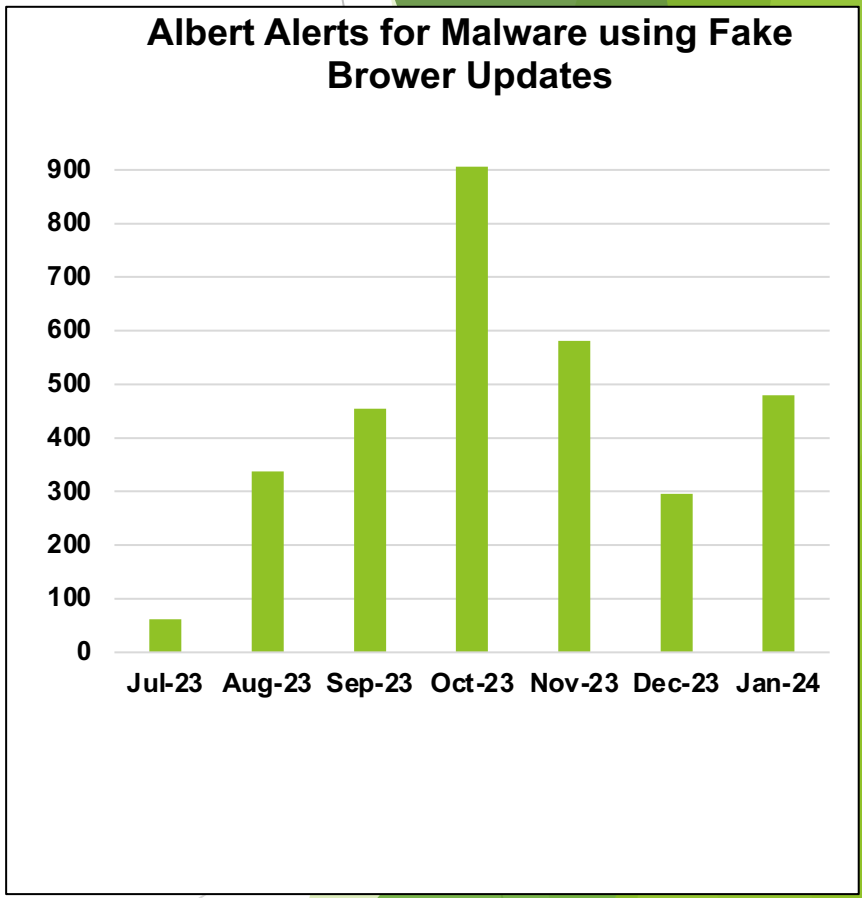


Moving the button shows the malicious script

Fake Browser Updates Deliver Malware

Exploiting the End User

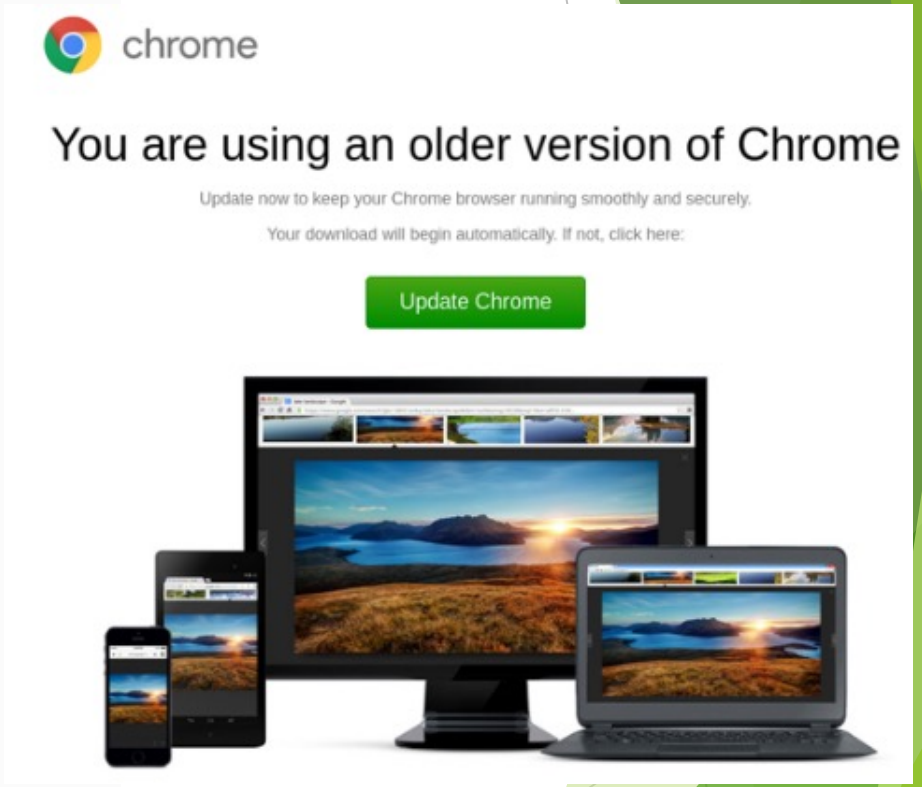
- Overview:
  - The campaigns compromise websites and display a fake update notification tailored to the user's browser.
- How It Works:
  - Users are led to compromised websites through:
    - Email, social media sites, search engines, or direct navigation.
  - Threat actors use JavaScript/HTML to direct traffic to a domain they control, then overwrite the webpage with a fake browser update to deliver the malware.
- Why It's Effective:
  - Takes advantage of end-users' security training and trust in the website or browser.



