JOINT BASE CHARLESTON – COMPUTER EMERGENCY QUICK RESPONSE AID

VIRUS/NETWORK ATTACK SYMPTOMS

- Request To Provide, Reset, Or Change Password
- Notification Of Logon Attempts By Unknown User
- Unexplained Inability To Log On, New Files/File Names
- Inability To Save Files
- Unexplained Modifications/Deletion Of Data
- Unfamiliar Error Messages
- Sudden Lack Of Hard Drive Space
- Computer Continually Restarts
- Out-of-Memory Error Messages

VIRUS/NETWORK ATTACK RESPONSE

1. STOP USING THE COMPUTER!
2. DISCONNECT NETWORK CABLE.
3. DO NOT POWER OFF OR LOG OFF.
4. Run a custom scan on your computer.
   a. Windows 7- select Menu, Programs, McAfee and then VirusScan Console.
      - When the VirusScan Console opens right-click Full Scan.
      - Click Start.
      - Once the scan completes, verify no viruses were detected.
   b. Windows 8 - select the "McAfee" icon in the system tray.
      - Select "Scan Computer" for "Threats".
      - Ensure "Memory for rootkits", "Running processes", "All local drives", & "Registry" are listed in Scan Locations and "Include subfolders" & "Scan boot sectors" are checked.
      - Select "Start".
5. If no virus was detected, plug PC back in and continue working.
6. If a virus is detected, immediately contact your POCs below.
   a. Ensure no one uses the computer.
   b. Follow the instructions of your POC; write down all of the information regarding the incident and any behaviors observed.
   c. Your POC may have you complete a statement regarding the incident. Ensure you write down all pertinent information.

PHISHING ATTEMPT OVERVIEW/RESPONSE

A phishing attempt is any attempt to solicit personal information like passwords, network login info, CAC PIN, etc. whether via phone or e-mail. When a suspected phishing attempt occurs:
1. Write down detailed information regarding the attempt, to include the contact info of the individual soliciting information and the type of information they were attempting to gather.
2. Provide detailed info to the POCs below.

POINTS OF CONTACT

Your Unit Cybersecurity Liaisons:

Primary: _____ DSN: _____

Alternate: _____ DSN: _____

Wing Cybersecurity Office - DSN: 673-8271/673-8272
628 CS/SCXS Wing Cybersecurity Office – 628cs.wingiao@us.af.mil

628 CS Communications Focal Point - DSN: 673-2666
628 CS/CFP Communications Focal Point – 628cs.cfp@us.af.mil

CMI OVERVIEW

A Classified Message Incident (CMI) occurs when there is classified information on a system that is not approved or authorized to contain that level of classification. For instance Secret/Top Secret data on the NIPRNet or Top Secret data on SIPRNet.

CMI RESPONSE

1. STOP USING THE COMPUTER!
2. DISCONNECT NETWORK CABLE.
3. DO NOT POWER OFF OR LOG OFF.
4. Do not delete, print, or forward the message.
5. Do not leave the computer unattended. The person protecting the computer should be cleared to the level of the message.
6. Immediately contact your POCs in the order provided on the flip side of this card. DO NOT MENTION THAT YOU SUSPECT A CMI HAS OCCURRED UNTIL THE AREA IS SECURED AND YOU ARE ON A SECURE LINE.
7. Treat information regarding the CMI at the same level of classification as the CMI.
8. Isolate all external media used (disks, CDs, etc.).

SUSPICIOUS EMAIL OR SPAM

If you receive any suspicious email (to include phishing attempts, pop-ups or spam), do not open any attachments or go to any links, contact your Unit POC immediately. The POC will notify the Wing Cybersecurity Office.

INFOCON LEVELS

INFOCON is a readiness strategy that provides the ability to continuously maintain and sustain one's own information systems and networks throughout their schedule of deployments, exercises and operational readiness life cycle independent of network attacks or threats. INFOCON levels are as follows:

INFOCON 5: Normal readiness of information systems and networks that can be sustained indefinitely. Update operating system with security patches, update antivirus and ensure passwords are changed every 90 days.

INFOCON 4: Increases NetOps readiness. Check explicit permissions on folders or files and ensure they have not been modified. Verify service account privileges are needed. Backup critical data and change passwords.

INFOCON 3: Enhanced readiness procedures. Increase the frequency of validation of information and its configuration. Impact to end user is minor.

INFOCON 2: Readiness condition requiring further increase in frequency of validation of the information network and its corresponding configuration. Impact to end-user could be significant for short periods, which can be mitigated through training and scheduling.

INFOCON 1: Highest Readiness Condition: addresses intrusion techniques that cannot be identified or defeated.

JBCHARLESTONVA33-282, 15 Jun 2016 Prescribing Directive AFMAN 33-282