Cyber Best Practices for State of Illinois Telework

It is especially important during this time that employees adhere to information security best practices and remain focused on cyber hygiene efforts. Please read the instructions and recommendations below.

1. **Only visit reputable websites.**
   - Think about what you are clicking when on the internet. In any time of disaster or large-scale events, malicious actors focus their efforts on the fears and anxiety of the general public. Be skeptical. Think before you click.

2. **Use trusted and secured wireless connections**. Free public Wi-Fi connections are often targeted by cyber-criminals looking for victims.

3. **Secure your Wi-Fi network at home**. Your home's wireless router is the primary entrance for cybercriminals to access your connected devices, and you can better secure your Wi-Fi network and devices by changing the factory-set default password and username for each one.

4. **System and Software Updates and Patching**
   - Ensure the automatic system update feature for your specific Operating System is turned on. For Windows users, go to the Start button, then Settings->Update & Security-> Windows Update, and select "Automatic Updates".
   - Enable other application software, such as browsers and Office software to automatically update.
   - What is this and why is it important?
     - Patching is like repairing holes in your umbrella. You may not see the holes, but they let things in that damage your computer and information stored on that computer. Patching and Updating plug those "holes". Think about this basic precaution like closing the doors and windows to your house. Closing doors and windows keeps unwanted things out.
     - Need help patching and updating?
       - Windows 10: https://support.microsoft.com/en-us/help/4027667/windows-10-update
       - MacOS: https://support.apple.com/en-us/HT201541
     - If you don't have Windows 10 or a Mac, please search Google on how to update your specific operating system and follow those directions.

5. **Anti-Malware**
   - Validate that you are running anti-malware/anti-virus.
   - Microsoft Defender Anti-malware is available on Windows 10 computers and tablets.
   - MAC/OSX: Useful tips to validate that anti-malware (XProtect) protection and other built-in security features are turned on: https://mashtips.com/built-in-mac-security-software/

6. **Physical and Data Protection Best Practices**
   - Never disclose confidential or sensitive data to any unauthorized personnel including friends and family.
   - Lock your computer when leaving it unattended.
   - Do not store State sensitive or confidential information on your personal computer.
   - Store any sensitive or confidential information on encrypted media provided by your agency.
   - Report security incidents or security concerns to DoIT.Security@illinois.gov.
   - Refrain from using personal email for business use.
   - Always comply with your organization's policies and procedures to protect specific high-risk data elements regulated by HIPAA, IRS, PCI, etc.

7. **Malicious actors often send out phishing e-mails** that appear to come from legitimate websites.

- Scammers are targeting consumers using phishing sites, phony websites, and even telephone-based scams. Be cautious and always validate the credibility of any phone call, website, and email to make sure it is legitimate. Report any suspicious activity to your Information Security Office.
- Be especially cautious of COVID-19 scams and malicious sites. Stick to known safe sites for COVID-19 updates such as the CDC website, the Illinois COVID-19 and IDPH websites

8. **Be suspicious of any email or text that:**
   - Requests personal information
   - Contains spelling and grammatical errors
   - Is unexpected or from a company or organization with whom you do not have a relationship

9. **If you are suspicious of an email**:
   - Do NOT click on the links provided
   - Do NOT open any attachments
   - Do NOT provide personal information or financial data

10. It is wise to be skeptical of any message, text, email, phone call or website that asks you to share personal data - especially if the request is from an unknown source.

11. **Personal Phone Protection**
    - Regularly Clean up Privacy Settings on Mobile Devices
    - For iOS: https://apps.apple.com/us/app/mypermissions-privacy-cleaner/id535720736
    - For Android: https://play.google.com/store/apps/details?id=com.mypermissions.mypermissions&hl=en_US

12. The remote work solutions deployed by the State of Illinois are designed to protect State data by keeping it separated from personal machines. Please do not save any state information or data on personal devices.

13. State issued equipment should only be used for state work. Do not share a state issued computer or data with anyone else.

14. Remember that our help desk will NEVER send emails that require you to send personal information via email, external web sites, links or pop-up windows. If in doubt, report any cybersecurity concerns regarding your SOI accounts to DoIT.Security@illinois.gov.