Fake Browser Updates Deliver Malware

Exploiting the End User

- SocGholish
  - Downloader written in JavaScript
  - Uses multiple methods for traffic redirection and payload delivery
  - Leads to various payloads such as Cobalt Strike, AsyncRAT, and NetSupport RAT
- RogueRaticate
  - Distinct from SocGholish but mimics its campaigns
  - Utilizes heavily obfuscated JavaScript
  - Leads to NetSupport RAT payload

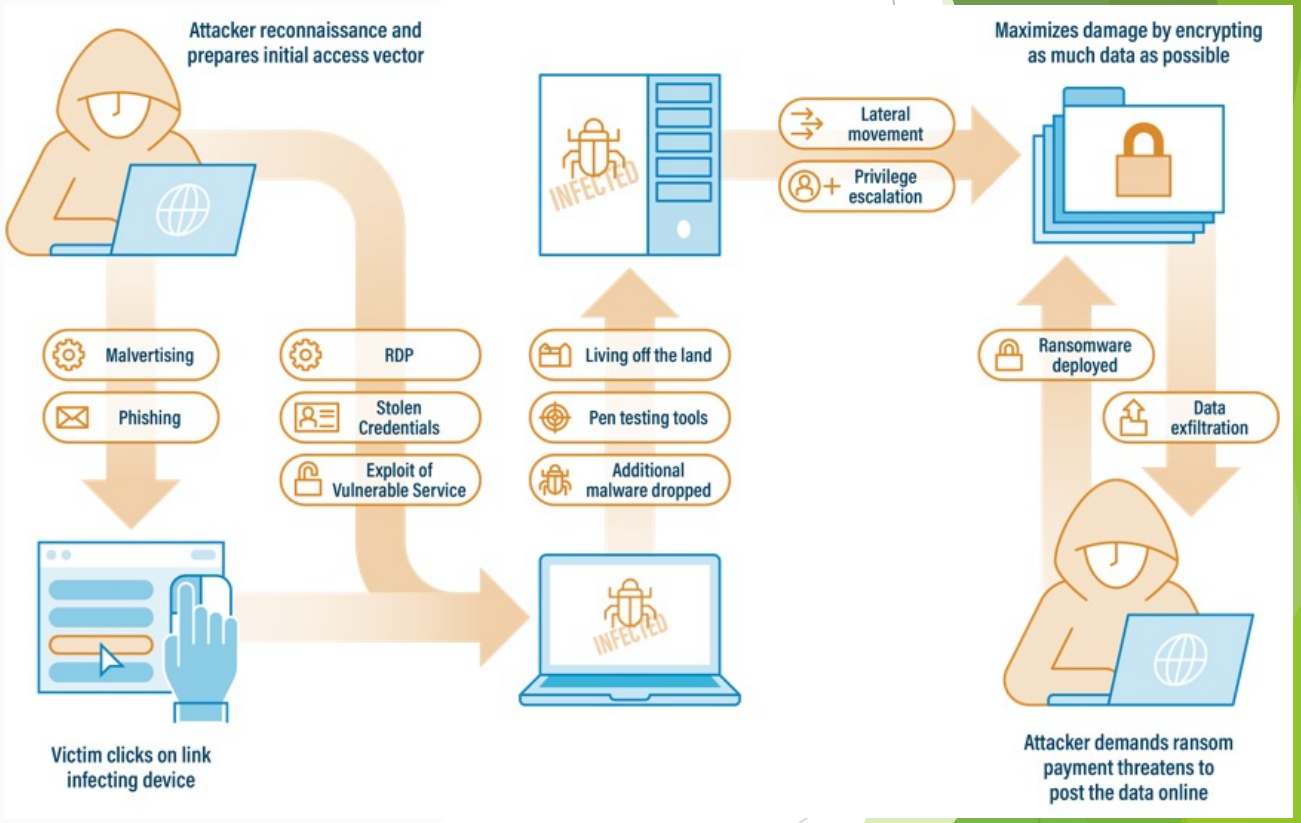


SocGholish Fake Browser Update
Source: Proofpoint

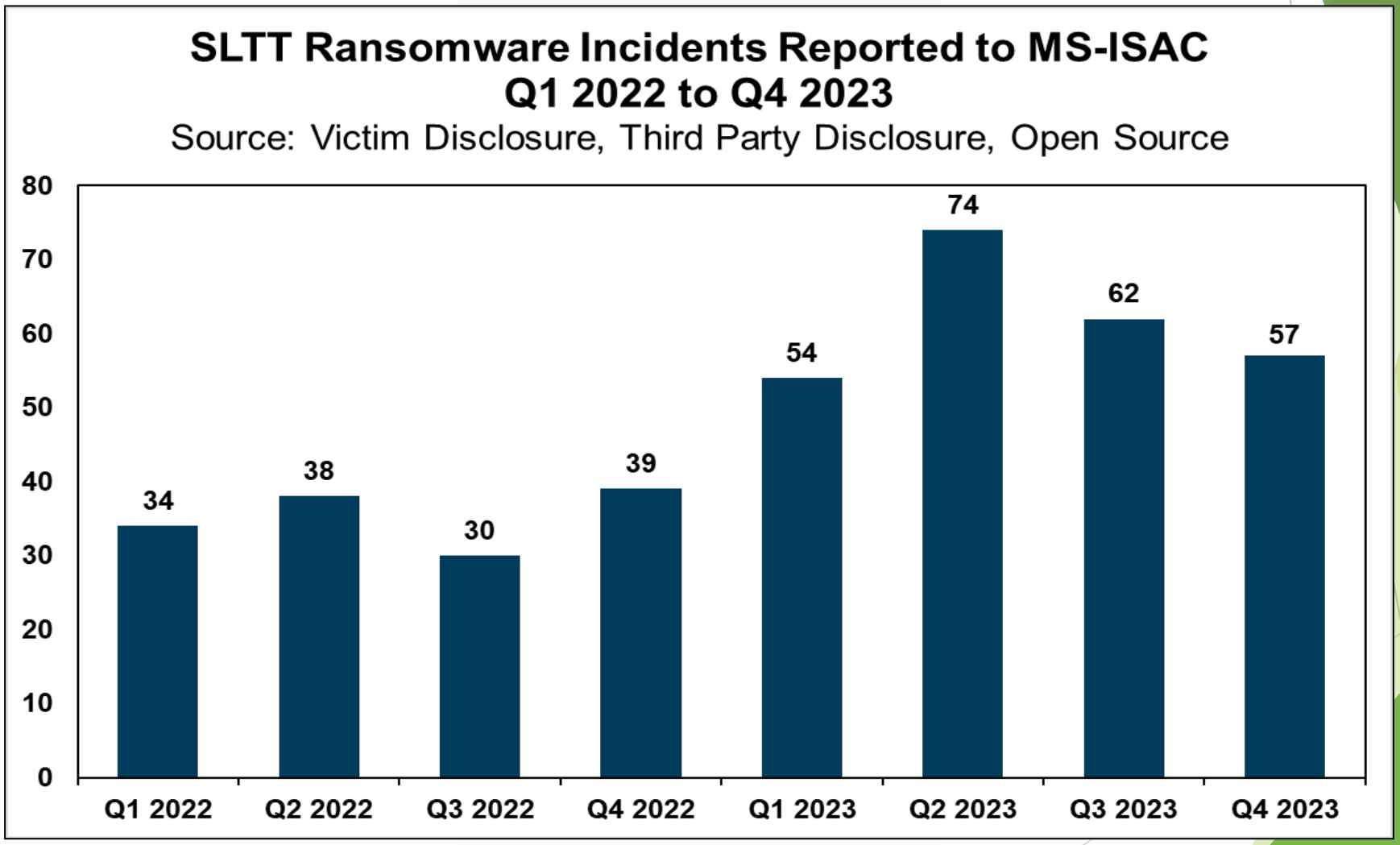
Classic Ransomware

Highest Impact Threat for State Local Tribal and Territorial Governments

- Malware typically encrypts data and attacker holds the key for ransom
- Evolution from commodity ransomware to big game hunting or post-compromise ransomware
- Increased use of double extortion
- Nearly half of all victims experienced data corruption
- Ransoms for SLTTs have increased into the 7-figure range

