Information Assurance Tips

- **Refresh your knowledge of Information Assurance (IA)** by completing the annual IA Awareness training at the Fort Gordon Information Assurance website. Review and maintain an updated Acceptable Use Policy.

- **Do not connect personally owned removable media (i.e., personal cell phones, personal or contractor issued computers, thumb drives, or other personal electronic devices) to the DoD network.**

- **Downloading unauthorized software to the DoD network is strictly prohibited**.

- **Keep your Common Access Card (CAC) in your possession at all times.** When you leave your computer unattended, you must remove and take your CAC with you.

- **Personally Identifiable Information (PII)- Do not reply to spam emails** or reveal personal information such as your date of birth, social security number or credit card information to unknown sources. This could result in your identity being stolen and used for illegal purposes. **When in doubt always encrypt and digitally sign all PII, OPSEC, medical, and/or contract sensitive data**.

The Information Assurance Manager (IAM) or the Information Assurance Security Team are your POCs for all IA related issues.

Contact Information

ITA Service Desk
Phone: (703) 571-4482
Email: usarmy.pentagon.hqda-ita.mbx.ita-service-desk@mail.mil

PENTCIRT
Pentagon Computer Incident Response Team
Phone: 703-695-CIRT (2478)
Email: usarmy.pentagon.hqda-ita-eima.mbx.pentcirt-ihb@mail.mil

Pentagon Force Protection Agency
Emergency Phone: 703-697-1001

Fort Gordon IA Training Center
https://ia.signal.army.mil/

IAPM: Mr. Darren King
Email: Darren.J.King.civ@mail.mil
Phone: 571-256-1585

IANM: Mr. Todd Bushman
Email: Jason.T.Bushman.civ@mail.mil
Phone: 703-545-6572

HQDA IAM: Mr. Bob Henderson
Email:
Bobby.R.Henderson4.civ@mail.mil
Phone: 703-545-3498

Information Security starts and ends with a SINGLE person –YOU!

The U.S. Army Information Technology Agency's

INFORMATION ASSURANCE INCIDENT RESPONSE CHECKLIST

A User's Guide to Information Security Quick Tips and Tools

U.S. ARMY INFORMATION TECHNOLOGY AGENCY
SERVICE & WORKFORCE EXCELLENCE

March 2013

http://ita.army.mil

INFORMATION ASSURANCE
INCIDENT RESPONSE CHECKLIST

Virus Infection/Suspicious Events

If you notice that your computer is:

- Running slower than usual
- Displaying strange error messages
- Suddenly out of space
- Unable to save files
- Pulling up corrupt files
- Missing recently used software or files
- Freezing often and has to be restarted
- Opening and closing the CD-ROM tray by itself
- Launching programs on its own
- Playing unusual sounds randomly

... Your computer is compromised. You need to complete the following actions:

Do:

- Call the ITA Service Desk: (703)571-4482
- Write down any errors that you observed on your system
- Notify your IA Staff or IAM

Do not:

- Turn off your computer
- Send any email
- Delete any files

Never open email or attachments from unknown/unexpected sources.

Unauthorized Disclosure of Classified Information

An Unauthorized Disclosure of Classified Information (UDCI) occurs when a classified message is sent on an unclassified network. For example, you receive an email to your NIPRNET account containing Secret or Top Secret information.

If a UDCI has occurred, follow these steps:

Do:

- Cease all work on the affected workstation
- Turn off the monitor
- Unplug the network cable
- Call the ITA Service Desk: (703)571-4482
- Notify your IA Staff or IAM
- Have someone with the appropriate clearance physically guard the machine

Do not:

- Leave your computer unattended
- Turn off your computer
- Send any email
- Delete any files
- Discuss details of the incident over unsecure communications

Check with your IAM or IASO to ensure that all devices are labeled properly with the correct level of classification.

CMI details are considered classified until all involved systems are sanitized.

Phishing Attacks

Phishing is any attempt to fraudulently acquire sensitive information such as passwords, personal information, military operations, and credit card/financial details, by masquerading as a trustworthy person.

To avoid falling victim to a phishing attack, follow these steps:

Beware of:

- Unsolicited email from outside of the DoD network
- Bad grammar, misspellings, and a false sense of urgency, are some typical indicators of phishing attacks
- Embedded links and attachments in unsigned and unsolicited emails

Do:

- Use strong passwords
- Use plain text or rich text formatted email
- Sign emails with your digital signature

Do not:

- Open unsolicited email messages
- Send email using HTML formatting
- Click on links in pop-ups

If you click on unreliable links or attachments, your computer or account will likely be compromised.