

Cyber Awareness Challenge Reference Material

E-mail Security

Tips About E-mail Use

Your organization requires that you agree with the following terms of use before accessing your e-mail.

E-mail use must not adversely affect performance of your role or reflect poorly on your organization.

To use e-mail appropriately:

- Do not use e-mail to sell anything
- Do not send:
 - Chain letters
 - Offensive letters
 - Mass e-mails
 - Jokes
 - Unnecessary Pictures
 - Inspirational stories
- Avoid using “Reply All” to prevent sending unnecessary e-mail traffic
- Only make personal use of e-mail if allowed by your organization
- Prevent viruses and downloading of **malicious code**:
 - View e-mail in plain text and don’t view e-mail in Preview Pane
 - Use caution when opening e-mail: Look for digital signatures if your organization uses them. Digitally signed e-mails are more secure.
 - Scan all attachments
 - Delete e-mail from senders you do not know
 - Don’t e-mail infected files to anyone
 - Don’t access Websites in e-mail or popups

Follow your organization’s policy on Webmail (a Web-based service that checks e-mail remotely). If Webmail is allowed, use caution as it may bypass built-in security features and other safeguards, such as encryption, and thus may compromise security.

Tips About Internet Hoaxes

Internet hoaxes:

- Clog networks
- Slow down Internet and e-mail services
- Can be a part of a distributed denial of service (DDoS) attack

To protect against Internet hoaxes:

- Use online sites to confirm or expose potential hoaxes
- Don't forward e-mail hoaxes
- Follow your organization's policies on loading files onto workstations and laptops

Tips About Phishing

Phishing attempts use suspicious e-mails or pop-ups that:

- Claim to be from your military service, government organization, Internet service provider, bank, or other plausible sender
- Direct you to a Website that looks real
- Claim that you must update or validate information
- Threaten dire consequences

Assume all unsolicited information requests are phishing attempts and follow your organization's IT security policies and guidelines.

To protect against phishing:

- Do not access sites by selecting links in e-mails or pop-up messages. Type the address or use bookmarks.
- Contact the organization using a telephone number you know to be legitimate if you are suspicious of a link or attachment
- Delete the e-mail or forward to your security POC
 - Report e-mails requesting personal information to your security POC or help desk
 - If you are a member of the intelligence community, report **all** phishing attempts to your security POC
- Look for digital signatures
- Never give out organizational, personal, or financial information to anyone by e-mail
- Avoid sites with expired certificates. If officially directed to a site with expired certificates, report it to your security POC or help desk.

Tips About Spear Phishing

Spear phishing is a type of phishing attack that targets particular individuals, groups of people, or organizations.

To protect against spear phishing:

- Be wary of suspicious e-mails that use your name and/or appear to come from inside your organization or a related organization
- Forward the spear phishing e-mail to your security POC and then delete it

Tips About Whaling

Be aware that high-level personnel may be targeted through complex and targeted phishing attacks called “whaling.”

Whaling:

- Is targeted at senior officials
- Uses personalized information: Name, title, official e-mail address, sender names from personal contact lists
- Is an individualized, believable message
- Exploits relevant issues or topics

To protect against whaling:

- Be wary of e-mails that ask for sensitive information, contain unexpected attachments, or provide unconfirmed URLs
- Forward the whaling e-mail to your security POC and then delete it