PUBLIC SAFETY ANSWERING POINT (PSAP) CYBERSECURITY AWARENESS WEBINAR

Webinar “Ground Rules”

- Copies of slides and a handout with supplemental resources will be provided
- Ask questions by “raising hand” or putting them in the chat section
- What we mean by PSAPs [includes Emergency Communications Centers (ECCs)]
- Any slide with a green background is a Best Practice recommendation

Program Sections

I. Program Intro and Overview

II. Why PSAPs are a Target

III. Types of Attacks

IV. Specialized Attack Situations – Examples and Protection

V. Cyber Hygiene and Best Practices

VI. Responding To and Reporting Cyber Incidents

VII. Summary

VIII. Closing Thoughts

SECTION I
PROGRAM INTRO & OVERVIEW

Recent Attack Examples

On the morning of April 26, 2023, an Oregon county server provided alerts regarding malicious activity taking place. Following an assessment, it was identified the system activity resembled an encryption event from a ransomware attack.

This ransomware encrypted critical files and systems, disabling access, and rendering devices on the county network inoperable.

The County Sheriff's Office Emergency Communications Center (ECC), which provides 911 services for the county, was impacted by the ransomware rendering computer terminals and critical systems such as Computer-aided Dispatch (CAD) inoperable.

The County's Land Mobile Radio System (LMRS) and 911 Phone System were not impacted by the cyber incident and continued to function normally.

Hackers- What Is Their Motive?

Disruption

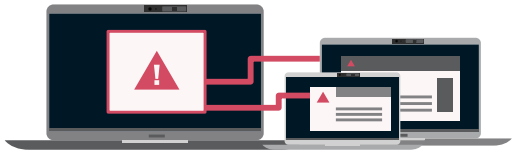
Cyberattacks may shut down public access to 9-1-1, leading to public confusion and disrupting the dispatch of First Responders

Ransom

As the networks, data, and services are vital to public safety, PSAPs are more likely to pay a Bitcoin ransom in order to restore service

Target of Opportunity

PSAPs, municipalities, may not have a strong cyber defense system – especially when compared to other targets

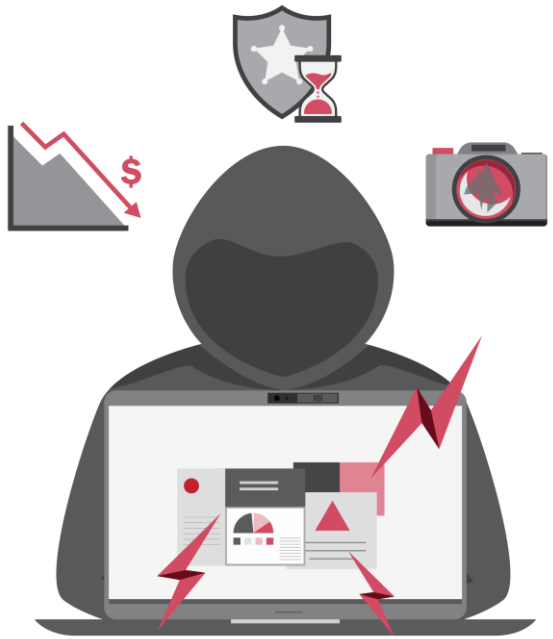


Collateral Damage

Victim of Lateral Attack where hackers are looking to get a toehold and spread to as many connected netowrks

The Potential Cyberattack Impact

- Telephony Denial of Service (TDoS) may prevent the public from reaching 9-1-1 or the 10-digit admin line
- Computer-Aided Dispatch (CAD) or records systems encrypted – no access
- Delay in dispatching first responders
- Destroying evidence, such as body camera footage
- Financial loss



Why This Webinar Was Developed

- Attacks are on the rise and can have a devastating effect on the primary mission of the PSAP
- Webinar serves as awareness education and is part of a larger education/ protection program
- Provides threat preparedness and response suggestions

SECTION II
WHY PSAPS ARE VULNERABLE TO ATTACKS

PSAP Cybersecurity

ECCs are much more dependent on technology to operate than they were years ago

- **Defending:**
  - 9-1-1 Call Handling
  - CAD
  - Radio
  - Records
  - Critical Systems

Risk Level Increases With NG9-1-1

- **Next Generation 9-1-1 (NG9-1-1) is different from traditional systems:**
  - Requires standardized identity management and credentialing across systems
  - Introduces new attack vectors
  - Possible to launch multiple distributed attacks with greater automation from a broader geography against more targets

Current Vectors

New Vectors

Why Is the Public Sector A Target?

- **Willingness to pay the ransom**
  - PSAPs are critical to the effective delivery of life-saving public safety services
  - Desire to avoid negative publicity and loss of public confidence
  - Agencies are frequently tasked with providing services to citizens with limited access to technical and cybersecurity resources

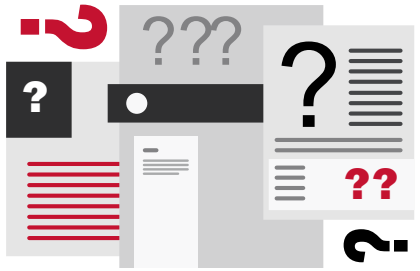
What Is “Cyber Reflection” a.k.a. Hacktivism?

- For every geopolitical protest you see happening in-person, there’s a reflection associated with the demonstration happening in cyberspace
- Just as people protest in-person, many times they also protest in cyberspace

Cyberattacks During Civil Unrest – Why?

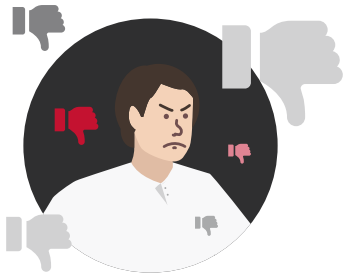
Disruption

Cyberattacks may shut down public access to 9-1-1, leading to public confusion and disrupting dispatch



Disinformation

Spreading false or misleading information about the events or situation



Loss of Confidence

If citizens are unable to connect with law enforcement/PSAP, they will lose confidence and may take matters into their own hands

Cyberattacks During Civil Unrest - Examples

- Minneapolis PD was the target of a cyberattack executed in support of the protests occurring in May 2020
- Ferguson (MO) PD's website and e-mail were attacked after the grand jury declined to indict the officer and the Chief's personal information was stolen and released in a doxxing attack
- Baltimore city website and other government systems were compromised during the civil unrest in April 2015

Defending Against Attacks During Civil Unrest

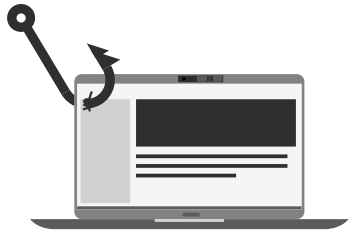
Over the rest of this presentation, we will discuss:

- Why PSAPs should employ a Voice Firewall capable of detecting TDoS attacks
- Why antivirus software is important to keep systems secure
- Example security practices that help minimize the risk of outside access to your information
- Creating a plan to ensure successful and efficient communication, mitigation, and recovery should an attack occur

SECTION III
TYPES OF ATTACKS

Types of PSAP Cyberattacks

Direct TDoS Attack Against 9-1-1 and Admin Phone Lines



Phishing: Over 90% of successful attacks

Indirect Attack: Lateral, Ransomware, etc.

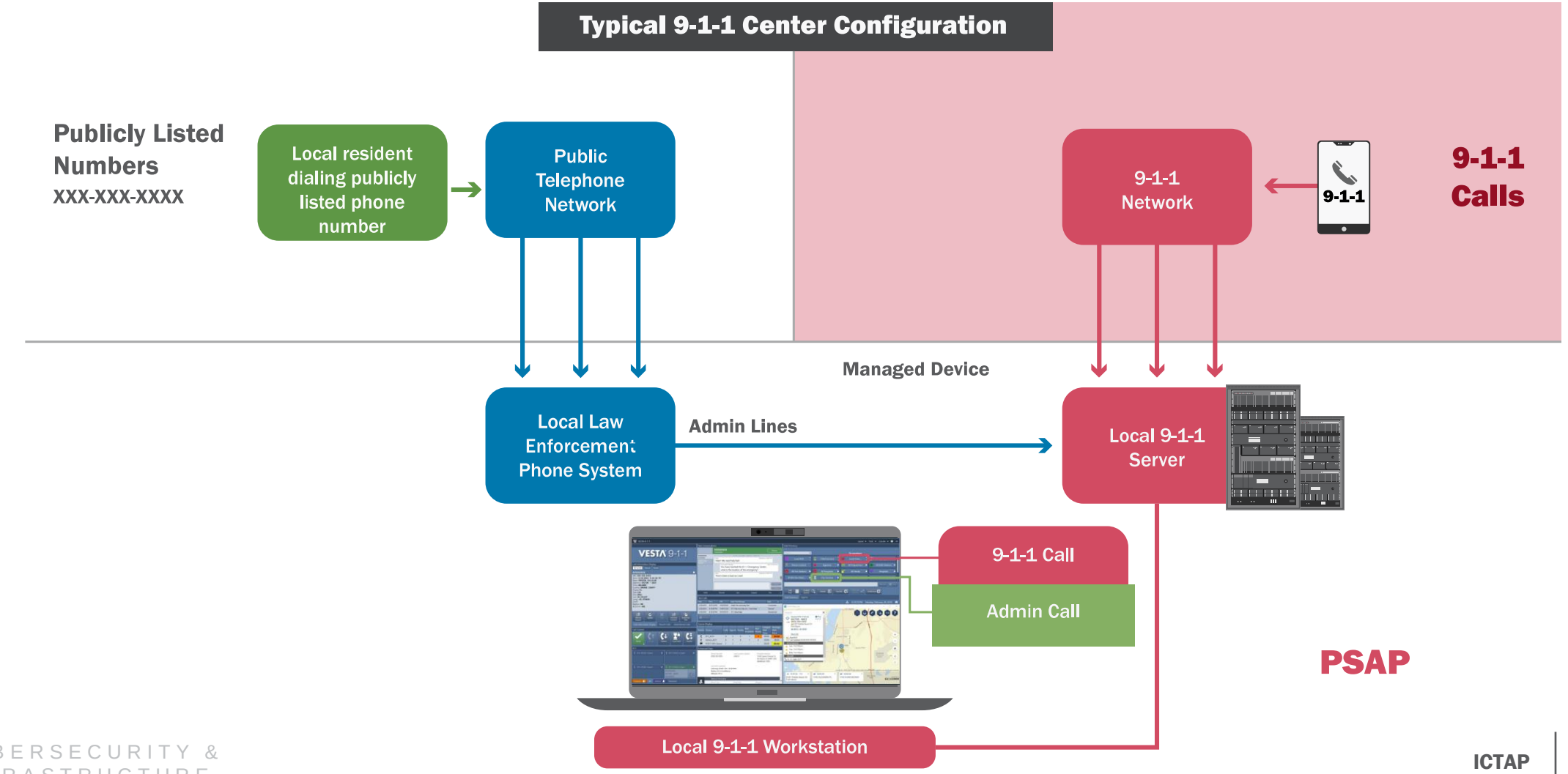
Remote Access to Systems

Attacks Against PSAPs and Admin Phone Lines TDoS

Denial of Service Attacks (DoS)

- An attempt to exhaust resources available to a network or server and interrupt access to genuine users (such as 9-1-1)
- One of the oldest forms of cyberattacks
- TDoS is the voice communications version of Digitial DoS (DDoS)

