OFFICE of
information
technology
services

Cautiously Embracing the Future

Telework and Artificial Intelligence (AI) from a Cyber Security Mindset

ITS CISO Staff

- Brian Reed – Acting ITS CISO
- Matt Aslett – Chief Compliance Officer
- Elizabeth Knox – Policy and Programs Officer

Working Remotely

- When you work remotely, you do not have the protection of your organization's network, so it is critically important that you:
  - Make use of complex and secure passwords. Wherever possible, use multi-factor authentication.
  - Don't fall for credential phishing attacks.
  - Don't click on links; bookmark the sites you frequently visit.
  - Follow instructions from your IT department when it comes to software updates.
  - Separate work and personal data.
  - Stay committed to general security awareness.
  - Work policies still apply
  - Use VPN whenever connecting to public or guest Wi-Fi

Securing your Home Office

- When you work from home you likely rely heavily on the internet. As such, protecting your home network is paramount to security.
  - Log in to your router to access its settings. If you're unsure of how to log in, look up your router's model on the internet and you'll find plenty of how-to articles with simple instructions.
  - Change your router's username and password. Most routers ship with default login credentials that are public knowledge and must be changed immediately.
  - Change the SSID (Service Set Identifier). The SSID is the name of your wireless network. Change it to something unique and protect it with a strong password.
  - If available, enable automatic updates so your router is always on the most recent firmware or software version.
  - Use a virtual private network (VPN). A VPN is software that encrypts your internet connection and prevents others from viewing your internet traffic. Many organizations require the use of a VPN for remote workers.

Device Defense

- With your network secured, let's highlight a few ways to ensure your workspace is also secured.
  - Use strong passwords. All accounts and devices require strong, unique passwords. Don't share those passwords with anyone for any reason.
  - Lock your workstation. When not in use, always lock your workstation and ensure no one else in your household can access work-related information or accounts.
  - Beware of smart devices. Ensure voice-controlled smart devices can't listen in on any discussions that involve confidential information. Ideally, remove smart devices from your workspace.
  - Separate work and personal. Don't use work devices or accounts for personal reasons. If you have approval to work on a personal computer, protect it with antivirus software.
  - Always follow policy. No matter where you work, remember that organizational policies apply and must be followed at all times. Have questions? Please ask!

General Remote Reminders

- SHOULDER SURFERS. When remotely accessing sensitive information of any kind, be sure no one is looking over your shoulder or spying on your screen. Never forget the "Human Domain!"
- PUBLIC WIFI. Perhaps the biggest threat, public Wi-Fi invites a host of security issues. Avoid accessing or sending any sensitive information when connected to public networks unless you know how to do so securely and within our policy guidelines. DISABLE AUTO-CONNECT
- BE DISCREET. If you're in a public setting and conducting private business, make sure no one can overhear your discussions or spy on your screen.
- KEEP TRACK OF INVENTORY. When traveling, keep all devices (and anything with sensitive info) on your person or in your sight at all times. Never trust strangers to "watch your stuff."
- AVOID USING REMOVABLE STORAGE. USB flash drives and other external data storage devices are easy to lose and easy to steal. If you must use them, encrypt and password protect them.

AI, What is it?

- Artificial Intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to mimic human-like cognitive functions such as learning, problem-solving, perception, and decision-making. AI technologies enable computers and machines to perform tasks that typically require human intelligence, including understanding natural language, recognizing patterns in data, making predictions, and adapting to new situations.
- Generative AI is revolutionizing the world of work. But it can also pose a threat to cybersecurity, from fake photos, videos, or voices that sound deceptively realistic to automated generation of disinformation and machine-programmed malware and viruses.

Characteristics of Trustworthiness of AI

- Transparency: The workings, capabilities, and limitations of GAI systems will be understandable by their users and stakeholders
- Accountability: For every GAI solution, there shall be a clear line of accountability to ensure responsible decision-making
- Fairness: GAI technologies will be implemented with minimizing biases in mind, particularly in the generated content
- Privacy: The use of GAI will respect privacy rights and data protection regulations
- Safety and Robustness: GAI solutions will be developed with controls to prevent misuse, ensuring their safety and reliability

Drafting Documents or Letters

- Do's:

- Try to be specific in the prompt. If you give more context, the answer becomes more relevant.
- Edit and review the content. Regardless of how the content was authored, you and ITS will bear responsibility for its use in the public.

- Don'ts:

- Do not include confidential information in the prompt.
- Do not rely on Text GAI to provide accurate answers.
- Do not use Text GAI to create communication regarding sensitive topics. For instance, a renowned institution was criticized for using Text GAI to write a press release regarding a shooting.

Drafting Content in Plain Language

- Do's:
  - Try to be specific in the prompt. If you give more context, the answer becomes more relevant.
  - Edit and review the content. Regardless of how the content was authored, you and ITS will bear responsibility for its use in the public.

- Don'ts:
  - Do not include confidential information in the prompt.
  - Do not rely on Text GAI to provide accurate answers.
  - Do not use Text GAI to create communication regarding sensitive topics. For instance, a renowned institution was criticized for using Text GAI to write a press release regarding a shooting.

Summarizing Text

- Do's.

- Be aware that the resulting summary might have biases as it will tend to present language that is more frequent in the data used to train the model. You can use changes to the prompt to enhance the results by suggesting that the result incorporates perspectives from marginalized groups. Even better, you can engage with some individuals in these communities to better understand their perspectives on the text generated.
- If you plan on making a decision based on the summary, Read the entire document(s) to ensure you did not miss, or miss characterized the original document.

- Don'ts:

- Do not include confidential information in the prompt: make sure you have deleted confidential information from your notes or other inputs.

Questions?