SHAW AFB
NETWORK INCIDENT REPORTING AID

OPSEC: DO NOT DISCUSS/TRANSMIT CRITICAL INFORMATION VIA NON-SECURE MEANS

COMPUTER MALWARE
REPORTING PROCEDURES FOR USERS

STEP 1	*STOP! DISCONNECT THE LAN CABLE.* Discontinue Use, mark computer "Do Not Use"
STEP 2	LEAVE THE SYSTEM POWERED UP. Personnel should 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 and that you took during the suspected incident. (i.e. Sites/programs were in use, malware received from an e-mail attachment/download, etc.)
STEP 5	REPORT IT IMMEDIATELY! Contact the Communications Focal Point (CFP) at 895-2666 opt 2 and/or your Cybersecurity Liaison (CL).

NOTE: Report the following information to the CFP or CL:
- Event Date and Time
- Report Date and Time
- Your name, telephone number, bldg, and organization
- Location of infected system(s)

CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES

A CMI is defined as a classified message that has been sent and/or received over a network that is not approved for the classification in question.

STEP 1	*STOP! DISCONNECT THE LAN CABLE.* Discontinue Use, mark computer/printer "Do Not Use"
STEP 2	SECURE affected system(s) and/or printer(s) in a GSA-approved container or vault, or post a guard with the appropriate clearance.
STEP 3	REPORT INCIDENT IMMEDIATELY by telephone or in person to your Security Manager, CL, or CFP (POC info on back of this card). You may only say, "I'd like to report a possible CMI" via non-secure means and wait for Helpdesk personnel to assist.

Note: For users with government-issued Mobile Devices involved in a suspected CMI, follow steps 2 and 3 above. CMIs on AFNET e-mail can also propogate to the mobile device.

PHISHING EMAILS *PROCEDURES*

Phishing: a form of online identity theft where attackers deceive internet users into submitting personal information to illegitimate web sites or through email.

STEP 1	**DO NOT RELEASE PERSONAL INFORMATION** through the internet/email unless you verify who is receiving the information and the site/email is secure. (i.e. encrypted email, HTTPS site) (NOTE: For general Spam, block the sender and delete message.)
STEP 2	**DRAG EMAIL FROM YOUR INBOX TO YOUR DESKTOP** to save the email. DO NOT click reply or forward on original email.
STEP 3	**ATTACH SAVED EMAIL TO NEW EMAIL** and send it to 20fw.ia@us.af.mil. Email will be an attachment.

*Emails that contain illegal content, **STOP!** Notify your USM and supervisor.*

INFOCON LEVELS

INFOCON presents a structured, coordinated approach to defend against and react to adversarial attacks on DoD computer / telecommunication systems and networks.

INFOCON levels are as follows:

Level 5: Routine NetOps: Normal Readiness of information systems and networks that can be sustained indefinitely.
Level 4: Increased Vigilance: In preparation for operations or exercises, with a limited impact to the end user.
Level 3: Enhanced Readiness: Increases the validation frequency of information networks and the corresponding configuration. Impact to end-user is minor.
Level 2: Greater Readiness: Increases the validation frequency of information networks and the corresponding configuration. Impact to administrators will increase and impact to end-user could be significant.
Level 1: Maximum Readiness: Addresses intrusion techniques that cannot be identified or defeated at lower readiness levels. Only implemented in limited cases. Could be significant impact on administrators and end-users.

DISPLAY/POST THIS AID NEAR COMPUTER WORKSTATION

SHAWAFBVA33-1, 14 March 2019
OPR: 20 CS/SCXS
Prescribing Directive: AFI17-203
ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at www.e-publishing.af.mil.
RELEASABILITY: There are no releasability restrictions on this publication.