Typical 9-1-1 Center



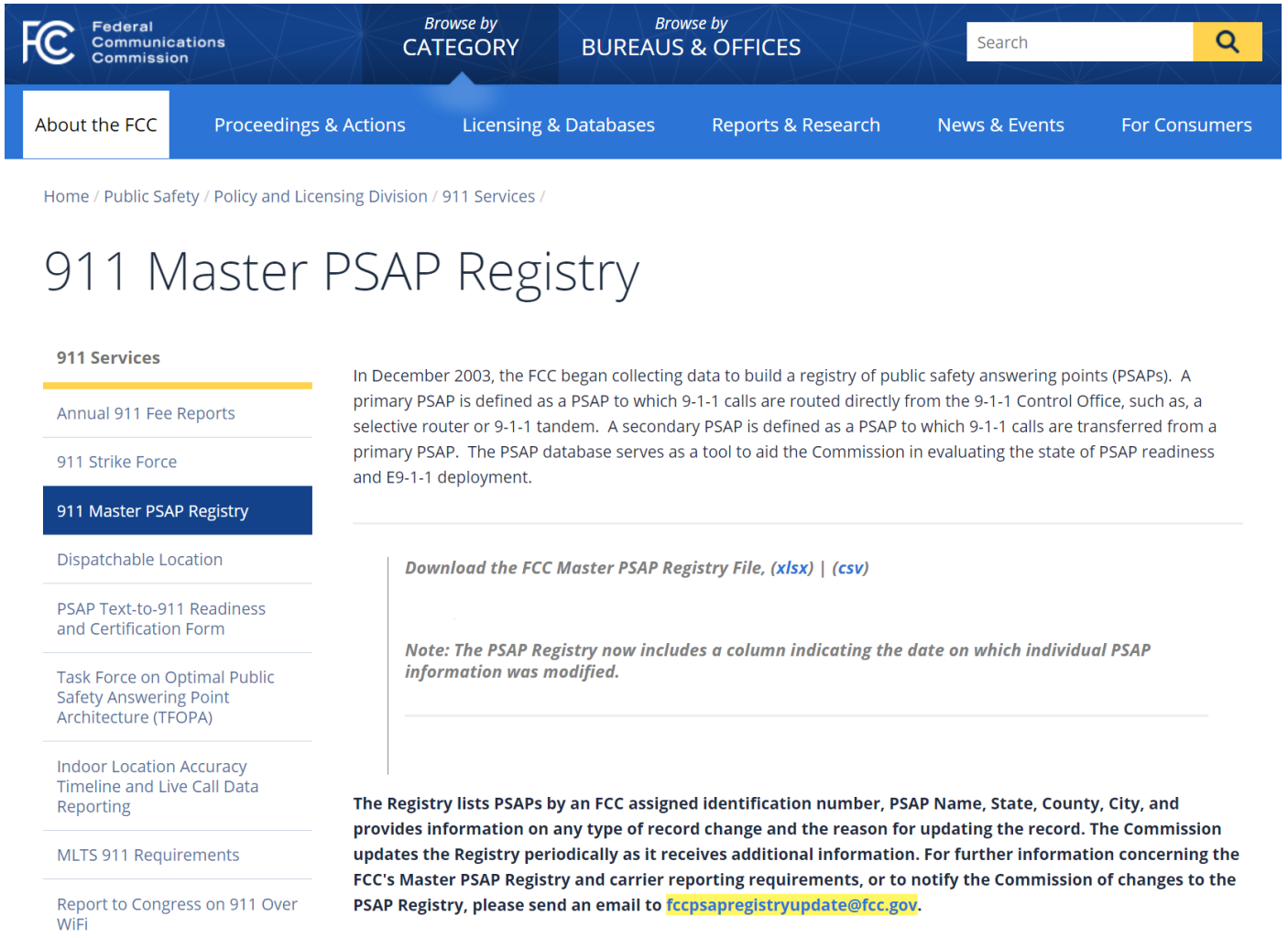
Example – TDoS Attack Actors

- Actors located in the Gaza Strip
- Attacked PSAPs in numerous states beginning in 2019
- An attack can last hours or days

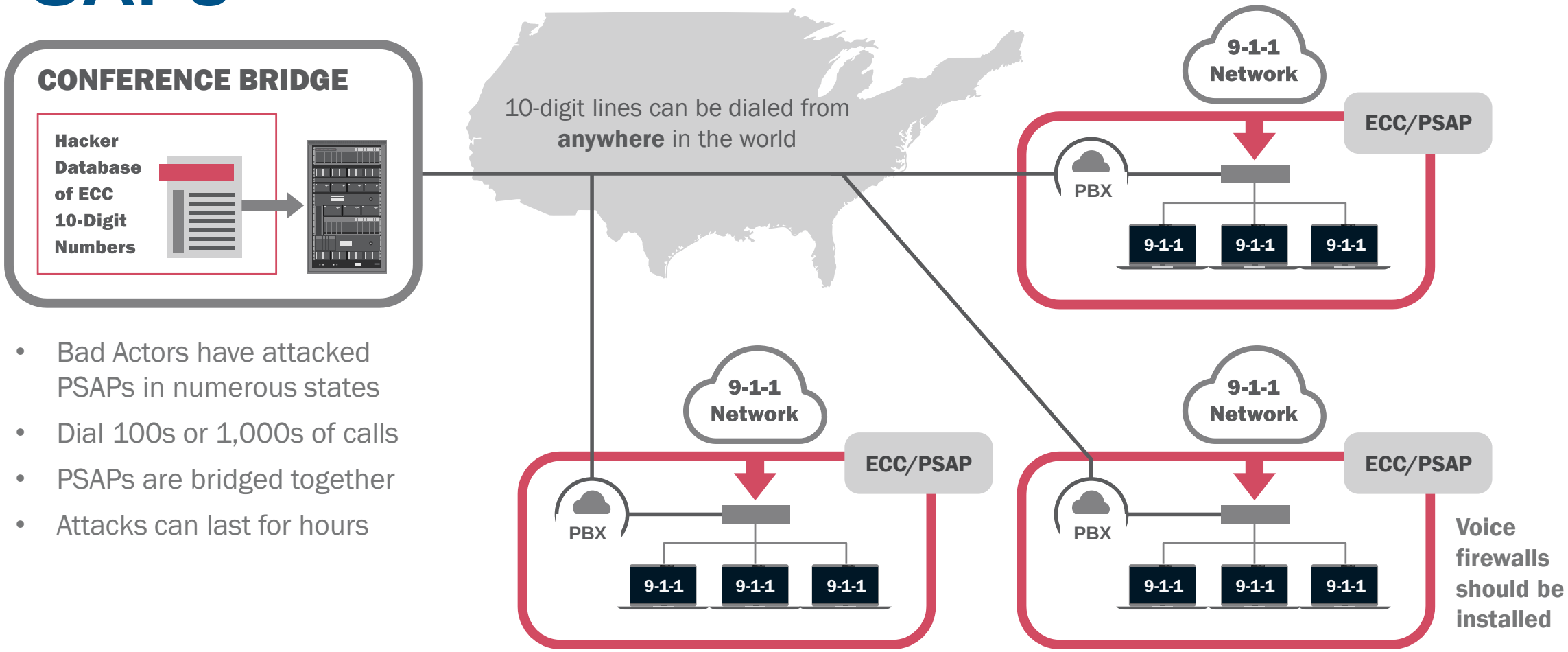
Attack Methods:

- Dialing/Hang Up on PSAP Answer
- Conference PSAPs Together
- Verbal Threats to Call Takers

PSAP Locations Are Available Online



TDoS Attack – Admin Lines – Multiple PSAPs

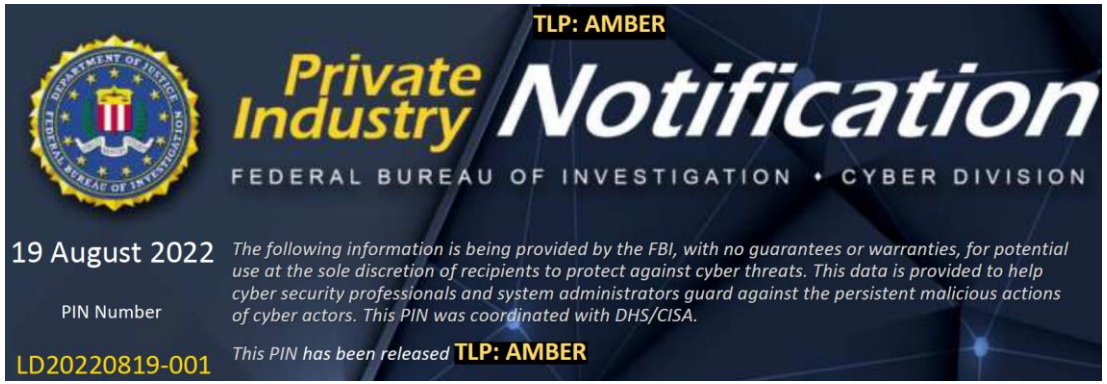


- Bad Actors have attacked PSAPs in numerous states
- Dial 100s or 1,000s of calls
- PSAPs are bridged together
- Attacks can last for hours

Industry Best Practice – Voice Firewall

Industry Examples

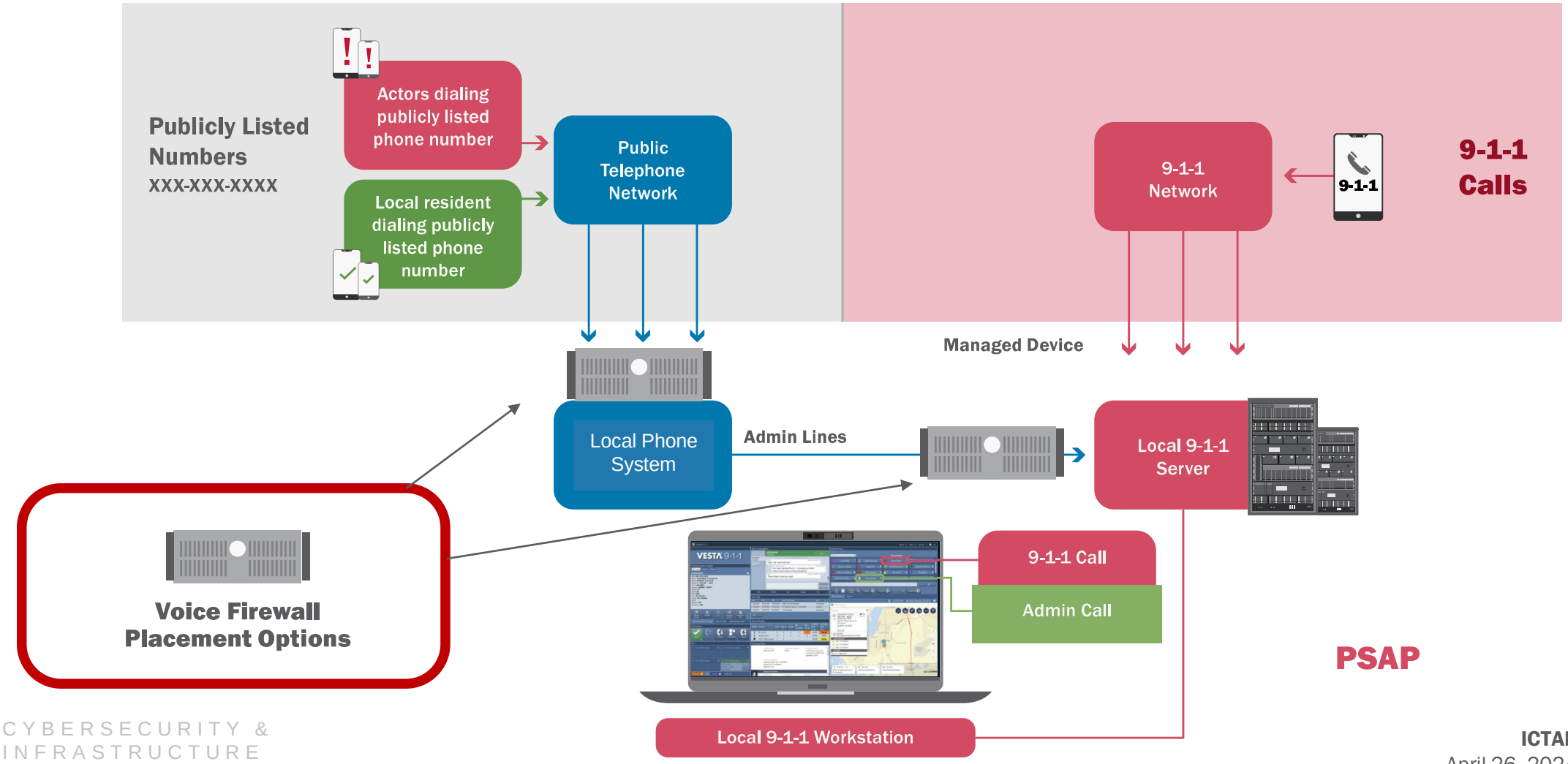
- Military Bases
- Healthcare: Hospitals
- Financial: Banking
- Call Centers