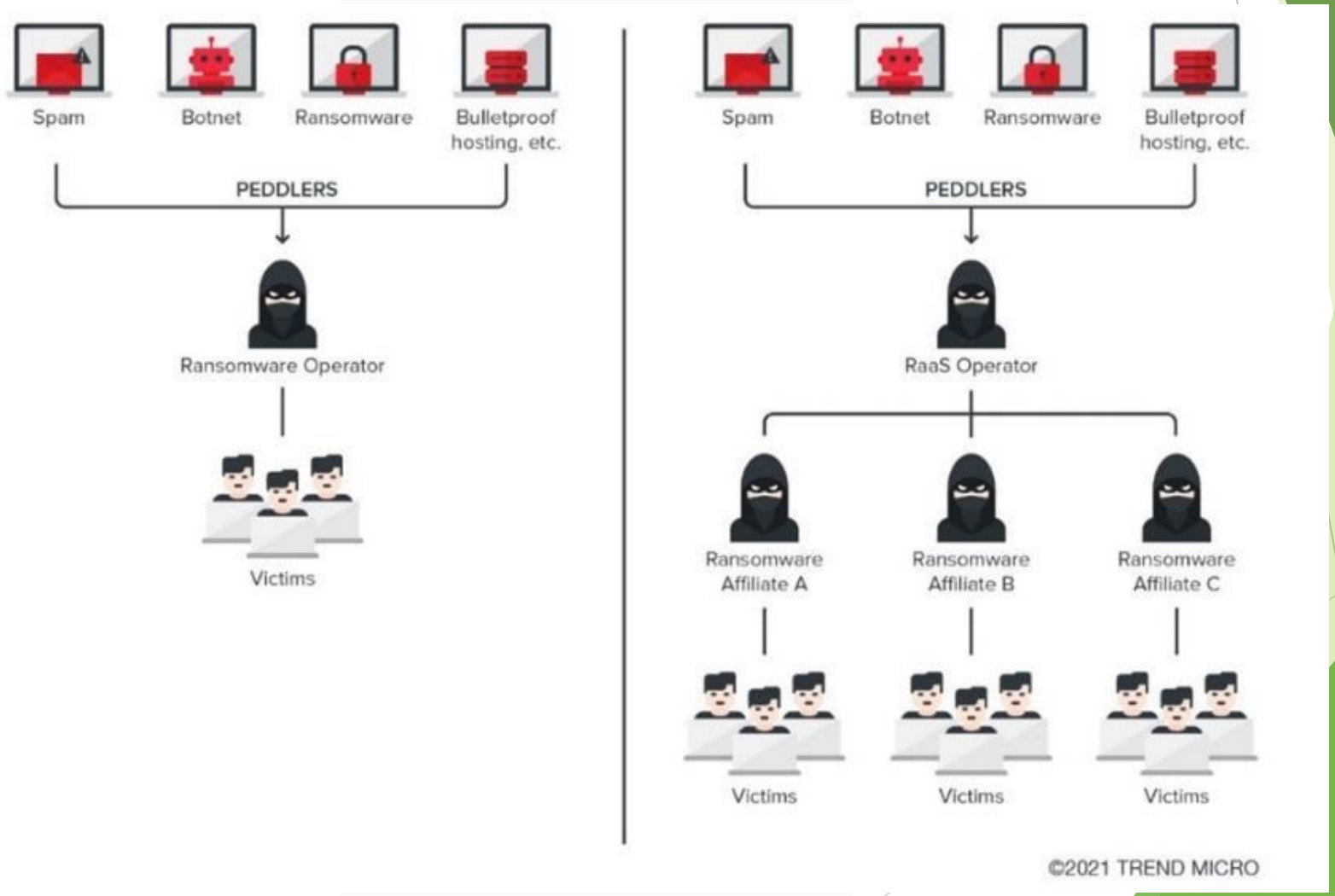


State Local Tribal and Territorial Governments Ransomware Incidents



Ransomware-as-a-Service Model

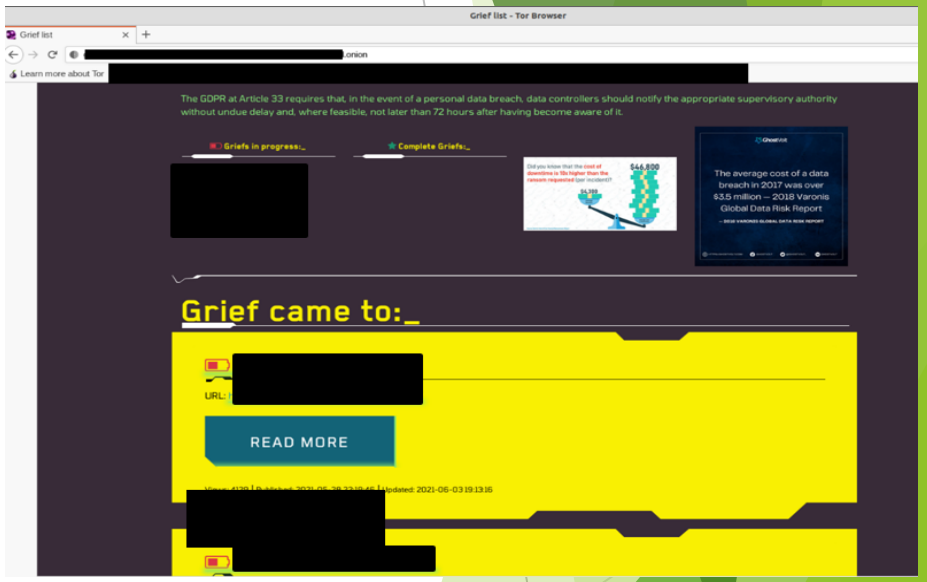
Franchising expands the potential victim set



Double Extortion & Encryption-less Data Extortion

Hybrid Ransomware Attacks and Other Harassment Tactics

- Encryption and exfiltration
  - Two forms of leverage or extortion, hence “double extortion”
- Other forms of extortion or harassment:
  - Distributed Denial of Service Attacks
  - Contacting the victim and associated parties to harass them
  - Publicizing attacks. For example, threat actor released a video detailing the type of data stolen from a K-12 school.
- Encryption-less data extortion
  - Multi-State Information Sharing and Analysis Center Cyber Threat Intelligence Team is observing attacks that involve exfiltration and data extortion without encryption



Ransomware Data Leak Site

LockBit Ransomware Group

Longstanding Threat to State Local Tribal and Territorial Governments

- Currently known as LockBit 3.0
- Active since September 2019
  - 2,000 plus U.S. organizations targeted since 2020 (Source: FBI)
- Most active ransomware data leak site
  - 2022: Claimed 830 victims
  - 2023: Claimed 1,049 victims