SHAW AFB
NETWORK INCIDENT REPORTING AID
OPSEC: DO NOT DISCUSS/TRANSMIT CRITICAL INFORMATION VIA NON-SECURE MEANS
COMPUTER MALWARE
REPORTING PROCEDURES FOR USERS
STEP 1 STOP! DISCONNECT THE LAN CABLE. Discontinue Use, mark computer "Do Not Use"
STEP 2 LEAVE THE SYSTEM POWERED UP. Personnel should 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 and that you took during the suspected incident. (i.e. Sites/programs were in use, malware received from an e-mail attachment/download, etc.)
STEP 5 REPORT IT IMMEDIATELY! Contact the Communications Focal Point (CFP) at 895-2666 opt 2 and/or your Cybersecurity Liaison (CL).
NOTE: Report the following information to the CFP or CL:
- Event Date and Time
- Report Date and Time
- Your name, telephone number, bldg, and organization
- Location of infected system(s)
CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES
A CMI is defined as a classified message that has been sent and/or received over a network that is not approved for the classification in question.
STEP 1 STOP! DISCONNECT THE LAN CABLE. Discontinue Use, mark computer/printer "Do Not Use"
STEP 2 SECURE affected system(s) and/or printer(s) in a GSA-approved container or vault, or post a guard with the appropriate clearance.
STEP 3 REPORT INCIDENT IMMEDIATELY by telephone or in person to your Security Manager, CL, or CFP (POC info on back of this card). You may only say, "I'd like to report a possible CMI" via non-secure means and wait for Helpdesk personnel to assist.
Note: For users with government-issued Mobile Devices involved in a suspected CMI, follow steps 2 and 3 above. CMIs on AFNET e-mail can also propogate to the mobile device.
PHISHING EMAILS PROCEDURES
Phishing: a form of online identity theft where attackers deceive internet users into submitting personal information to illegitimate web sites or through email.
STEP 1 DO NOT RELEASE PERSONAL INFORMATION through the internet/email unless you verify who is receiving the information and the site/email is secure. (i.e. encrypted email, HTTPS site) (NOTE: For general Spam, block the sender and delete message.)
STEP 2 DRAG EMAIL FROM YOUR INBOX TO YOUR DESKTOP to save the email. DO NOT click reply or forward on original email.
STEP 3 ATTACH SAVED EMAIL TO NEW EMAIL and send it to 20fw.ia@us.af.mil. Email will be an attachment.
Emails that contain illegal content, STOP! Notify your USM and supervisor.
INFOCON LEVELS
INFOCON presents a structured, coordinated approach to defend against and react to adversarial attacks on DoD computer / telecommunication systems and networks.
INFOCON levels are as follows:
Level 5: Routine NetOps: Normal Readiness of information systems and networks that can be sustained indefinitely.
Level 4: Increased Vigilance: In preparation for operations or exercises, with a limited impact to the end user.
Level 3: Enhanced Readiness: Increases the validation frequency of information networks and the corresponding configuration. Impact to end-user is minor.
Level 2: Greater Readiness: Increases the validation frequency of information networks and the corresponding configuration. Impact to administrators will increase and impact to end-user could be significant.
Level 1: Maximum Readiness: Addresses intrusion techniques that cannot be identified or defeated at lower readiness levels. Only implemented in limited cases. Could be significant impact on administrators and end-users.
DISPLAY/POST THIS AID NEAR COMPUTER WORKSTATION
SHAWAFBVA33-1, 14 March 2019
OPR: 20 CS/SCXS
Prescribing Directive: AFI17-203
ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at www.e-publishing.af.mil.
RELEASABILITY: There are no releasability restrictions on this publication.

INFOCON PROTECTIVE MEASURES

Network User "DO's and DON'Ts"

Don't download a game or program from the Internet without formal software approval.
Don't ever leave your computer unattended without locking your workstation and removing your CAC.
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 **malware** attacks and unauthorized persons asking for potentially sensitive information, e.g. 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.

When to sign and/or encrypt E-mail

PKI Digital Encryption -- Use DoD PKI certificates to encrypt e-mail containing For Official Use Only, Privacy Act, and Personally Identifiable information; individually identifiable health information; and other sensitive, but unclassified information.
PKI Digital Signature -- Use digital signatures whenever it is necessary for the recipient to be assured of the sender's identity or to have confidence the message has not been modified.

Important Contact Information

Wing Cybersecurity Office: 895-1133
Communications Focal Point (CFP): 895-2666 Opt 2
Wing Information Protection: 895-3638

Your Cybersecurity Liaisons (CL): Name:_____

Phone:_____ Name:_____

Phone:_____

Your Client Service Center (CSC):

Name:_____Phone:_____

Name:_____Phone:_____

Unit Security Manager (USM): Name:_____

Phone:_____ Name:_____

Phone:_____

NOTES

DISPLAY/POST THIS AID NEAR COMPUTER WORKSTATION

SHAWAFBVA33-1, 14 March 2019
OPR: 20 CS/SCXS
Prescribing Directive: AFI17-203

REVERSE

INFOCON PROTECTIVE MEASURES

Network User "DO's and DON'Ts"

Don't download a game or program from the Internet without formal software approval.
Don't ever leave your computer unattended without locking your workstation and removing your CAC.
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 **malware** attacks and unauthorized persons asking for potentially sensitive information, e.g. 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.

When to sign and/or encrypt E-mail

PKI Digital Encryption -- Use DoD PKI certificates to encrypt e-mail containing For Official Use Only, Privacy Act, and Personally Identifiable information; individually identifiable health information; and other sensitive, but unclassified information.
PKI Digital Signature -- Use digital signatures whenever it is necessary for the recipient to be assured of the sender's identity or to have confidence the message has not been modified.

Important Contact Information

Wing Cybersecurity Office: 895-1133
Communications Focal Point (CFP): 895-2666 Opt 2
Wing Information Protection: 895-3638

Your Cybersecurity Liaisons (CL): Name:_____

Phone:_____ Name:_____

Phone:_____

Your Client Service Center (CSC):

Name:_____Phone:_____

Name:_____Phone:_____

Unit Security Manager (USM): Name:_____

Phone:_____ Name:_____

Phone:_____

NOTES

DISPLAY/POST THIS AID NEAR COMPUTER WORKSTATION

SHAWAFBVA 33-1, 14 March 2019 OPR: 20 CS/SCXS
Prescribing Directive: AFI17-203

REVERSE