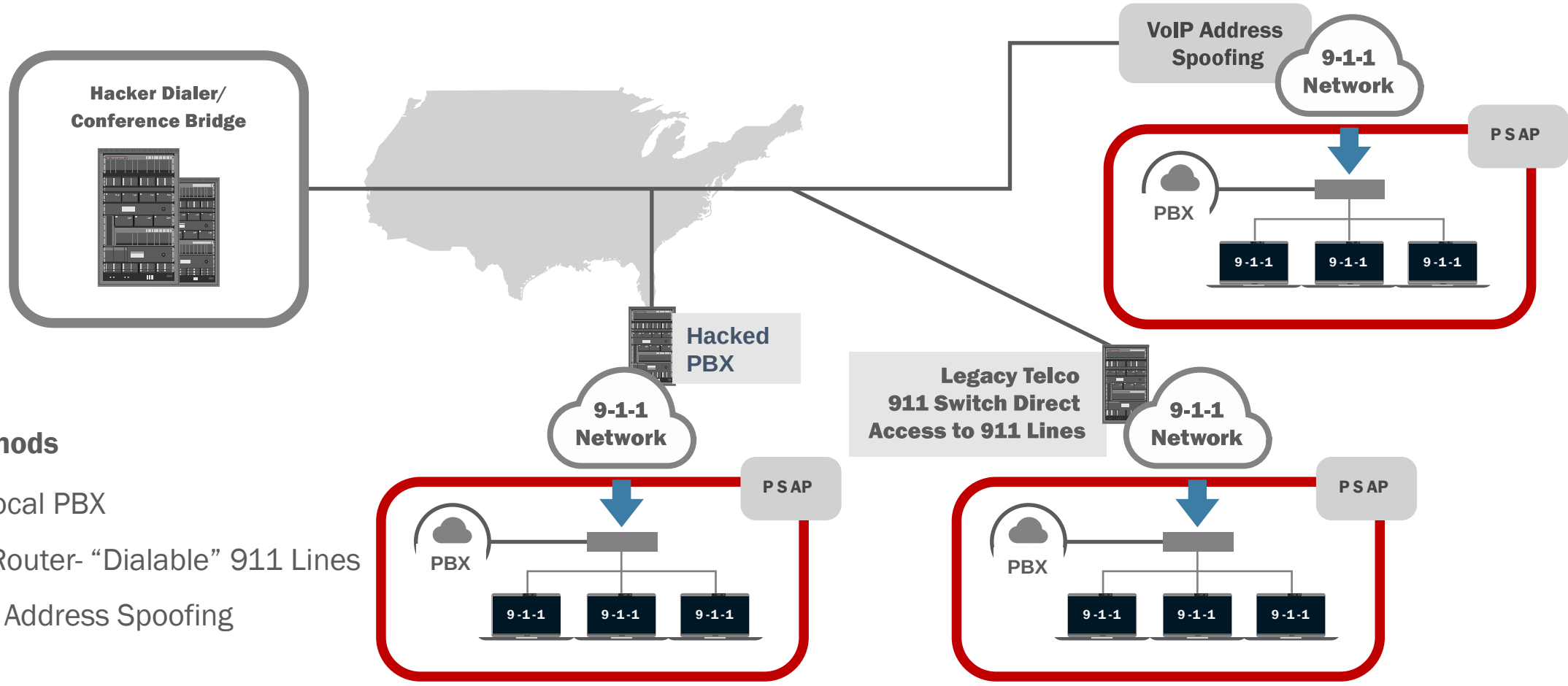
Recommendations

- Voice Firewall Should be Installed on Admin Lines at PSAPs
- Protection against Robo Calls
- Stops TDoS Attacks

Protecting Admin Lines



TDoS Attack- 911 Lines- Multiple PSAPs



Multiple Methods

- Hacking Local PBX
- Selective Router- “Dialable” 911 Lines
- VoIP Local Address Spoofing

Protections Against Erroneous Blocking

FEDERAL REGISTER
The Daily Journal of the United States Government

September 2020
AGENCY: Federal Communications Commission (FCC)
ACTION: Final rule

- Calls to PSAPs via 9-1-1 are also extremely important and the FCC makes clear that 9-1-1 calls should never be blocked unless the voice service provider knows without a doubt that the calls are unlawful
- Though some unwanted and illegal calls may reach 9-1-1 call centers

"The FCC Believes that 9-1-1 call centers themselves are best equipped to determine how to handle the calls they receive."

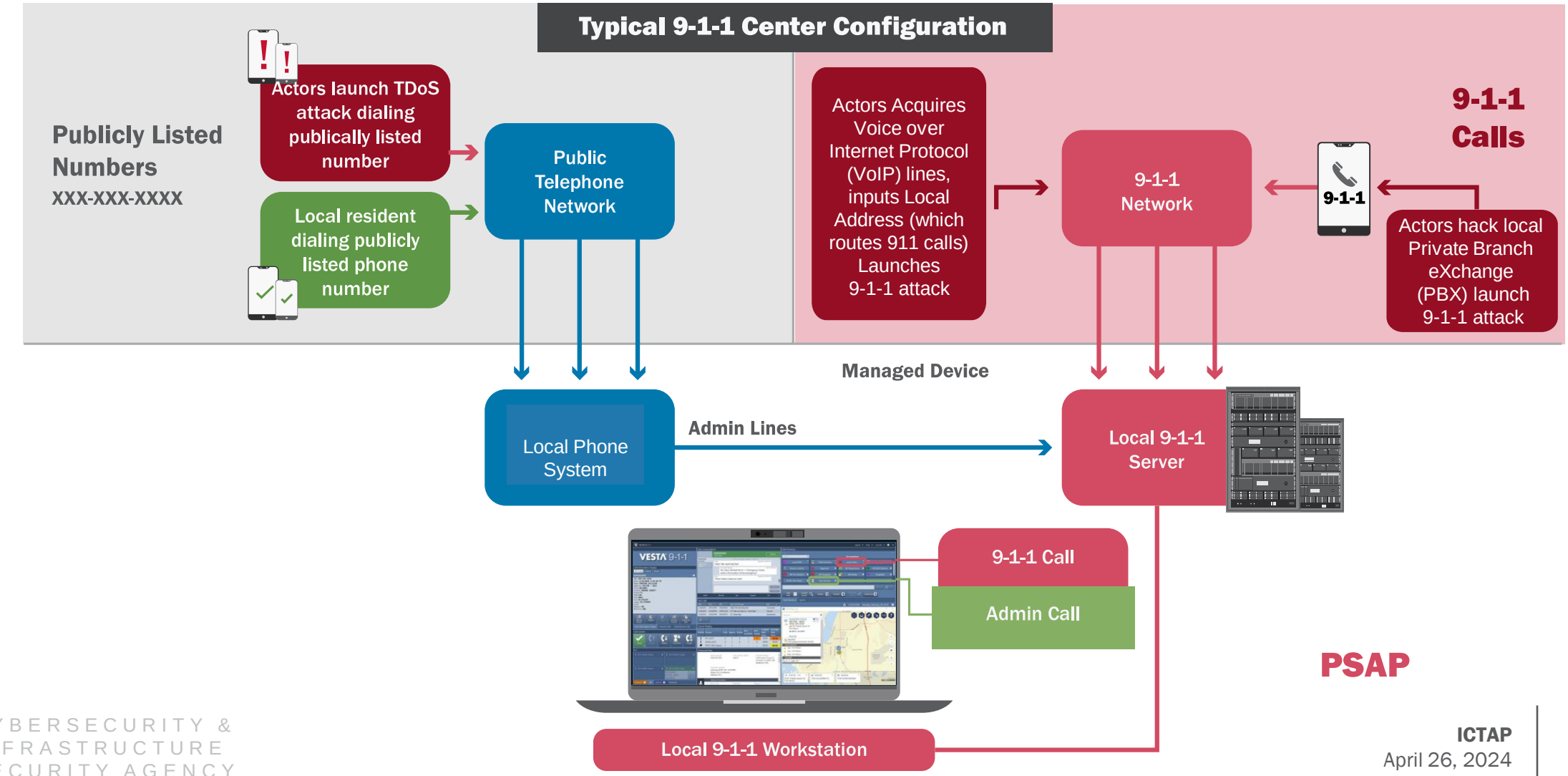
9-1-1 During a TDoS Attack

Routing to specific workstations

- Based on information in call details
- Establish separate group of workstations
- If you have a relationship with the carrier, they may be able to help with routing changes at their level

Employing an IVR

TDoS- Joint Attack on Admin and 9-1-1



Other Telephony Attacks Against 911

SWATTING

- Reported incidents prompt a significant law enforcement response
- Presents significant risk to person “SWATTED” as well as the responders
- May be used to distract police while another crime is being perpetrated
- Fake Active School Shooter SWATTING
  - NPR Report found between October 13th – October 21st , 2022
  - 182 Schools
  - 28 States

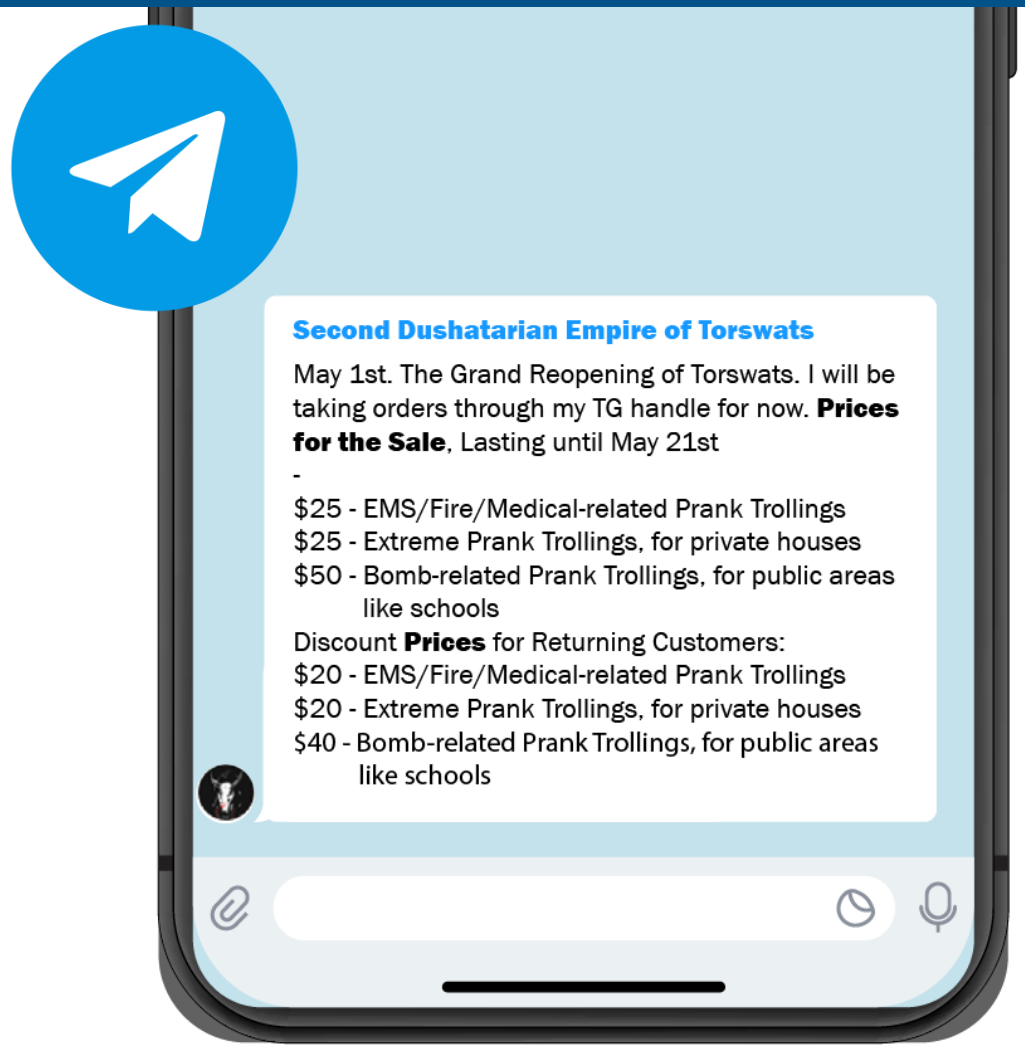
Fake Active Shooter SWATTING

- SWATTING as a Service Available on Platforms Such as Telegram
- Individual or Group is Paying for SWAT Services