  - Customized tooling for data exfiltration
- Ransomware-as-a-Service Group
  - Recruits affiliates to conduct attacks
  - Wide variation in tactics, techniques, and procedures (TTPs)

Source: The Hacker News

LockBit Ransomware Group

Joint Cybersecurity Advisory

June 14, 2023
Joint Cybersecurity Advisory

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

In 2022, LockBit was the most deployed variant across the world and continues to be prolific in 2023. Since January 2020, affiliates using LockBit have attacked organizations of varying sizes across an array of critical infrastructure sectors, including financial services, food and agriculture, education, energy, government and emergency services, healthcare, manufacturing, and transportation

- LockBit group was taken down in joint operation – February 20th 2024
- LockBit group is currently active.

Ransomware Impacts

Disruptions to Resources and Process

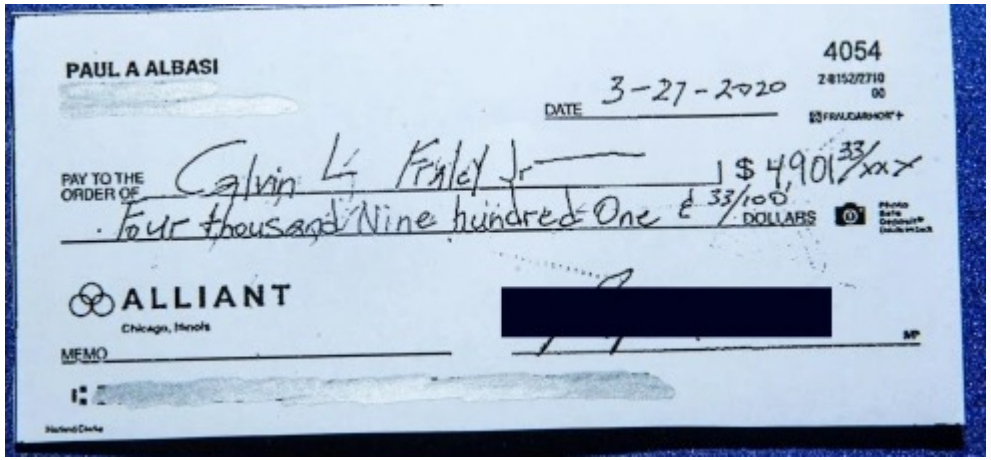
- Network downtime and disruption to critical systems
- Potential months long remediation, if not longer
- Significant remediation costs, sometimes over $1 million
- Sensitive data exfiltrated from network during attack
- Assume that it's not a matter of *if* you will be attacked, but *when* you will be attacked. Preparation is key.

