NETWORK INCIDENT REPORTING AID
REMEMBER OPSEC! DO NOT DISCUSS CRITICAL INFORMATION BY NON-SECURE MEANS

SUSPICIOUS EMAIL REPORTING PROCEDURE

User receives an email that may include phishing, a scam, cybersecurity threat, fraud, identity theft, social engineering, or fake website

STEP 1	**Network Security first!! DO NOT reply & never provide CAC PIN to anyone!**
STEP 2	**Report the Cyber Threat via "IT Support & Services" desktop icon.**
STEP 3	**Click "Self-Service IT Support and Services".**
STEP 4	**Click "Fix IT", Report an IT Issue, select Email or Messaging, select next and complete the required fields.**

COMPUTER VIRUS REPORTING PROCEDURE

STEP 1	**STOP USING THE SYSTEM! Unplug the network cable from back of computer, immediately.**
STEP 2	**DO NOT SHUT OFF THE COMPUTER Label computer "DO NOT USE" (back of card) Write down observed errors. DO NOT run antivirus software**
STEP 3	**REPORT IT IMMEDIATELY Report incident to your unit Commander Support Staff (CSS) and Unit Security Manager (USM)**

DATA SPILLAGE INCIDENT REPORTING PROCEDURE

Data Spillage Incident is defined as classified information in any form that has been sent or received over an unclassified network

STEP 1	**STOP USING THE SYSTEM - Unplug the network cable from computer and/or printer. DO NOT email, delete, move or save message**
STEP 2	**LEAVE COMPUTER POWERED ON Label computer "DO NOT USE" (back of card) Keep Under Positive Control - Protect as Classified**
STEP 3	**REPORT IT IMMEDIATELY Contact Unit CSS Representative and USM, in person or via secure phone.**

UNAUTHORIZED REMOVABLE MEDIA ON DOD SYSTEMS

STEP 1	**NOTIFY your Unit ISSO if you find unauthorized removable media!**
STEP 2	**SECURE the device until give further instruction! Do not connect it to any other systems.**
STEP 3	**VIOLATORS will have their network accounts suspended and must re-accomplish their annual Cyber Awareness Challenge training plus their unit CC could impose additional administrative punishments!**

How to disconnect computer from the network

DEPLOY/POST THIS AID NEAR ALL CYBERSPACE SYSTEMS

STEP 1	**Locate the LAN Jack on the Laptop/Computer**
STEP 2	**Depress the tab on the cable connector and gently pull**

Do Not Discuss Classified information on Unclassified communication systems.

Phishing Emails:

Phishing emails are malicious attempts to obtain sensitive information such as passwords, credit card numbers, or personal details:

- Look Authentic: Mimic reputable organizations (banks, online services, etc)
- Sense of Urgency: Urge immediate action to prevent negative consequences (e.g., 'Your account will be suspended!')
- Links & Attachments: Contain links or attachments that lead to malicious websites or install malware
- Personal Information: Request personal information directly (passwords, account numbers)

Spam Emails:

Spam emails, on the other hand, are usually harmless but unwanted messages sent in bulk:

- Advertisements: Promote products, services, or get-rich-quick schemes
- Non-Personalized: Lack personalized content; generic and mass-produced
- Annoyance: Mostly irritating but not dangerous
- Frequency: Repeatedly sent from the same sender, often ending up in the spam folder

Tips to Identify:

Check the Sender's Email: Phishing emails often have strange or misspelled sender addresses

Look for Typos: Poor grammar and spelling errors are common in phishing emails

Verify Links: Hover over links to see the URL; phishing links may look suspicious or unrelated

Be Skeptical of Requests for Personal Info: Legitimate organizations rarely ask for sensitive info via email

HOW TO SEARCH FOR EMAILS FROM SAME SENDER

1. In Outlook, right-click the message from the sender
2. Select **Find Related > Messages from Sender**

CSS/USM Contact Information:

CSS: Name:_____Phone:_____

USM: Name:_____ Phone:_____

DISPLAY/POST THIS AID NEAR COMPUTER WORKSTATION

KEESLER AFBVA_17-1 6 MARCH 2026

OPR: 81 CS/SCXS
Per DAFMAN17-301, AFI 17-203

Releasability: There are no releasability restrictions on this publication
Supersedes: KeeslerAFBVA 17-1, 18 June 2020

Do Not Use

FOLD

INCIDENT INFORMATION FOR USER TO REPORT
USER NAME:
USER PHONE:
USER EMAIL:
USER ORGANIZATION:
FSO POC:
EVENT DATE/TIME:
LOCATION: BLDG/ROOM/CUBICLE
NOTES: DOCUMENT ANY MESSAGES / POP-UPs / CONTACTS / ACTIONS DURING EVENT

KEESLER AFBVA_17-1 6 MARCH 2026
OPR: 81 CS/SCXS
Per DAFMAN17-301, AFI 17-203
Releasability: There are no releasability restrictions on this publication
Supersedes: KeeslerAFBVA 17-1, 18 June 2020