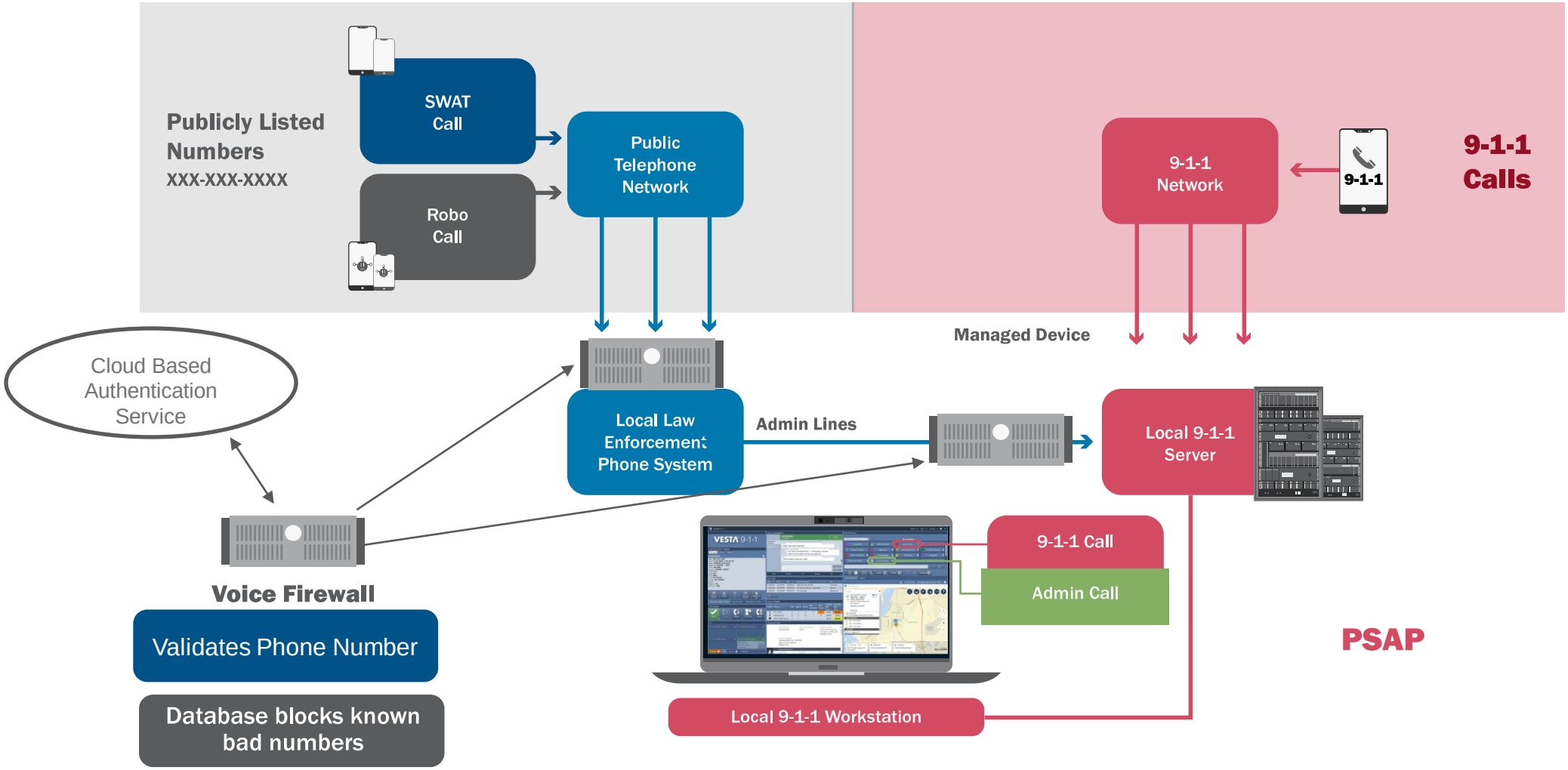
February 22nd
23 Schools Colorado
March 21st
30 Schools Iowa
March 28th
28 Schools Massachusetts

April 3rd
13 Schools Wyoming
April 4-9th
10 Universities
April 13th
20 Schools Illinois

Fake Active Shooter SWATTING



Identifying Spoofed SWAT Calls



Phishing
E-mail
Social Media

What Is Social Engineering?

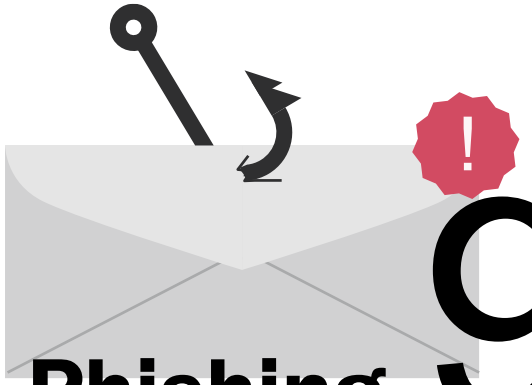
- The term is used for a broad range of malicious activities accomplished through human interactions
- It uses psychological manipulation to trick users into making security mistakes that they would not normally do or giving away sensitive information

How do they get people to "bite"?

- Urgency/Time Sensitive: Urgent requirement
- Scarcity: You will lose out on something if you do not act quickly
- Personal Health or Importance: Update on virus in your agency or community

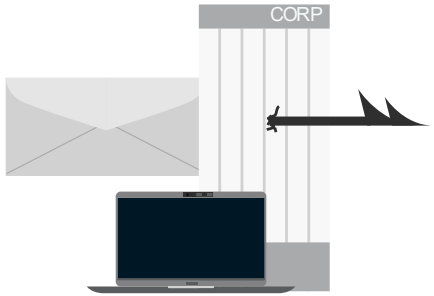
What Is Phishing?

"Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as trustworthy entity in an electronic communication."



Phishing accounts for 90% of successful cyberattacks

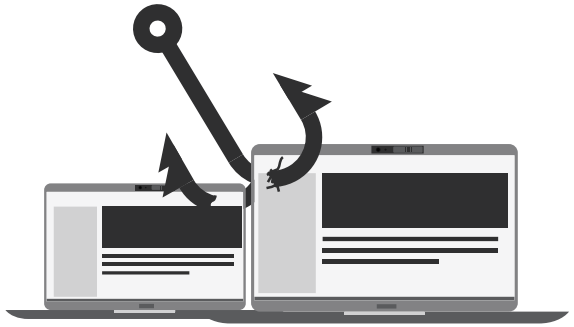
Phishing



Spear Phishing

Phishing messages crafted specifically for an individual target or group

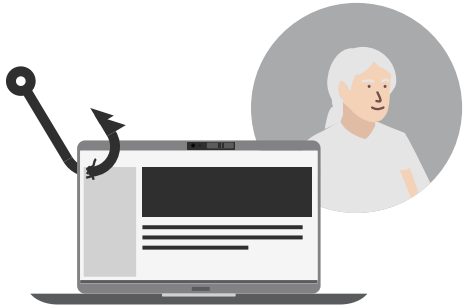
A phishing attempt directed at a particular individual or company



Clone Phishing

Legitimate, previously delivered online correspondence used to create a clone e-mail

Where a legitimate and previously delivered, bit of online correspondence is used to create an almost identical or "clone" e-mail



Whaling

Spear-phishing targeted at high-level, high-value employees

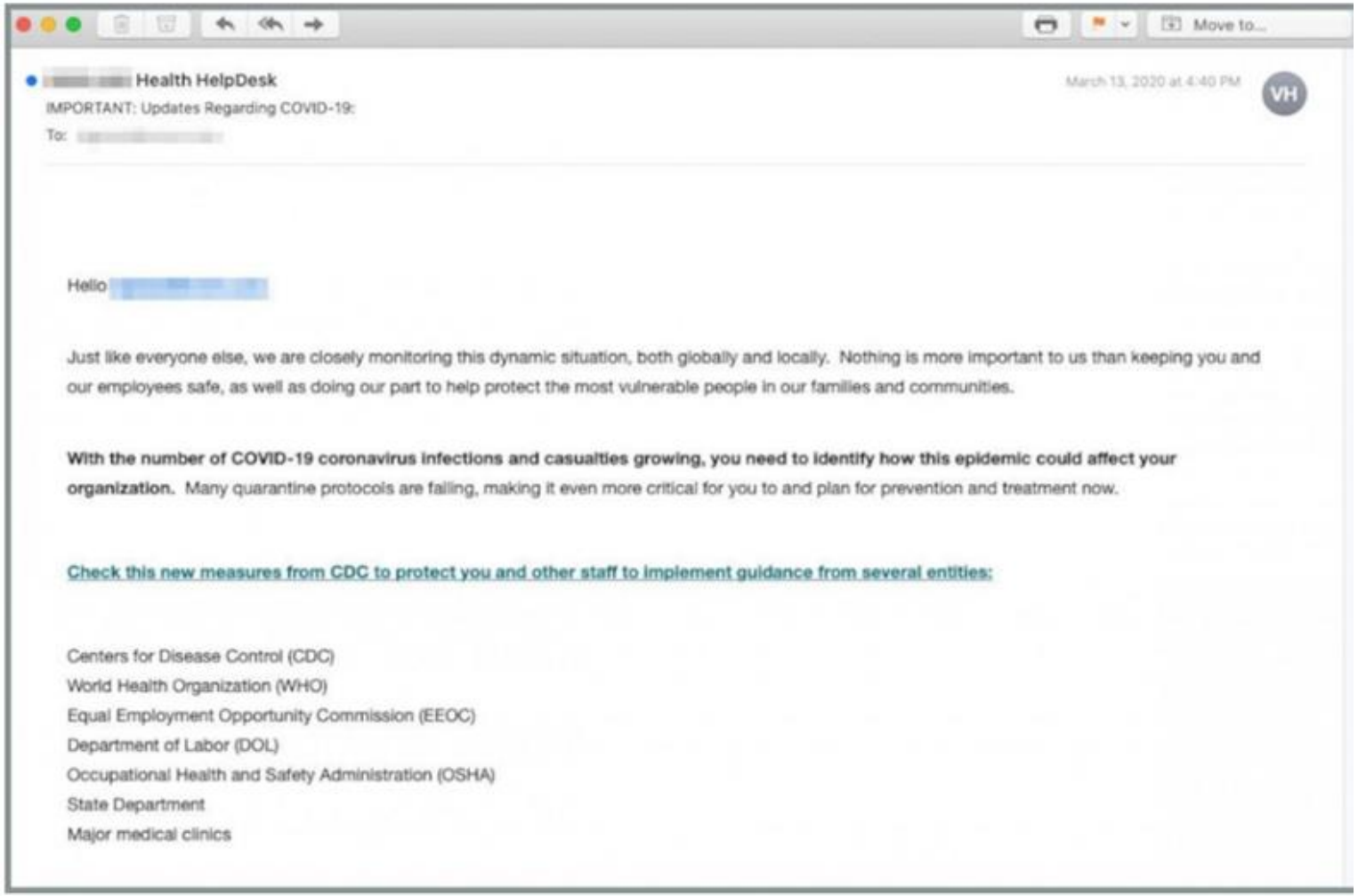
A phishing attempt directed specifically at a senior-level employee

Current Events Encourage Action

- Criminals are using world or seasonal events as phishing lures, for example using holiday shopping deals during the holiday season or tax themes during tax seasons
- Other current events such as public health crises or political issues to encourage action

Spoofed E-mail Example

Could include that the Coronavirus has "officially become airborne" and there "have been confirmed cases of the disease in your location."

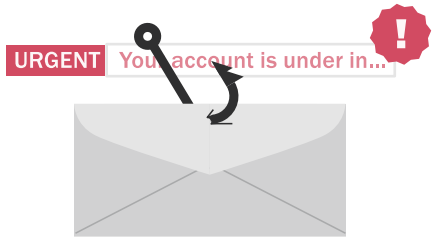


Cybersecurity experts have identified a significant uptick in coronavirus-related phishing scams.
Courtesy of INKY

How Spear Phishing Typically Works

Spear phishing messages appear to be sent from an identity – an individual or brand – this is known and trusted by the recipient