Suspect #6
Check Fraud-

Here's how it unfolds: its old fashioned but it still works. Your checking account info is out there; perhaps you check is also accessible….

What it looks like: Check Fraud

Fraudster alters name, amount, endorsement on your government check – Now instead of paying PPL your paying Calvin Finley Jr?

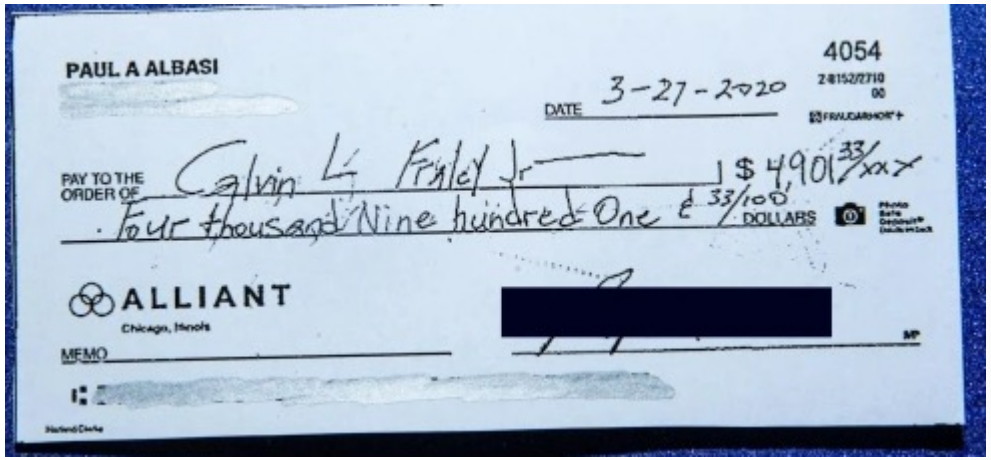


Did not have fraud services on account – did not reconcile or review accounts on a daily basis = Caught fraud too late. Likelihood of recovery is low.

- Move to electronic payments – ACH or commercial card or real time payment.
- Implement check fraud service – Payee positive pay: verify the check number; the amount and the payee info!

What it looks like: Check Fraud

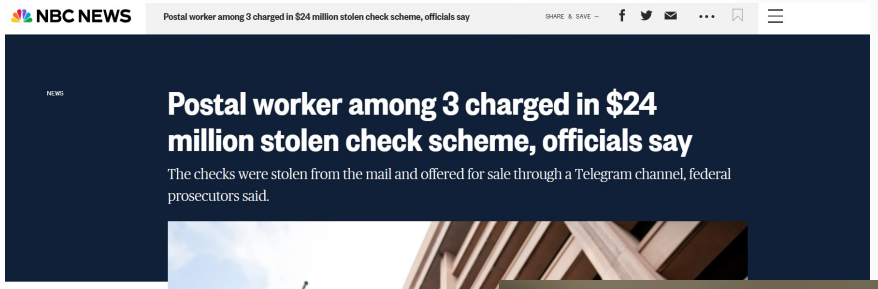
Fraudster alters name, amount, endorsement on your government check – Now instead of paying PPL your paying Calvin Finley Jr?

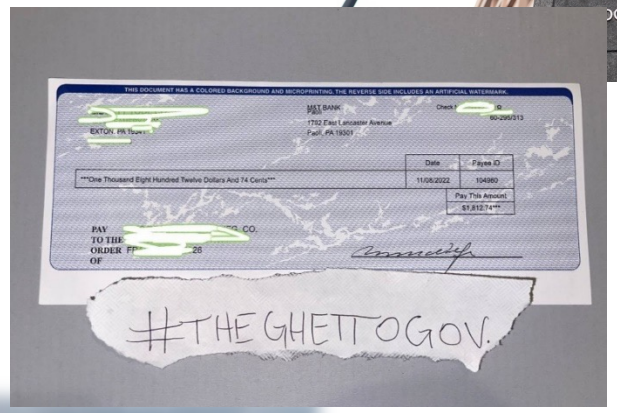


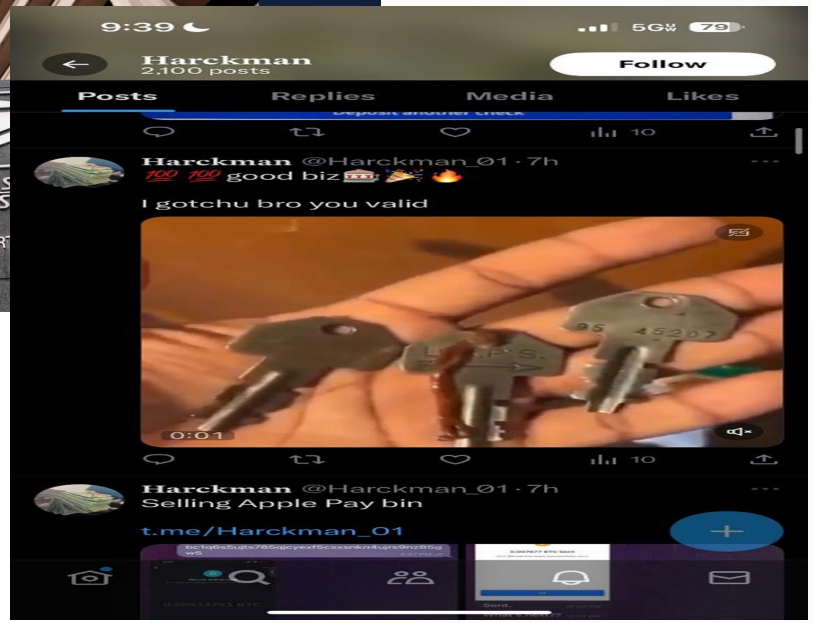
Continuation of this fraud – <u>You catch</u> the fraud manually and recover funds; Fraudsters continue to submit checks (months or even years later) to "test the waters" again. They may even try accounts that you do not process checks out of…

