PROTECT YOUR CENTER FROM RANSOMWARE

PLACE STATE AGENCY/DEP/DIV LOGO OR SEAL

[INSERT NAME OF STATE AGENCY /DEPT/DIVISION]

****PRELIMINARY DRAFT - DO NOT DISTRIBUTE Work Product Only*****

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