Hacker identifies a target and researches the victim



Hacker sends a targeted, legitimate looking e-mail

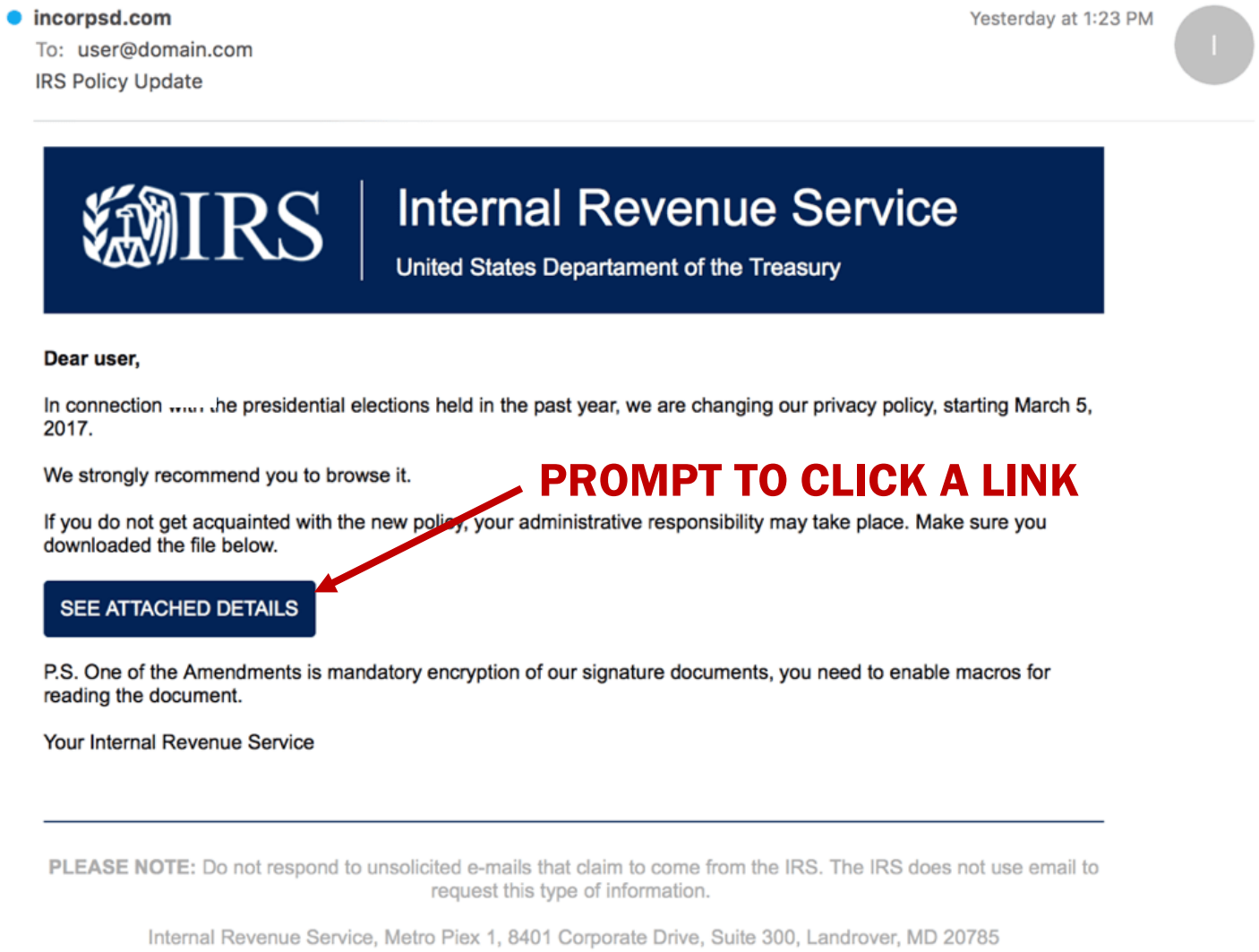
Victim opens an e-mail containing malware

Hacker uses access to steal data from victim's computer or network

Phishing Examples

Uncommon Situations or Requests	John Smith, CEO is asking you to update your health benefits as soon as possible, Click Here to update.
False E-mail Addresses	john.smith@fairfax-va.com Itmanager@cityofbaltimore.com
Fake URLs & Hyperlinks	http://cityofbaltimore911.com/login/unlock.html Click Here
"Urgent Problem" Messages	Your password has expired and must be reset immediately. Click Here to reset your login
Illegal Activity Scares	Warning: your account has been suspended for policy violation-xxxadult sites. Contact your IT manager for more information
Unclaimed Prizes	Congratulations! You have been selected to receive a $50 Amazon gift card. Click Here to claim your valued customer reward

Phishing Sample E-mail



incorpsd.com

Yesterday at 1:23 PM

To: user@domain.com

IRS Policy Update

IRS | Internal Revenue Service

United States Departament of the Treasury

Dear user,

In connection with the presidential elections held in the past year, we are changing our privacy policy, starting March 5, 2017.

We strongly recommend you to browse it.

PROMPT TO CLICK A LINK

If you do not get acquainted with the new policy, your administrative responsibility may take place. Make sure you downloaded the file below.

SEE ATTACHED DETAILS

P.S. One of the Amendments is mandatory encryption of our signature documents, you need to enable macros for reading the document.

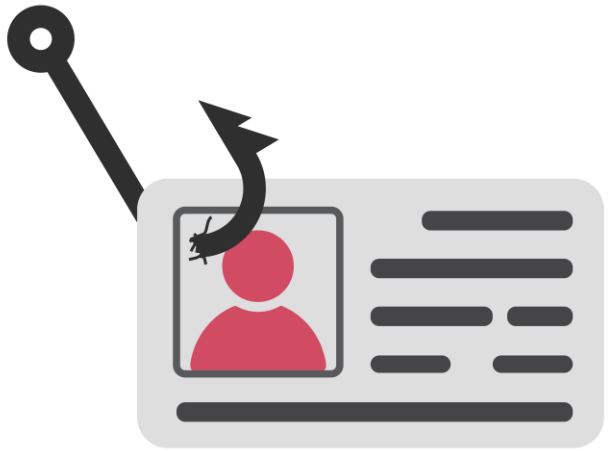
Your Internal Revenue Service

PLEASE NOTE: Do not respond to unsolicited e-mails that claim to come from the IRS. The IRS does not use email to request this type of information.

Internal Revenue Service, Metro Piex 1, 8401 Corporate Drive, Suite 300, Landrover, MD 20785

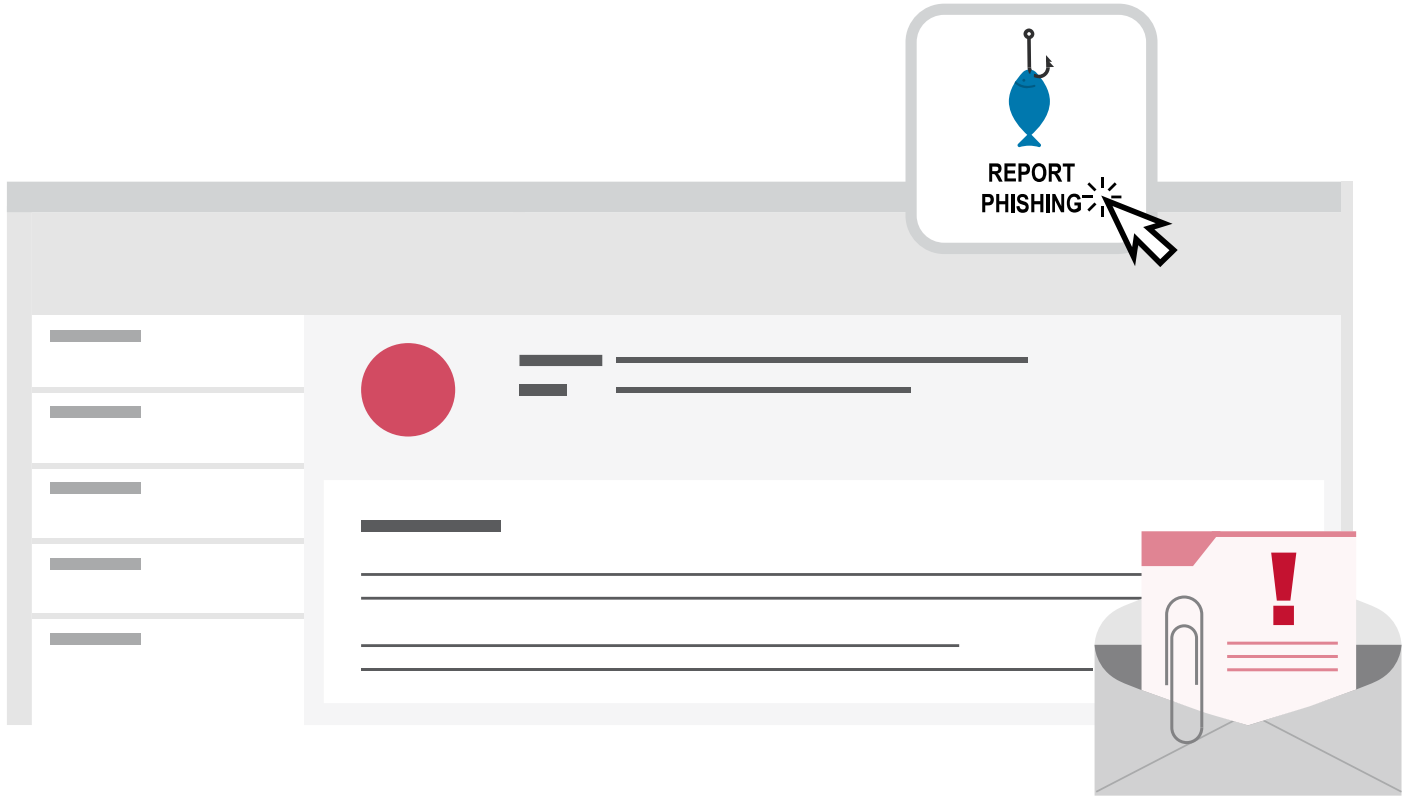
Credential Theft

- 75% of phishing attacks are aimed at obtaining the user's credentials
- Link directs user to what appears to be a legitimate Microsoft Outlook sign-on screen, so user enters credentials
- Credentials are harvested and then user is routed to the correct site



Fake/Infected Attachments

Instead of a link, they use a document attachment that might be a PDF, Microsoft Word, or other common file type



Best Practices - Phishing

- Implement a cybersecurity user awareness and training program
- Include guidance on how to identify and report suspicious activity (e.g., phishing) or incidents
- Conduct organization-wide phishing tests to gauge user awareness
- Reinforce the importance of identifying and reporting on potentially malicious e-mails
- Reminders to staff that clicking on *Links* may be dangerous

Personal Email Use – Same Concerns

Phishing is the major concern

Social Media & Personal E-mail Access

Do Not Allow on the PSAP Network:

- Social Media
- Personal Web-Based E-mail

Best Practices

- Phishing best practices…
- Report suspicious activities on their machines like software installs they don’t recognize, machine running slower than usual, knowing who to report those observations to

Indirect or Outside Attack Not on the 9-1-1 System

Ransomware

Lateral Attacks

Cryptojacking

USB Drives

Ransomware

Ransom: Money demanded for releasing captive

+

Ware: reference to software and/or files

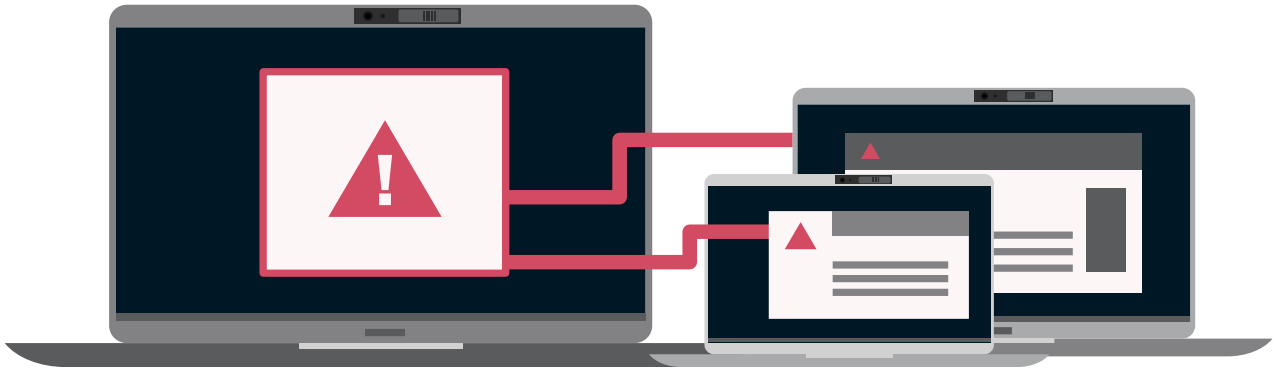
- A form of malware designed to encrypt files rendering the files and systems unusable
- Incidents have become increasingly prevalent among government entities and critical infrastructure
- Once encrypted, no security software or outside experts can restore the files