- Lock down accounts: Check block
- Utilize one account for all transaction and lock down sub accounts

How did the fraudster get your check?







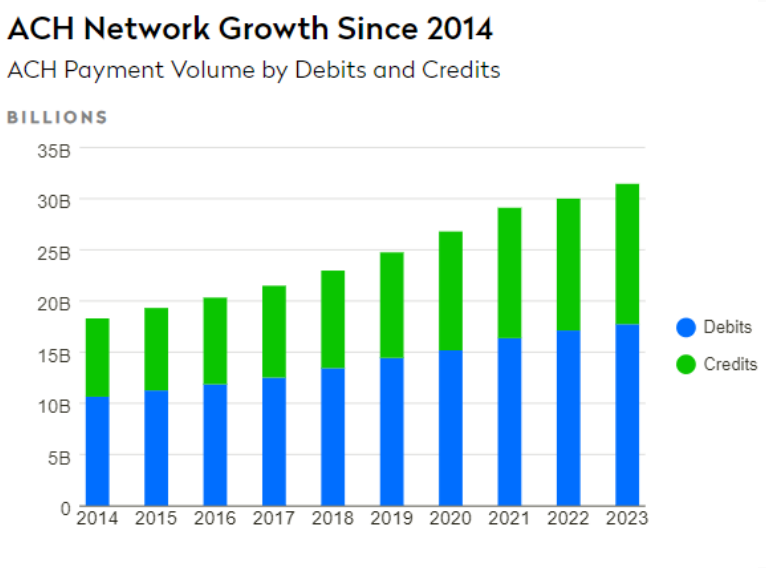
- Move to electronic payments – ACH or commercial card or real time payment.
- Implement check fraud service – Payee positive pay: verify the check number; the amount and the payee info!

Suspect #7 ACH Fraud

Here's how it unfolds: They have your info – your account is charged via ACH for a transaction you do not recognize…..

What it looks like: Check Fraud

Fraudster utilizes dark web and has access to your ACH info or fraudster requests changes to ACH payment via email; phone or mail -



- Do not accept changes via phone, email, or postal mail. Verification of payment beneficiary via a call back using confirmed contact information from company website.
- ACH and wire payments should be initiated under dual control using two separate computers (e.g., one person creates the funds transfer, and a second person approves the funds transfer from a different computer system)

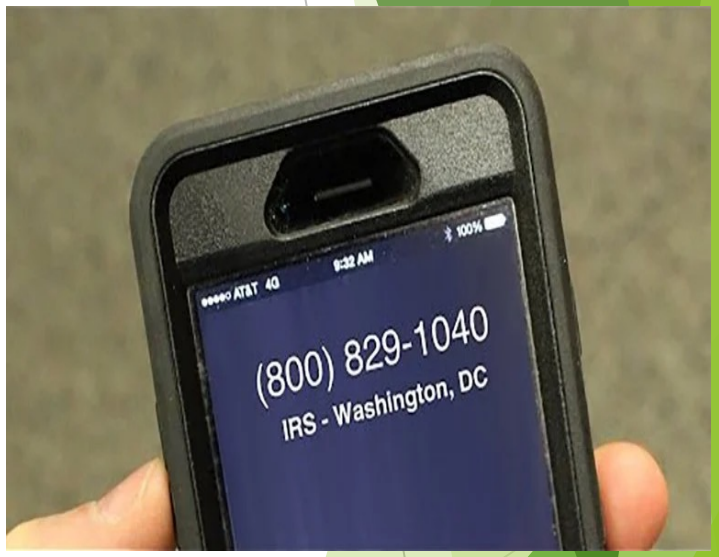
- Implement Fraud Services: ACH Monitor– Authorizes certain entities to debt your account while blocking all others. Email alerts are issued for any debts not matching your preapproved authorization. Make pay or return decisions that do not match pre-authorization.
- Lock down accounts that do not utilize ACH but that are still open to fraud – ACH Block

Suspect #8 Phone Spoofing; Customer Service Impersonation

Here's how it unfolds: You receive a call from your financial institution customer service number….

