


Little Rock AFB
NETWORK INCIDENT REPORTING AID
OPSEC DO NOT DISCUSS/TRANSMIT CRITICAL INFORMATION VIA NON-SECURE MEANS

COMPUTER VIRUS
REPORTING PROCEDURES FOR USERS


- STEP 1** **STOP! DISCONNECT THE LAN CABLE.** 
 Discontinue Use
- STEP 2** **LEAVE THE SYSTEM POWERED UP.**
DO NOT click on any prompts, close any windows, or shut down the system.
- STEP 3** If a message appears on the monitor of the affected system **WRITE IT DOWN!**
- STEP 4** **WRITE DOWN ALL ACTIONS** that occurred during the suspected virus attack. (Did the virus come from an e-mail attachment, CD or DVD, diskette, etc..?)
- STEP 5** **REPORT IT IMMEDIATELY!** Contact your unit's Cybersecurity Liaison (CSL). The CSL will contact the COMM FOCAL POINT (CFP) at 987-2666 Opt. 2

NOTE: When reporting a suspected virus to your CSL and the COMM FOCAL POINT (CFP) ensure that you give the following information to the technician:

- Event Date and Time
- Report Date and Time
- Your name, telephone number, bldg, and organization
- Name of your CSL
- Location of infected system(s)

CLASSIFIED MESSAGE INCIDENT (CMI)
CLASSIFIED SPILLAGE
REPORTING PROCEDURES FOR USERS

A CMI is defined as a classified message that has been sent and/or received over an unclassified network. Classified Spillage is defined as any Classified information discovered on a system of a lower classification.

- STEP 1** **STOP! DISCONNECT THE LAN CABLE** of the affected computer system(s) and/or printer(s) 
- STEP 2** **SECURE** affected system(s) and/or printer(s), maintain positive control. Store in a GSA-approved container or vault, or post a guard with the appropriate clearance.
- STEP 3** **REPORT INCIDENT IMMEDIATELY** by secure telephone or in person to your Unit CSL. The Unit CSL will contact the Security Manager and COMM FOCAL POINT (CFP) located in building 988.
*** Do not report or discuss incident over unsecure line.**

PHISHING E-MAILS


- STEP 1** DO NOT REPLY, and never provide ANY information or click on any links!
- STEP 2** Right click on email, click on Junk Email, then Add Sender to Blocked Senders List.
- STEP 3** Delete all Junk Email from the Junk Email Box.

Unit Security Manager (USM)	Name: Ext:
Cybersecurity Liaison (CSL)	Name: Ext:
Comm Focal Point (CFP)	Extension: 987 – 2666 Opt. 2

**DISPLAY/POST THIS AID NEAR
 COMPUTER WORKSTATION**

Little Rock AFB
NETWORK INCIDENT REPORTING AID
OPSEC DO NOT DISCUSS/TRANSMIT CRITICAL INFORMATION VIA NON-SECURE MEANS

COMPUTER VIRUS
REPORTING PROCEDURES FOR USERS


- STEP 1** **STOP! DISCONNECT THE LAN CABLE.** 
 Discontinue Use
- STEP 2** **LEAVE THE SYSTEM POWERED UP.**
DO NOT click on any prompts, close any windows, or shut down the system.
- STEP 3** If a message appears on the monitor of the affected system **WRITE IT DOWN!**
- STEP 4** **WRITE DOWN ALL ACTIONS** that occurred during the suspected virus attack. (Did the virus come from an e-mail attachment, CD or DVD, diskette, etc..?)
- STEP 5** **REPORT IT IMMEDIATELY!** Contact your unit's Cybersecurity Liaison (CSL). The CSL will contact the COMM FOCAL POINT (CFP) at 987-2666 Opt. 2

NOTE: When reporting a suspected virus to your CSL and the COMM FOCAL POINT (CFP) ensure that you give the following information to the technician:

- Event Date and Time
- Report Date and Time
- Your name, telephone number, bldg, and organization
- Name of your CSL
- Location of infected system(s)

CLASSIFIED MESSAGE INCIDENT (CMI)
CLASSIFIED SPILLAGE
REPORTING PROCEDURES FOR USERS

A CMI is defined as a classified message that has been sent and/or received over an unclassified network. Classified Spillage is defined as any Classified information discovered on a system of a lower classification.