Examples of Ransomware Impact

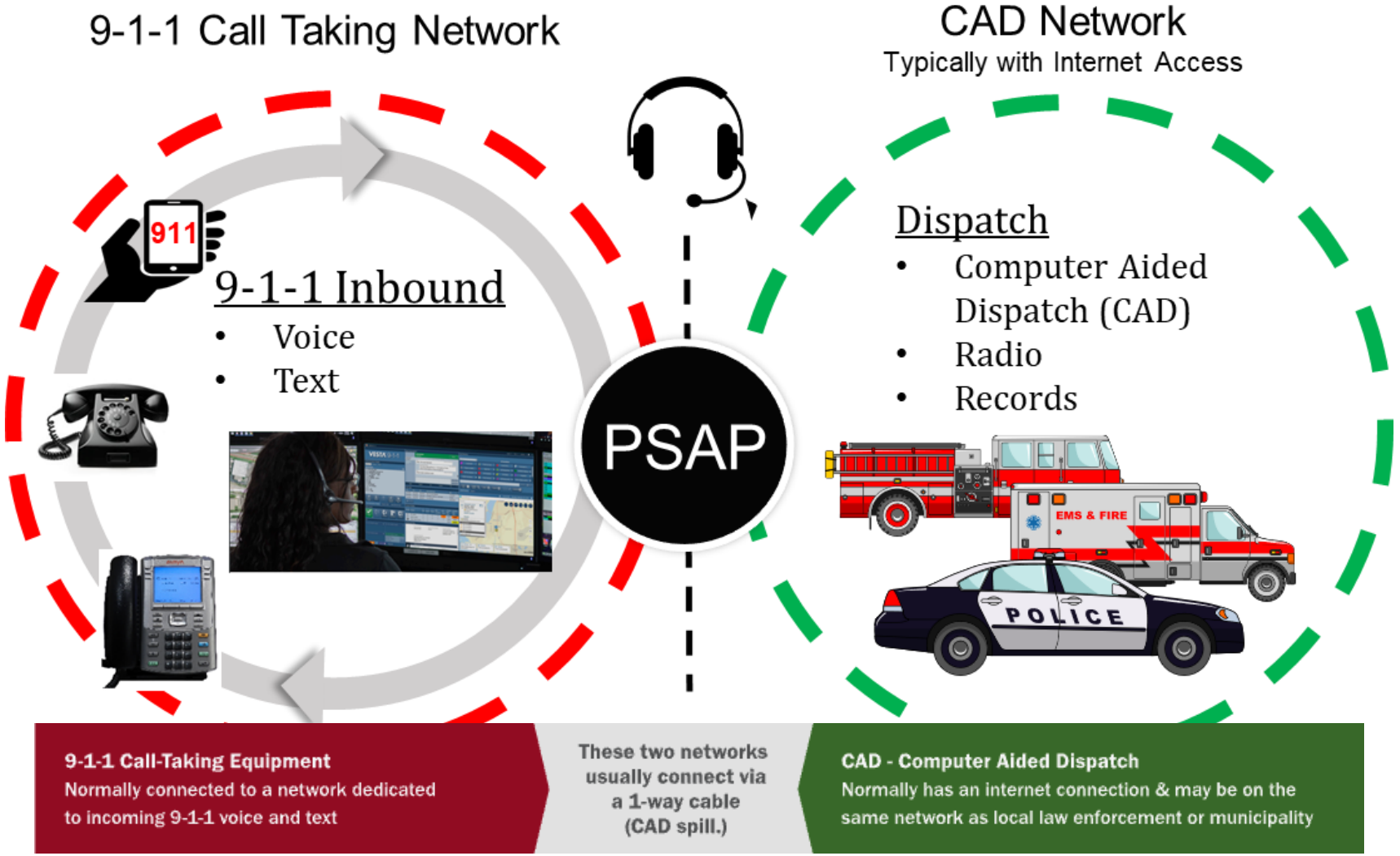
- Dallas County paid ransom of $8.5 million and received the key to decrypt files
- Attack compromised data of over 30,000 individuals
- Dallas Police Department, 311 Customer Service, Dallas City Courts, Dallas Water Utilities, Code Compliance Services, Dallas Animal Services, and the City Secretary's Office and Development Services were all affected.

Lateral Attacks

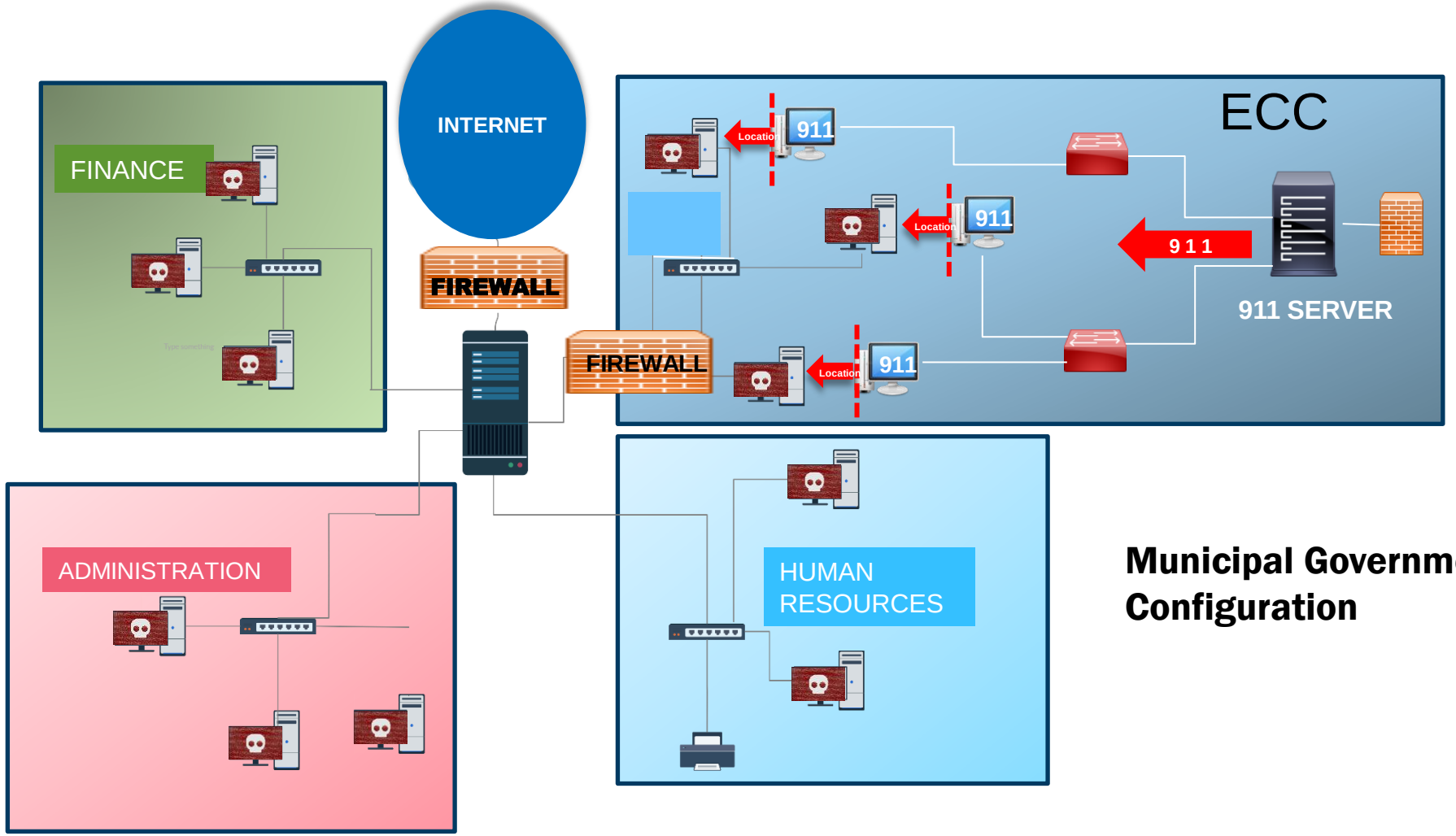
- Once hackers are in, they will try to propagate the attack to the greatest number of connected systems that they can
- In the case of the Lateral Attack, the PSAP is an unintended target
- The cyberattack is on a different municipal department, but makes its way into all governmental systems, including the PSAP



PSAP – Dual Networks



Lateral Ransomware Attack Scenario



Municipal Government Configuration

What are your options?

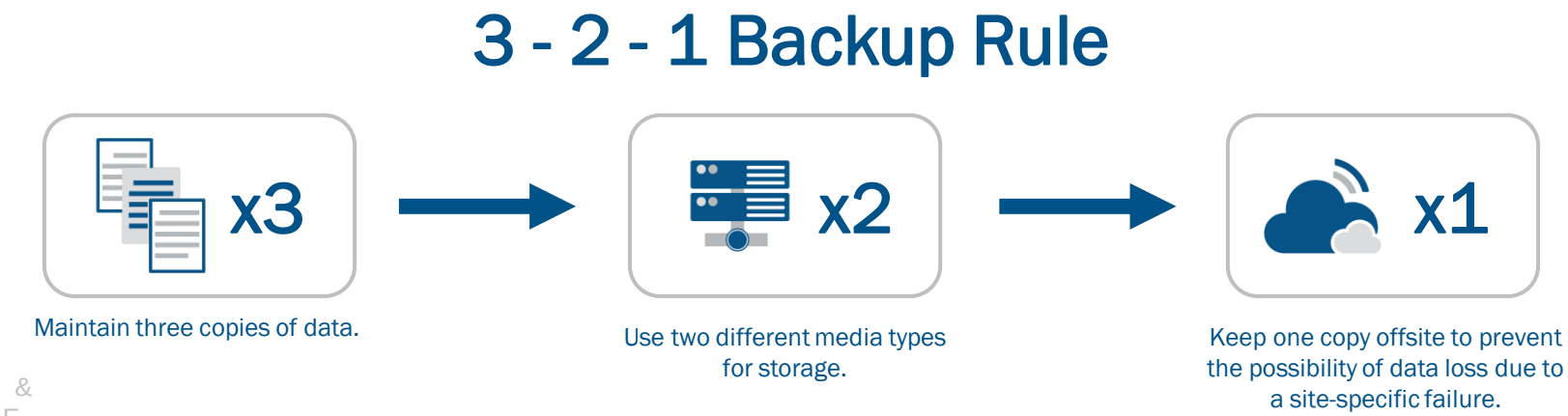
If you do not have a Continuity of Operations Plan (COOP), your only option may be to pay the ransom…

If You Pay the Ransom…

Payment **does not guarantee** the attacker will provide the encryption key

Best Practice – Current/Clean Backups

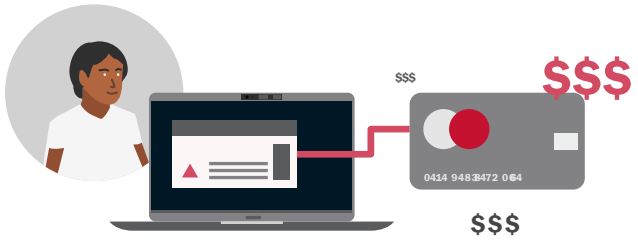
- Maintain them offline – having current backups is critical
- Replication of data is not the same as a backup
- No need to pay a ransom for data that is readily accessible to your organization
- Regularly scheduled
- Restoration Plan/Procedures in Place – Include your vendors



Cryptojacking

- Mining crypto currency using your systems
- Goal is to stay undetected to maintain an ongoing revenue stream for the attacker

Cryptojacking is the Third Wave



1st Wave

Hack into computer system, steal data and then sell it for profit (example credit card information)

2nd Wave

Hack into computer system, lock it down with ransomware and demand payment in bitcoin

3rd Wave

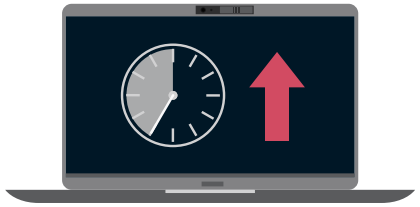
Hack into computer system and use the computing power, electricity and network access that someone else pays for to 'mine' cryptocurrencies for profit.

How Do They Get Into Your PSAP?

Most CAD systems have a web browser and internet connection on the workstation

- **Phishing Attack:** Click on an attachment – File-based based cryptojacking malware works just like regular malware. It loads directly onto a computer and runs quietly in the background
- **Poorly Protected Remote Access Points:**
- **Browser-based Attack:** Code is injected on websites or delivered with ads
- **Insider:** Cases where an employee intentionally loads the cryptojacking malware on their employer's system

Detecting Cryptojacking



Slow performing CAD computers

Spike in electricity bill

Review outbound internet traffic

This happened to a PSAP in the Mid-Atlantic States.