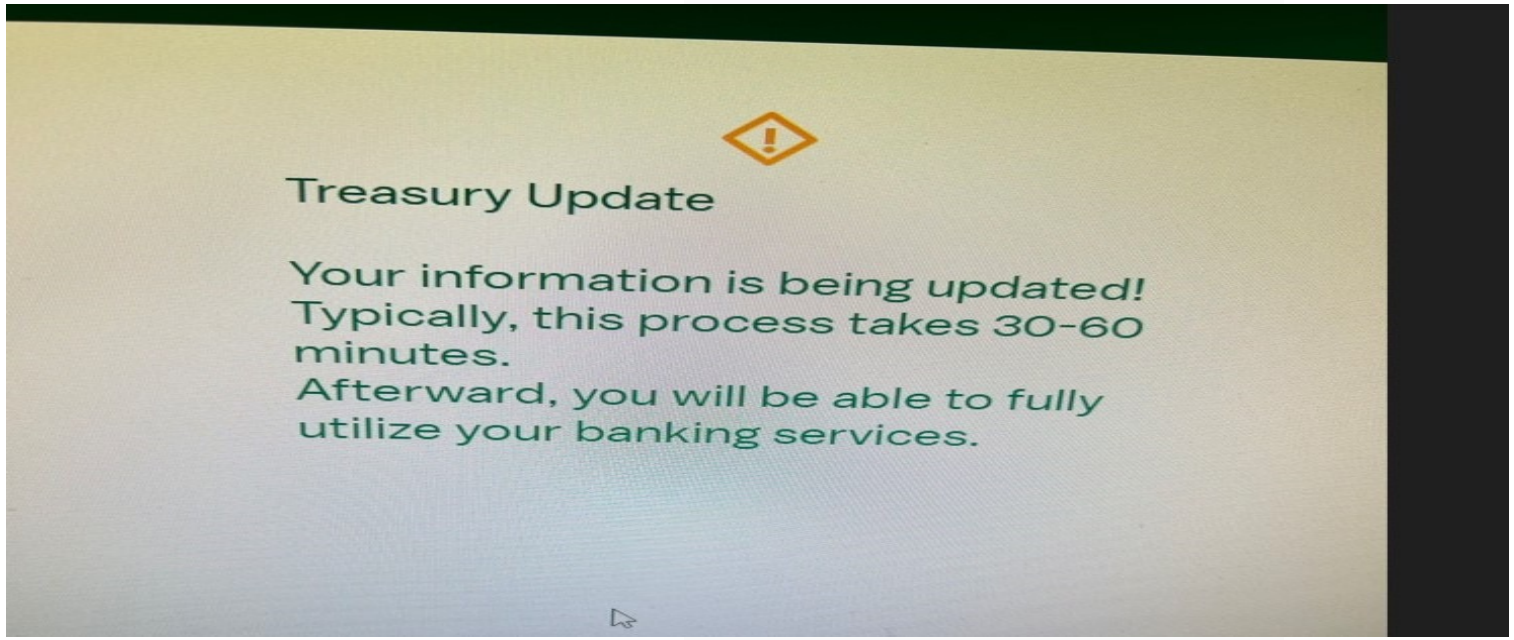
What it looks like: Phone Spoofing / Account takeover

- Fraudsters are calling customers pretending to be employees of banks
- Telling customers their account has had a recent fraud or their online banking needs a malware update
  - Customer gives access
- Fraudster tells customer to stay out of online platform while fix applied
- Fraudster changes phone number and address
- Fraudster sends wires and/or ACH Payments
  - Fraudster processes 10 wires – approx. $4.2MM



- Call the Bank at a number you have
- Establish Dual authorization approval for changes to online banking services

What it looks like: Phone Spoofing / Account takeover

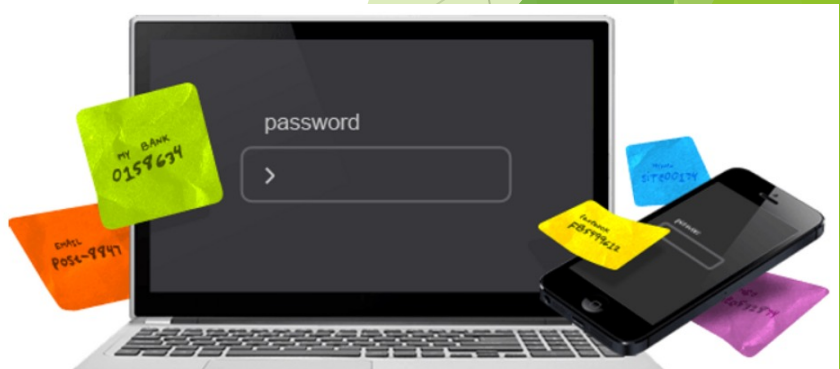


- When logging into online banking, please verify that the login URL is correct. We recommend that you do not search for it via a search engine, as fraudsters will often try to impersonate bank screens by creating links with extra characters or different domains.

Practical Strategies to Prevent and Protect

Passwords

- Nobody likes creating, managing and changing passwords
- Hackers can purchase tools and algorithms to crack them if they're not long and strong
- Passwords should be:
  - Longer
  - Stronger
  - Don't use info readily available on your social media pages (kid's or pet names)
  - Don't reuse passwords ESPECIALLY for financial sites
  - Don't share passwords
  - Use upper case letters, lower case letters, numbers, special characters



Passwords

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case aplhabets	Mixed numbers, Lower and Upper case aplhabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

Prevention Considerations

- Implement an awareness and training program. Because end users are targeted, employees and individuals should be made aware of the threat of ransomware and how it is delivered.
- Patch operating systems, software, and firmware on devices, which may be made easier through a centralized patch management system.
- Ensure anti-virus and anti-malware solutions are set to automatically update and that regular scans are conducted.
- Manage the use of privileged accounts. Implement the principle of least privilege: no users should be assigned administrative access unless absolutely needed; those with a need for administrator accounts should only use them when necessary.
- Configure access controls, including file, directory, and network share permissions, with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

Source: Federal Bureau of Investigation - Cyber Task Forces - www.fbi.gov/contact-us/field

