

30th Space Wing Network Incident Reporting Aid

OPSEC – Do not discuss/transmit critical information by non-secure means

SUSPICIOUS ACTIVITY PROCEDURES FOR USERS

SITUATION	ACTION	REASON
Unknown personnel in your area with questionable behavior	<ol style="list-style-type: none"> 1. Challenge unknown personnel 2. Do not give any sensitive information 3. Report to security 	 <p>He or she may want to gain unauthorized network access or access to sensitive information.</p>
Roaming cursor/ strange pop-ups	<ol style="list-style-type: none"> 1. DISCONNECT THE LAN CABLE. 2. Follow Computer Virus Reporting steps below 	Someone may have unauthorized remote access to your computer.
Email with a hyperlink that may ask you to update/validate information	<ol style="list-style-type: none"> 1. Look for a digital signature before clicking links or replying 2. If it's not there, DELETE the email. 	 <p>It may be a phishing attempt. Your unit Information System Security Officer (ISSO) can verify its authenticity.</p>
Website asking for personal information	<ol style="list-style-type: none"> 1. Check the URL 2. If it looks suspicious (www.dissa.mil.com), check with your unit ISSO before entering any information 	It may be a phishing attempt. Your ISSO can verify its authenticity.
Email with virus warnings	<ol style="list-style-type: none"> 1. DELETE. Do not forward. 2. Advise your unit ISSO 	These emails are intended to clog the email system.

NEVER GIVE ANYONE YOUR CAC PIN OR PASSWORD!

COMPUTER VIRUS REPORTING PROCEDURES FOR USERS

If you are experiencing:	<ul style="list-style-type: none"> - Unusually slow performance - Files disappearing - Constant computer error messages - Antivirus program is disabled for no reason
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	WRITE DOWN: <ul style="list-style-type: none"> - ACTIONS prior to suspected virus (i.e. received suspicious email with attachments, inserted unchecked drive/disk, downloaded unchecked files, etc.) - Any error messages - Date & time
STEP 4	REPORT IT IMMEDIATELY! Contact your unit ISSO or Client Support Technician (CST). If they cannot be reached, contact the Wing Cybersecurity Office (WCO) at 606-7173. After normal duty hours, contact the Communications Focal Point (CFP) at 606-2622.

CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES FOR USERS

If you think a classified message has been sent and/or received over an unclassified network:	
STEP 1	STOP! DISCONNECT THE LAN CABLE of the affected computer system(s) or printer(s). DO NOT POWER OFF!
STEP 2	GUARD the entire system as if it were classified itself and do not use it further until it is purged by authorized personnel.
STEP 3	REPORT INCIDENT IMMEDIATELY by telephone or in person to the ISSO or CST. If they cannot be reached, contact the WCO at 606-7173. After normal duty hours contact the CFP at 606-2622. Note: You may only say "I'd like to report a possible CMI" via non-secure means.
STEP 4	SECURE affected system(s) or printer(s) in a GSA-approved security container or vault, or post a guard with the appropriate clearance, and wait for authorized personnel to assist.

30SWVA33-5, 24 Feb 2016 Prescribed by AFI 33-115
Supersedes 30 SWVA 33-5, 8 JUNE 2011
OPR: 30 SCS/SCXSI

RELEASABILITY: There are no releasability restrictions on this publication.

30th Space Wing Network Incident Reporting Aid

OPSEC – Do not discuss/transmit critical information by non-secure means

SUSPICIOUS ACTIVITY PROCEDURES FOR USERS

SITUATION	ACTION	REASON
Unknown personnel in your area with questionable behavior	<ol style="list-style-type: none"> 1. Challenge unknown personnel 2. Do not give any sensitive information 3. Report to security 	 <p>He or she may want to gain unauthorized network access or access to sensitive information.</p>
Roaming cursor/ strange pop-ups	<ol style="list-style-type: none"> 1. DISCONNECT THE LAN CABLE. 2. Follow Computer Virus Reporting steps below 	Someone may have unauthorized remote access to your computer.
Email with a hyperlink that may ask you to update/validate information	<ol style="list-style-type: none"> 1. Look for a digital signature before clicking links or replying 2. If it's not there, DELETE the email. 	 <p>It may be a phishing attempt. Your unit Information System Security Officer (ISSO) can verify its authenticity.</p>
Website asking for personal information	<ol style="list-style-type: none"> 1. Check the URL 2. If it looks suspicious (www.dissa.mil.com), check with your unit ISSO before entering any information. 	It may be a phishing attempt. Your ISSO can verify its authenticity.
Email with virus warnings	<ol style="list-style-type: none"> 1. DELETE. Do not forward. 2. Advise your unit ISSO 	These emails are intended to clog the email system.

NEVER GIVE ANYONE YOUR CAC PIN OR PASSWORD!

COMPUTER VIRUS REPORTING PROCEDURES FOR USERS

If you are experiencing:	<ul style="list-style-type: none"> - Unusually slow performance - Files disappearing - Constant computer error messages - Antivirus program is disabled for no reason
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	WRITE DOWN: <ul style="list-style-type: none"> - ACTIONS prior to suspected virus (i.e. received suspicious email with attachments, inserted unchecked drive/disk, downloaded unchecked files, etc.) - Any error messages - Date & time
STEP 4	REPORT IT IMMEDIATELY! Contact your unit ISSO or Client Support Technician (CST). If they cannot be reached, contact the Wing Cybersecurity Office (WCO) at 606-7173. After normal duty hours, contact the Communications Focal Point (CFP) at 606-2622.

CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES FOR USERS

If you think a classified message has been sent and/or received over an unclassified network:	
STEP 1	STOP! DISCONNECT THE LAN CABLE of the affected computer system(s) or printer(s). DO NOT POWER OFF!
STEP 2	GUARD the entire system as if it were classified itself and do not use it further until it is purged by authorized personnel.
STEP 3	REPORT INCIDENT IMMEDIATELY by telephone or in person to the ISSO or CST. If they cannot be reached, contact the WCO at 606-7173. After normal duty hours contact the NCC at 606-2622. Note: You may only say "I'd like to report a possible CMI" via non-secure means.
STEP 4	SECURE affected system(s) or printer(s) in a GSA-approved security container or vault, or post a guard with the appropriate clearance, and wait for authorized personnel to assist.

30SWVA33-5, 24 Feb 2016 Prescribed by AFI 33-115
Supersedes 30 SWVA 33-5, 8 JUNE 2011
OPR: 30 SCS/SCXSI

RELEASABILITY: There are no releasability restrictions on this publication.