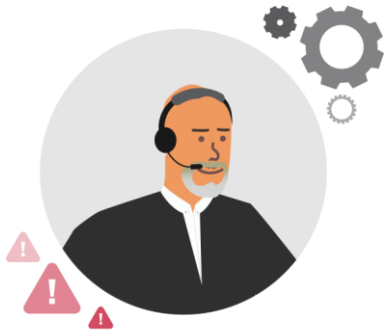
Remote Access
Remote Access in General
Working with Vendors

Remote Access

- Even the most secure systems are made vulnerable when remote access is enabled
- Hackers are constantly trolling for systems with open access to attack

Any ‘Closed Network’ is made vulnerable by remote access

Working With Our Vendors - Risks



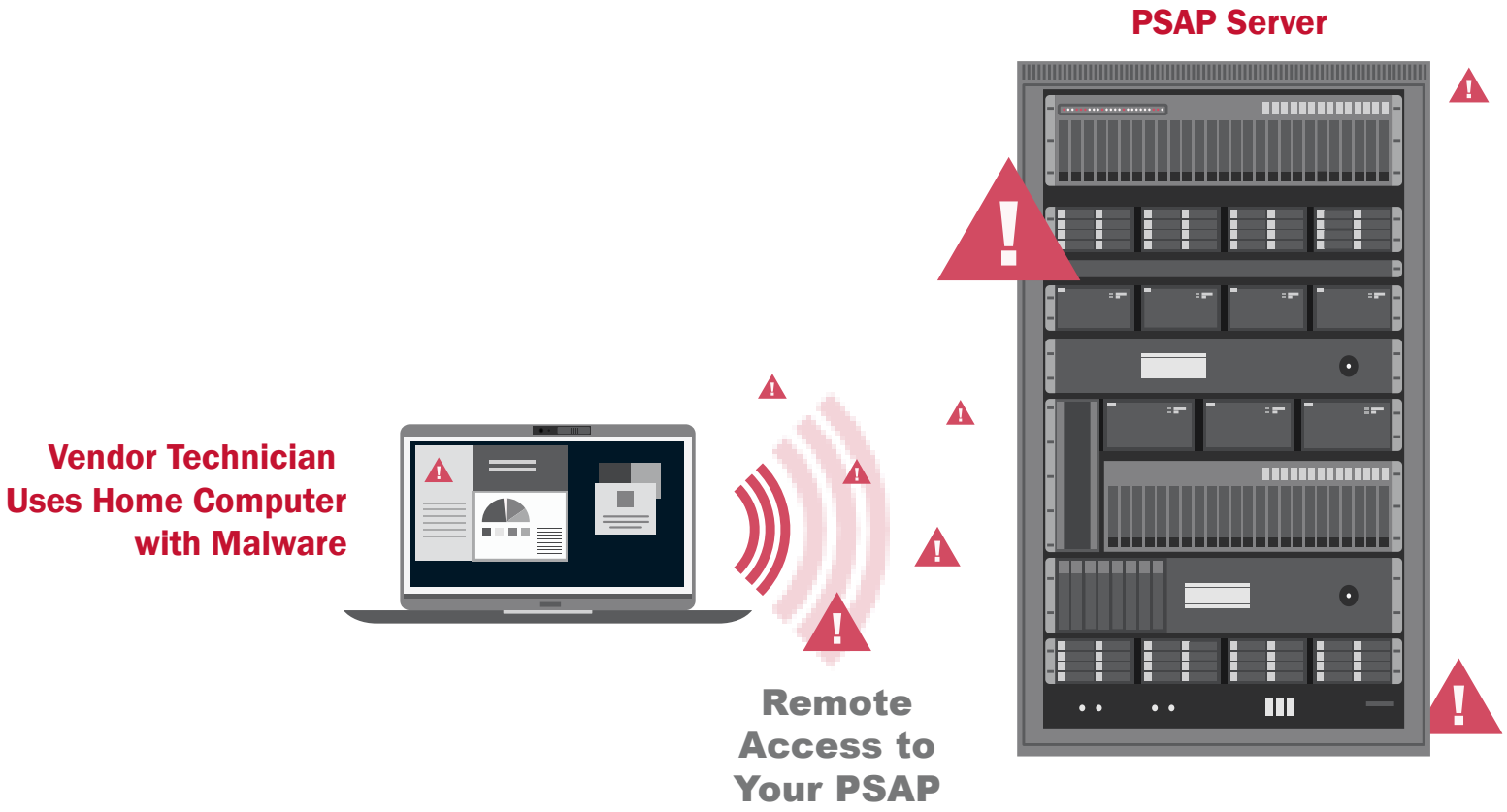
Vendors provide valuable support, but also carry certain risks

Take into consideration the risk management and cyber hygiene practices of third parties your organization relies on to meet its mission

Vendors have been an infection point for ransomware

Your Vendors and Remote Access

- Can technicians remote into your system with their home computer?
- Does the vendor have policies for the use of USB drives?
- Does each technician have a unique username and password?



Best Practices – Your Vendor and Remote Access

- Vendors typically have remote access to your call handling system
- Request an audit of who has access to your system
- Insist that each person supporting your system has a unique login
- Ask your vendor how they handle accounts after an employee event (e.g., termination, resignation, promotion, etc.)
- Keep remote access disabled and only open it up for the period of time when your vendor/support needs to use it

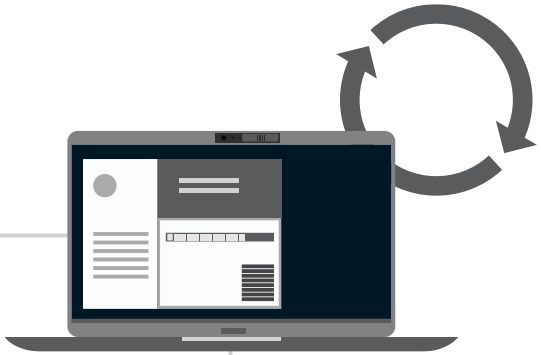
SECTION V
CYBER HYGIENE & BEST PRACTICES

What is Cyber Hygiene

- Practices and steps computer and device users can follow to maintain network health and online security
- Routines for computer and device use that improves the safety of personally identifiable information (PII) and other data that could be stolen or corrupted

Best Practice – Software Updates

- We trust our vendors to keep our systems updated with the latest security patches…
- It is important to understand their policy for reviewing security alerts and installing updates
- Sooner rather than later!



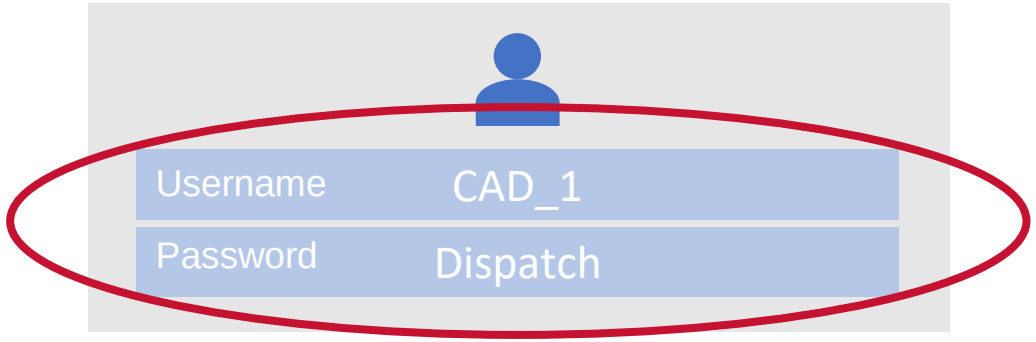
Regularly update software as prompted, and/or update to current & better versions of software

Why Update?

- Patched security holes
- Improved functionality
- Bug Fixes

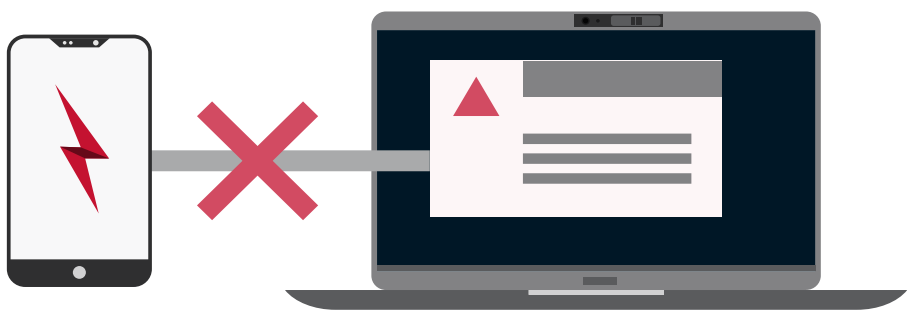
Best Practice – Individual Logons For All Users

- In numerous PSAPs across the country, all Telecommunicators use a single username and password for the 9-1-1 systems
- This provides no logging or auditing capability
- Your vendors may be using similar practice



Best Practice – Disable USB Ports

- Disable USB Ports on PSAP Computers
- Access only available when an administrative password is entered
- It is recommended that personal smartphones not be allowed to be charged via a USB attached to any computer on the center's network



Best Practice – Passwords

- Use complex passwords that contain upper and lowercase, numbers and symbols
- Regularly change passwords and **NEVER** post passwords where they are visible to other personnel visitors, or could accidentally be seen in social media posts, etc.
- Never send passwords over the internet, do not use the same password across logins and accounts
- Strong Passwords
  - Password Length: 8-16+ characters
  - Includes Symbols: @#$%^!
  - Includes Numbers: 123456…
  - Includes Lowercase: abcdefg…
  - Includes Uppercase: ABCDEFG…

Best Practice – Multi Factor Authentication (MFA)

- MFA is a layered approach to securing online accounts and the data they contain using a combination or two or more authenticators to verify a user's identity before the service grants access
- Security works best when deployed in layers, MFA is just another layer to a good password policy

Why This Area Is So Important?

- Username and passwords are an important way to keep the hackers out of your network
- Over 90% of successful attacks result from employee actions like clicking on an infected item/link
- People are not as good at identifying a potential attack as they think they are

Credentials – Outsiders

Multi-Factor Authentication should go beyond our own people

Mutual Aid:

If we bring in personnel from other PSAPs and public safety entities through mutual aid, what are our SOPs for credentialing these end-users and what permissions do they have on our systems?

Vendors:

If we have vendors accessing our systems and secure physical areas for maintenance or incident response, what are our standard operating procedures (SOPs) for credentialing and verifying these end-users or technicians?

SECTION VI
RESPONDING TO AND REPORTING CYBER INCIDENTS

It Is Almost Inevitable…

- It is no longer a question of if your systems will be successfully attacked, it is just a question of when…
- Must have some plans in place to minimize the impact

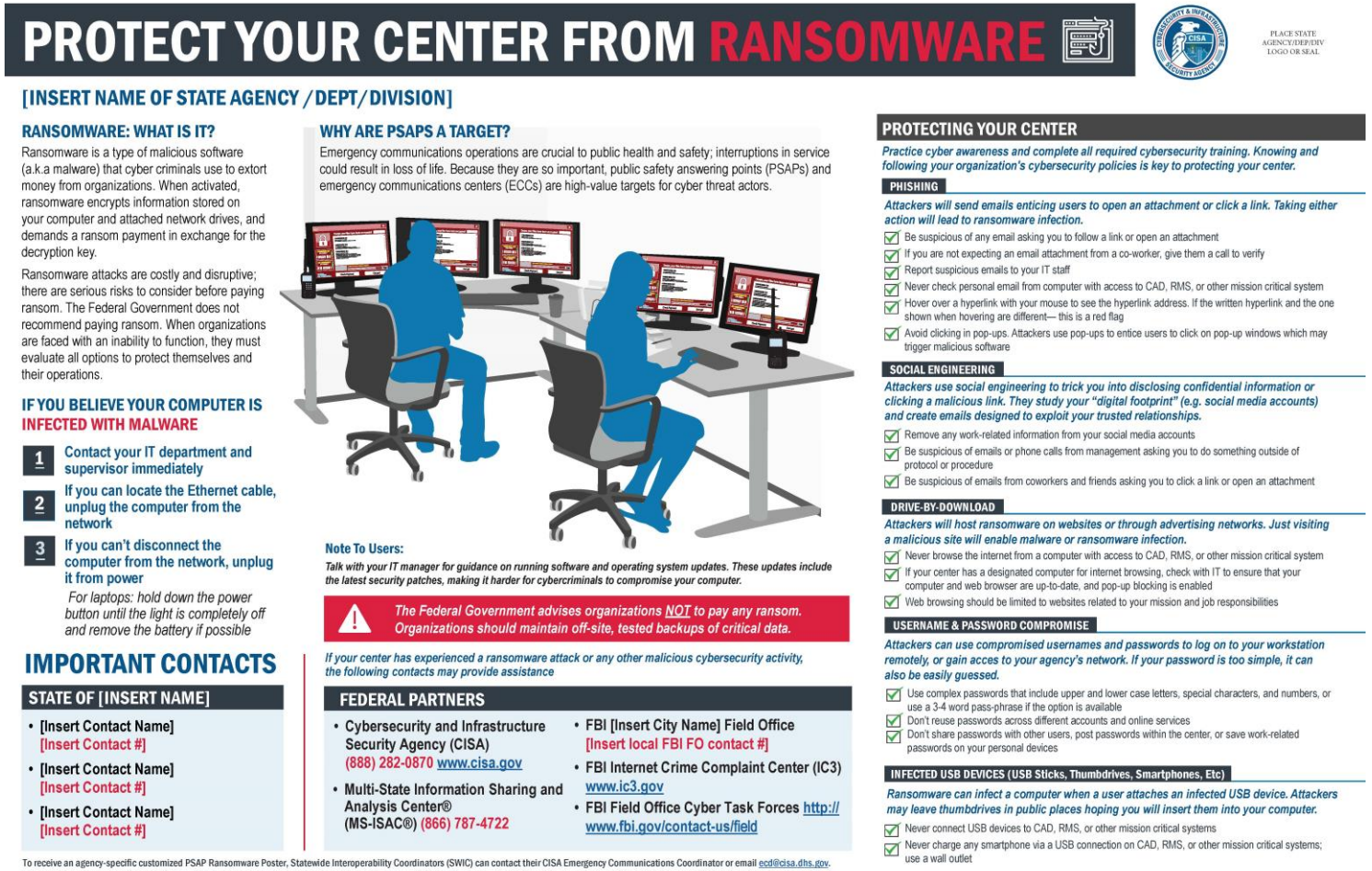
CAD Is Down – What Can We Do?

