Online Behavior

Social Networking

Follow information security best practices at home and on social networking sites. Be aware of the information you post online about yourself and your family. Sites own any content you post. Once you post content, it can't be taken back. The social networking app TikTok is banned on all Government devices.

Social Networking: Protect Yourself

To protect yourself:

- Understand and use the privacy settings
- Create strong passwords
- Don't give away your position through GPS or location links or updates about places where you are or where you will be
- If possible, validate all friend requests through another source, such as phone or e-mail, before confirming them
- Don't connect with people you don't know, even if you share mutual connections
- Beware of links to games, quizzes, and other applications available through social networking services
- Avoid posting personally identifiable information (PII):
    - Social Security Number
    - Date and place of birth
    - Mother's maiden name
    - Home address

Social Networking: Protect Your Organization

To protect your organization:

- Don't speak or appear to speak for your organization or post any embarrassing material
- Carefully consider who you accept as a friend and validate, if possible, before acceptance
- If posting pictures of yourself in uniform or in a work-setting, make sure there are no identifiable landmarks or items visible
- When establishing personal social networking accounts, use only personal contact information, never your Government contact information
- If you work with classified or sensitive material as a Federal Government civilian employee, military member, or contractor:
    - Inform your security POC of all non-professional or non-routine contacts with foreign nationals, including, but not limited to, joining each other's social media sites
    - If you believe a foreign national is contacting you specifically, seek further guidance from your security POC

Disinformation

Adversaries exploit social and other media to share and rapidly spread false or misleading news stories and conspiracy theories about U.S. military and national security issues. Using fake accounts on popular social networking platforms, these adversaries:

- Disseminate fake news, including propaganda, satire, sloppy journalism, misleading headlines, and biased news
- Share fake audio and video, which is increasingly difficult to detect as the creation technology improves
- Gather personal information shared on social media to devise social engineering attacks

Digital Literacy

Most media messages intend to influence you, if only to attract traffic. Ask yourself:

- Who provided the information, and why?
- How does the information provider want you to act?
- Whose interests would your reaction serve?

To avoid being misled by disinformation:

- Research the source to evaluate its credibility and reliability
- Read beyond the headline
- Check against known facts and other sources on the topic
- Consider whether the story is intended as a joke
- Check your personal biases
    - Consider whether your views or beliefs are affecting your judgement
    - Actively seek opposing or disconfirming content

Online Misconduct

Keep in mind when online: Online misconduct is inconsistent with DoD values. Individuals who participate in or condone misconduct, whether offline or online, may be subject to criminal, disciplinary, and/or administrative action. When online:

- Treat others with respect and dignity
- Do NOT use electronic communications for:
    - Harassment
    - Bullying
    - Hazing
    - Stalking
    - Discrimination
    - Retaliation

Remember: No one is truly anonymous online!

Social Engineering

Social engineers use telephone surveys, e-mail messages, websites, text messages, automated phone calls, and in-person interviews. To protect against social engineering:

- Do not participate in telephone surveys
- Do not give out personal information
- Do not give out computer or network information
- Do not follow instructions from unverified personnel
- Document interaction:
  - Verify the identity of all individuals
  - Write down phone number
  - Take detailed notes
- Contact your security POC or help desk
- Report cultivation contacts by foreign nationals

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
- Directs you to a website that looks real
- Asks you to call a phone number to make any change to your computer, such as to help clean a virus from your computer
- 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
  - Report e-mails requesting personal information to your security POC or help desk
- 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.

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
- Report the spear phishing e-mail to your security POC

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 contacts 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
- Report the whaling e-mail to your security POC

Smishing

Smishing is a type of social engineering that uses a Short Message Service (SMS) message to deceive you. SMS messages are commonly known as text messages. The goal is to obtain your personal information or gain access to your device. To protect against smishing:

- Do not reply or click the link in the message
- Delete the message

Vishing

Vishing is a type of social engineering that uses voice calls to deceive you into giving up personal information or installing software that provides access to your devices or network. To protect against vishing:

- Let calls from unknown numbers go to voicemail. Legitimate callers will leave a message.