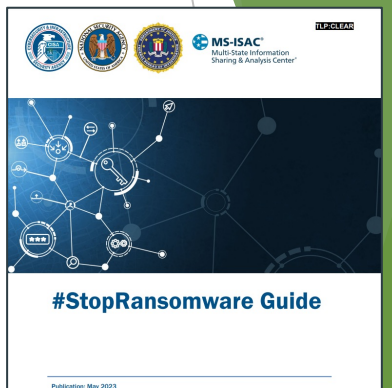
Prevention Considerations

- CIS Critical Security Controls
- SLTTs: Malicious Domain Blocking & Reporting (MDBR)
- Cybersecurity Awareness Campaign
- Keep Software Updated
- Identify & Patch Vulnerabilities
- Backup, Backup, Backup
- Secure Network Access
- Implement Multi-Factor Authentication (MFA)
- Enforce Password Policy
- Refer to CISA resources on Securing Supply Chain

Recommendations for SLTTs

Preparation is Key

- #StopRansomware Guide
  - Best practices and incident response guidance
  - Joint guide (CISA, FBI, NSA, and MS-ISAC)
- CIS Critical Security Controls
  - Provide a prioritized set of actions to protect your organization and data from known cyber-attack vectors.
- CIS Community Defense Model 2.0
  - How effective are the CIS Controls against the most prevalent types of attacks?



CIS Controls

Top 5 Attacks	IG1 CIS Safeguards IG1 can defend against XX% of ATT&CK (Sub-)Techniques	All CIS Safeguards CIS Safeguards can defend against XX% of ATT&CK (Sub-)Techniques
Malware	77%	94%
Ransomware	78%	92%
Web Application Hacking	86%	98%
Insider and Privilege Misuse	86%	90%
Targeted Intrusions	83%	95%

All percentages are based on ATT&CK (sub-)techniques assigned to an ATT&CK mitigation.

No-Cost CIS/MS-ISAC Benefits

https://learn.cisecurity.org/ms-isac-registration

Cyber Threat Intelligence

- Cyber Alerts & Advisories
- Quarterly Threat Report
- Regular IOCs
- White Papers
- Cyber Threat Briefings
- Real-Time Intelligence Feeds

Cybersecurity Services

- 24x7x365 Security Operations Center (SOC)
- ISAC Threat Notification Service (IP & Domain Monitoring)
- Malicious Domain Blocking & Reporting (MDBR)

Security Best Practices

- CIS SecureSuite Membership
  - *Tools to implement the CIS Critical Security Controls and CIS Benchmarks*

Other Member Resources

- MS-ISAC Webinars
- MS-ISAC Working Groups
- Nationwide Cybersecurity Review (NCSR)
- Homeland Security Information Network (HSIN)
- CIS CyberMarket

WHAT TO DO IF YOU SUFFER FRAUD OR SUSPECT FRAUD

In the event you become a victim of fraud, help protect your financial interests with the following recommendations:

- Immediately contact your financial institution to request that the following actions, and any others you consider appropriate, be taken to help contain the incident:
  - Change online banking passwords
  - Confirm recent account transactions
  - Close existing account and open new account(s), as appropriate
- Ensure that no one has requested an address change, title change, PIN change or ordered new cards, checks or other account documents be sent to another address
- Immediately cease all activity from computer systems that may be compromised
- Log-off and shut down PC
- Unplug the Ethernet or cable modem connections to isolate the system from remote access
- Immediately contact your security officer or other security advisor to ensure you are following appropriate security guidelines and procedures to help contain the situation
- Contact your local police department. This can help with recovery and insurance claims
- File a report with www.ic3.gov. FBI's site can sometimes help with recovery

What should I do if my business is attacked by fraud?

Time is critical. The following

6 steps

can help you act quickly to gather as much information as possible.

Step 1

NOTIFY YOUR BANK

They can help expedite a resolution.

Step 2

CHANGE ALL ONLINE PASSWORDS

Step 3

PULL PAYMENT REPORTS

Get a top-line view of all transactions.

Step 4

STOP UNPROCESSED PAYMENTS

Step 5

REVIEW USER AUDIT REPORTS

Disable unrecognized users.

Step 6

INITIATE PAYMENT RECALLS

Make the requests; they are not always guaranteed.

TAKE AWAYS

- Institute continuous education with staff at all levels on recognizing fraud, risks and mitigants
- Work with your IT department or consultant to harden your systems.
- Implement a stand-alone computer for banking access only
- Limit paper payment methods in favor of more secure electronic payment options
- Work with your financial institution to enable the most comprehensive fraud prevention
- Vigilance – See something – Say something

John Callahan
Senior Vice President |Government Banking
Relationship Manager
M&T Bank
213 Market Street, 1st Floor,
Harrisburg PA 17101
jcallahan@mtb.com
Cell: 717-852-5960
https://www.linkedin.com/in/govbanking/

Jesse Adams
GSEC, GICSP
Cyber Threat Intelligence Analyst
31 Tech Valley Drive
East Greenbush, NY 12061
Jesse.adam@cisecurity.org

Q and A - Discussion

“The greatest compliment that was ever paid me was when someone asked me what I thought, and attended to my answer.” – Henry David Thoreau

Disclosures

- This presentation is for informational and educational purposes only. Nothing herein should be considered or relied upon as legal advice. The author assumes no responsibility or liability for the specific applicability of the information provided. Please consult your own legal counsel for any legal advice.
- Some products and services may be provided through subsidiaries or affiliates of M&T Bank.
- Visa is a registered trademark of Visa International Service Association.
- Unless otherwise specified, all advertised offers and terms and conditions of accounts and services are subject to change at any time without notice. After an account is opened or service begins, it is subject to its features, conditions and terms, which are subject to change at any time in accordance with applicable laws and agreements. Please contact an M&T representative for full details.