- STEP 1** **STOP! DISCONNECT THE LAN CABLE** of the affected computer system(s) and/or printer(s) 
- STEP 2** **SECURE** affected system(s) and/or printer(s), maintain positive control. Store in a GSA-approved container or vault, or post a guard with the appropriate clearance.
- STEP 3** **REPORT INCIDENT IMMEDIATELY** by secure telephone or in person to your Unit CSL. The Unit CSL will contact the Security Manager and COMM FOCAL POINT (CFP) located in building 988.
*** Do not report or discuss incident over unsecure line.**

PHISHING E-MAILS

- STEP 1** DO NOT REPLY, and never provide ANY information or click on any links!
- STEP 2** Right click on email, click on Junk Email, then Add Sender to Blocked Senders List.
- STEP 3** Delete all Junk Email from the Junk Email Box.

Unit Security Manager (USM)	Name: Ext:
Cybersecurity Liaison (CSL)	Name: Ext:
Comm Focal Point (CFP)	Extension: 987 – 2666 Opt. 2

**DISPLAY/POST THIS AID NEAR
 COMPUTER WORKSTATION**

Network User “DO’s and DON’Ts”

Don’t connect privately-owned media or personal devices to your computer. Cell phones (government issued cell phones are included), personal external hard drives, iPods, personally owned thumb drives or any personally owned devices are forbidden from being used on government systems. (These items are also not authorized in secured areas!)

Don’t connect ANY device to your government owned computer without getting authorization from your Unit CSL.

Don’t install, relocate, modify, or remove end user devices without prior coordination with your Unit CSL.

Don’t download a game or program from the Internet without formal software approval.

Don’t leave your computer unattended without removing your CAC from the CAC reader!

Do complete DoD IA training prior to accessing a government owned IS.

Do report suspicious activity. As the INFOCON level escalates, personnel should become increasingly mindful of situations that indicate information may be at risk. Stay alert for possible **computer viruses/malicious code attacks and unauthorized persons** asking for potentially sensitive information, i.e. user-ids, passwords, website or E-mail addresses. Heighten your awareness for signs that your E-mail, login account, or other correspondence might have been tampered with or opened.

Do review AFMAN 33-152, USER RESPONSIBILITIES AND GUIDANCE FOR INFORMATION SYSTEMS.

Common Acronyms

CAC - Common Access Card (ID card)
ESD - Enterprise Service Desk
FOUO - For Official Use Only
IA - Information Assurance
PII - Personally Identifiable Information

**DISPLAY/POST THIS AID NEAR
COMPUTER WORKSTATION**

Network User “DO’s and DON’Ts”

Don’t connect privately-owned media or personal devices to your computer. Cell phones (government issued cell phones are included), personal external hard drives, iPods, personally owned thumb drives or any personally owned devices are forbidden from being used on government systems. (These items are also not authorized in secured areas!)

Don’t connect ANY device to your government owned computer without getting authorization from your Unit CSL.

Don’t install, relocate, modify, or remove end user devices without prior coordination with your Unit CSL.

Don’t download a game or program from the Internet without formal software approval.

Don’t leave your computer unattended without removing your CAC from the CAC reader!

Do complete DoD IA training prior to accessing a government owned IS.

Do report suspicious activity. As the INFOCON level escalates, personnel should become increasingly mindful of situations that indicate information may be at risk. Stay alert for possible **computer viruses/malicious code attacks and unauthorized persons** asking for potentially sensitive information, i.e. user-ids, passwords, website or E-mail addresses. Heighten your awareness for signs that your E-mail, login account, or other correspondence might have been tampered with or opened.

Do review AFMAN 33-152, USER RESPONSIBILITIES AND GUIDANCE FOR INFORMATION SYSTEMS.

Common Acronyms

CAC - Common Access Card (ID card)
ESD - Enterprise Service Desk
FOUO - For Official Use Only
IA - Information Assurance
PII - Personally Identifiable Information

**DISPLAY/POST THIS AID NEAR
COMPUTER WORKSTATION**