Information Security Awareness Program

WORKING REMOTELY DURING EVACUATION

The need for a secure work device and connection when working remotely is extremely important. The ability to stop malicious activity while connecting remotely can be done in several ways. Using a GNWT computer is preferred when available; however, during our evacuation period, we realize that employees will be using public Wi-Fi, personal, or shared computers for work purposes.

Here are a few recommendations to reduce risks while working with non-GNWT networks and devices.

1. **Awareness of Risks:** Be cautious of remote work risks, whether at an evacuation center or a hotel's business center. Avoid saving GNWT information locally on these machines. If necessary, ensure to delete files and clear the trash before logging out.
2. **Secure Public Wi-Fi:** While using public Wi-Fi, ensure your sessions are encrypted, and use the provided username and password for connecting.
3. **Shared Computer Usage:** When accessing GNWT email, SAM, or DIIMS on shared computers, clear browser history, close the browser, and consider restarting the machine before stepping away.
4. **Account and Password Security:** Do not enable account/password saving on shared or personal computers. This prevents unauthorized access and potential data breaches.
5. **Logout After Work:** Ensure to log out from applications, programs, email (e.g., MS Outlook/webmail), and your local device. Proactive logout prevents unauthorized access and maintains the confidentiality of sensitive government information.
6. **Anti-Virus Software:** If using a shared or personal computer, verify it has the latest anti-virus software version and is fully patched.
7. **Email Best Practices:** Avoid opening emails from external senders or opening attachments from unknown sources. These practices deter potential cyber threats and enhance the security of your remote work environment.
8. **Visit Secure Sites:** When browsing online, please ensure your sessions are secure and encrypted to ensure data is shielded from threats and unauthorized access.

For more information and resources, please visit the Information Security Awareness Training Site. The second course is fully dedicated to working remotely and provides comprehensive insights into maintaining a secure remote work environment.