Online Behavior

Social Networking

Follow these 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.

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

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

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!

Online Identity

Social networking sites are not the only source of your online identity. Many apps and smart devices collect and share your personal information, and contribute to your online identity. These include, but are not limited to:

- Fitness and health trackers
- Professional networking apps
- Dating apps and websites
- Secure chat
- Neighborhood advisory apps
- Audio-enabled personal digital assistants and the smart devices they support, such as phones, TVs, and speakers

Feeding off the data collected by these apps and devices, as well as information available in public records, online data aggregators collect and catalogue information about you. You should opt out of data aggregation and use these apps and devices with caution.

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 face 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

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

Internet Hoaxes

Internet hoaxes clog networks, slow down internet and e-mail services, and can be 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

Ethical Use of GFE

Ethical use of government furnished equipment (GFE):

- Use GFE for official purposes only
- Don't view or download pornography
- Don't gamble on the Internet
- Don't conduct private business/money-making ventures
- Don't load or use personal/unauthorized software or services, such as DropBox or peer-to-peer (P2P) software
    - P2P software can compromise network configurations, spread viruses and spyware, and allow unauthorized access to data
- Don't illegally download copyrighted programs or material

- Don't make unauthorized configuration changes
- Only check personal e-mail if your organization allows it
- Don't play games unless allowed by your organization to do so on personal time

Note: All DoD-owned devices are subject to monitoring. When you use these devices, you authorize the monitoring of your activity on these devices.

Use of Government 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 use e-mail for personal reasons if allowed by your organization
- Use a digital signature when sending attachments or hyperlinks, as required by the DoD
- Do not use personal accounts, such as webmail, to conduct official DoD communication

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.

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