**Key Takeaways from the Cybersecurity Fundamentals Training**

As a government employee, it is important that you be equipped to protect your department’s mission and the other important work of your government. Among other things, that means you must protect the government systems and information you have access to and be aware of cyber threats that may jeopardize your government’s ability to achieve your government mission. Below are Key Takeaways from the Cybersecurity Fundamentals Training which highlight important cybersecurity fundamentals.

***Cyber Threats to Government Missions***

* Cybersecurity threats to services are a *significant national security concern.*  Your job as a government employee is to protect government networks. Threat actors in cyberspace include people or organizations with the intent and motivation to compromise information systems. *Any government employee* can be a target of dangerous threat actors in cyberspace.
* Threat actors include hostile and state-sponsored actors; political and ideological actors; organized crime; insiders; and hackers.
* Common tactics used by threat actors in cyberspace include: phishing, the mis-use of hacked valid accounts, network sniffing, exploiting publicly available information found online, social engineering, and others.

***Cybersecurity Basics***

* Government employees can best fulfill their role in protecting the nation’s information security by *abiding by information security policies and practicing good cyber hygiene*.
* Good cyber hygiene includes setting secure passwords and not sharing them; avoiding reusing passwords on different systems and applications; locking your systems when you are physically away from them; using multi-factor authentication when available, and not attempting to work around enterprise and network controls.
* Protect government and personal information by using approved VPNs and encryption when available, especially when connecting to public Wi-Fi.
* Anti-virus software is a vital component of your overall cyber hygiene in its protection against security breaches, along with other threats. Beware of unlicensed anti-virus programs which may themselves introduce malware.

***Online Safety***

* Never conduct activities that involve sensitive data online while using a public or unsecured Wi-Fi network.
* Use multi-factor authentication where possible.
* Double-check the URLs of secure sites (such as financial institutions and other critical websites) to ensure they contain “https” and the appropriate country suffix. If you ever have any questions about inquiries received from financial institutions, contact the institution directly.
* Learn your organization’s policies regarding social media use and be aware that what you put online stays online. *Do not post any of your personally identifying information or sensitive government information online*.
* Recognizing disinformation is a skill everyone must develop. Before reposting content online ensure that it is factual. If you cannot verify that it is factual, do not repost it.

***Protecting Government Information and Systems***

* Using your government email account for personal matters or your personal account for official business may be prohibited in your organization’s policies. If possible, avoid using your personal email accounts when conducting official business because it may result in official government information being stored on servers that are beyond the government’s protection.
* When sending information to a printer, *make sure the documents are retrieved immediately*, and not left for others to view or collect.
* Backup your data on a regular basis.
* Practice good operations security by not discussing the details of your work outside of work, and not answering questions, however innocent they may seem, about your job, the equipment you use, or any security policies with untrusted persons.

***Mobile Device Security***

* Enable the sleep timer on your phone so that if your device is not being used it will lock automatically.
* If you do not have a need to access outside networks, consider turning off Wi-Fi and Bluetooth.
* When traveling, always maintain positive control of mobile devices, and do not leave them unattended – particularly in airports, hotel rooms, and restaurants.

For Questions Contact: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Your Organizational ICT Contact)