- Need to be able to continue to operate, dispatch units, document activities, etc.
- Establish an Essential Records Program
  - Records necessary to the continuing essential functions and resumption of normal operations
  - Run Cards/Unit Recommendations
  - Documentation of critical information items
- Incorporate Essential Records Program into overall continuity plans

www.dhs.gov/emergency-services-sector-continuity-planning-suite

Building Awareness

- CISA Customized Poster Program
- Word-of-mouth/ reminders



PROTECT YOUR CENTER FROM RANSOMWARE

PLACE STATE AGENCY/DEPT/DIV LOGO OR SEAL

[INSERT NAME OF STATE AGENCY / DEPT / DIVISION]

RANSOMWARE: WHAT IS IT?

Ransomware is a type of malicious software (a.k.a malware) that cyber criminals use to extort money from organizations. When activated, ransomware encrypts information stored on your computer and attached network drives, and demands a ransom payment in exchange for the decryption key.

Ransomware attacks are costly and disruptive; there are serious risks to consider before paying ransom. The Federal Government does not recommend paying ransom. When organizations are faced with an inability to function, they must evaluate all options to protect themselves and their operations.

IF YOU BELIEVE YOUR COMPUTER IS INFECTED WITH MALWARE

1. Contact your IT department and supervisor immediately
2. If you can locate the Ethernet cable, unplug the computer from the network
3. If you can't disconnect the computer from the network, unplug it from power

For laptops: hold down the power button until the light is completely off and remove the battery if possible

WHY ARE PSAPS A TARGET?

Emergency communications operations are crucial to public health and safety; interruptions in service could result in loss of life. Because they are so important, public safety answering points (PSAPs) and emergency communications centers (ECCs) are high-value targets for cyber threat actors.

Note To Users:

Talk with your IT manager for guidance on running software and operating system updates. These updates include the latest security patches, making it harder for cybercriminals to compromise your computer.

The Federal Government advises organizations NOT to pay any ransom. Organizations should maintain off-site, tested backups of critical data.

IMPORTANT CONTACTS

If your center has experienced a ransomware attack or any other malicious cybersecurity activity, the following contacts may provide assistance

STATE OF [INSERT NAME]

- [Insert Contact Name] [Insert Contact #]
- [Insert Contact Name] [Insert Contact #]
- [Insert Contact Name] [Insert Contact #]

FEDERAL PARTNERS

- Cybersecurity and Infrastructure Security Agency (CISA) (888) 282-0870 www.cisa.gov
- Multi-State Information Sharing and Analysis Center® (MS-ISAC®) (866) 787-4722
- FBI [Insert City Name] Field Office [Insert local FBI FO contact #]
- FBI Internet Crime Complaint Center (IC3) www.ic3.gov
- FBI Field Office Cyber Task Forces http://www.fbi.gov/contact-us/field

To receive an agency-specific customized PSAP Ransomware Poster, Statewide Interoperability Coordinators (SWIC) can contact their CISA Emergency Communications Coordinator or email ecd@cisa.dhs.gov.

PROTECTING YOUR CENTER

Practice cyber awareness and complete all required cybersecurity training. Knowing and following your organization's cybersecurity policies is key to protecting your center.

PHISHING

Attackers will send emails enticing users to open an attachment or click a link. Taking either action will lead to ransomware infection.

- ☑ Be suspicious of any email asking you to follow a link or open an attachment
- ☑ If you are not expecting an email attachment from a co-worker, give them a call to verify
- ☑ Report suspicious emails to your IT staff
- ☑ Never check personal email from computer with access to CAD, RMS, or other mission critical system
- ☑ Hover over a hyperlink with your mouse to see the hyperlink address. If the written hyperlink and the one shown when hovering are different— this is a red flag
- ☑ Avoid clicking in pop-ups. Attackers use pop-ups to entice users to click on pop-up windows which may trigger malicious software

SOCIAL ENGINEERING

Attackers use social engineering to trick you into disclosing confidential information or clicking a malicious link. They study your "digital footprint" (e.g. social media accounts) and create emails designed to exploit your trusted relationships.

- ☑ Remove any work-related information from your social media accounts
- ☑ Be suspicious of emails or phone calls from management asking you to do something outside of protocol or procedure
- ☑ Be suspicious of emails from coworkers and friends asking you to click a link or open an attachment

DRIVE-BY-DOWNLOAD

Attackers will host ransomware on websites or through advertising networks. Just visiting a malicious site will enable malware or ransomware infection.

- ☑ Never browse the internet from a computer with access to CAD, RMS, or other mission critical system
- ☑ If your center has a designated computer for internet browsing, check with IT to ensure that your computer and web browser are up-to-date, and pop-up blocking is enabled
- ☑ Web browsing should be limited to websites related to your mission and job responsibilities

USERNAME & PASSWORD COMPROMISE

Attackers can use compromised usernames and passwords to log on to your workstation remotely, or gain acces to your agency's network. If your password is too simple, it can also be easily guessed.

- ☑ Use complex passwords that include upper and lower case letters, special characters, and numbers, or use a 3-4 word pass-phrase if the option is available
- ☑ Don't reuse passwords across different accounts and online services
- ☑ Don't share passwords with other users, post passwords within the center, or save work-related passwords on your personal devices

INFECTED USB DEVICES (USB Sticks, Thumbdrives, Smartphones, Etc)

Ransomware can infect a computer when a user attaches an infected USB device. Attackers may leave thumbdrives in public places hoping you will insert them into your computer.

- ☑ Never connect USB devices to CAD, RMS, or other mission critical systems
- ☑ Never charge any smartphone via a USB connection on CAD, RMS, or other mission critical systems; use a wall outlet

Cyber Incident Response Plan

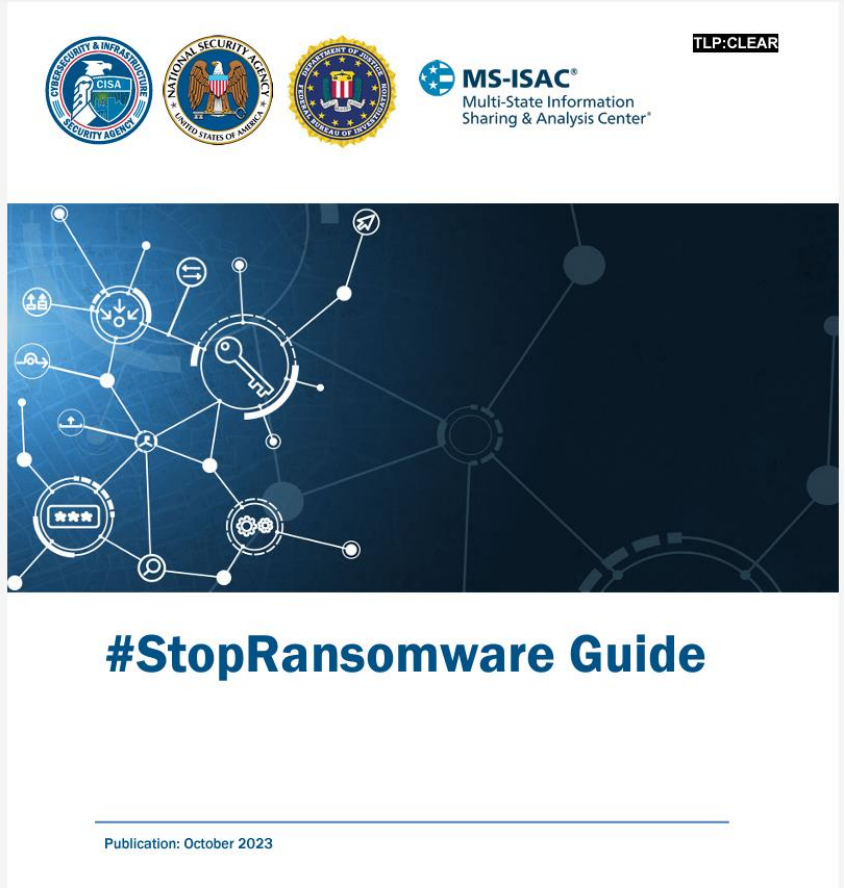
Contact Information

Consider filling out the following contact information for ready use should your organization become a victim of a ransomware incident. Consider contacting these organizations for mitigation and response assistance or for purpose of notification.

State and Local Response Contacts:		
Contact	**24x7 Contact Information**	**Roles and Responsibilities**
IT/IT Security Team - Centralized Cyber Incident Reporting		
Departmental or Elected Leaders		
State and Local Law Enforcement		
Fusion Center		
Managed/Security Service Providers		
Cyber Insurance		

Ransomware Quick References

- **Ransomware – Guidance & Resources (CISA)**
  www.cisa.gov/ransomware
- **Resources for State, Local and Tribal Governments (CISA)**
  - Case Studies
  - Toolkits
  - https://www.cisa.gov/audiences/state-local-tribal-and-territorial-government



Basic Response Planning Includes

1. Emergency contact list
2. Immediate actions to take
3. Notifications that need to be made
4. Develop an essential procedures and documents package so you can continue to function
5. Verify the existence and cleanliness of offline backups
6. Restoration procedures and resources
7. Forensic analysis/after-action report

Government Resources

- **CISA Provides**
  - Risk Assessments – Next slide
  - Cyber Exercises – To evaluate or help develop your cyber incident response plan
  - Cybersecurity Advisors (CSAs) – Advise on best practices and connect you to resources to manage cyber risk
- **DHS/ECD Resources**
  - Various resources are available in the areas of technology, sustainment, resilience, etc. are available
- **See Supplemental Handout for list on hotlinks**

SECTION VII
SUMMARY

The Bottom Line… (1 of 5)

- **PSAPs/ECCs Are Direct/Indirect Targets**
- **Attacks**
  - Are inevitable and will cause disruption
  - Some attacks hit behind the firewall
  - Admin/records and/or 9-1-1
  - Workarounds may help
- **TDoS Is A Real Threat**
  - Appliances may help
  - FCC will not block them

The Bottom Line… (2 of 5)

- **Ransomware Can Cause Weeks of Downtime**
  - Segmented Local Area Networks (LANs) will limit disruption
  - Offline/clean/current backups are critical
  - Have an Essential Records Program to allow continuity of operations during downtime (pen and paper/forms)
- **Employee Actions**
  - Disable USB ports/admin password access only
  - No social media or web-based personal e-mail

The Bottom Line… (3 of 5)

- **Vendors**
  - Critical, but there are risks with remote access
  - Require unique usernames/passwords for all users
  - Request policies and review them
  - Verify that the backups they generate will be “clean“
- **Phishing Is The Biggest Threat**
  - The key is employee education & training on a regular basis
  - Post-pandemic rise in remote work increases vulnerability

The Bottom Line… (4 of 5)

- **Phishing (continued)**
  - Social Engineering is how they get people to “bite”
  - Practice what you preach
  - Senior management is often the most vulnerable
- **Other Best Practices**
  - Individual logons for everyone
  - Install all software updates on a timely basis
  - Protect or limit access to physical assets, especially those outside of the dispatch center

The Bottom Line… (5 of 5)

- **Responding To/Reporting Cyber Incidents**
  - It's not "if", it's a question of "when"
  - Need to be prepared
  - Develop and exercise a plan
  - Must have clean/offline backups to restore
  - Involve your vendors
  - See links for Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS) for important contacts
  - Document actions for reference and/or insurance purposes

Closing Comments

- The focus of this program was awareness
- Hopefully, it expanded your understanding of cybersecurity threats that are faced by PSAPs and ECCs daily
- It is important that you have some type of plan to address the inevitability of your system(s) going down at some point
- We hope that you found this program interesting and worthwhile

Thank you for your time and attention!

QUESTIONS?


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY