

Cyber Awareness Challenge Reference Material

Social Networking

Guarding Your Online Privacy

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
- Beware of links to games, quizzes, and other applications available through social networking services
- Avoid posting personally identifiable information (PII):
 - Social security numbers
 - Dates and places of birth
 - Mothers' maiden names
 - Home addresses

Protecting Your Organization

To protect your organization:

- Don't speak for your organization or post any embarrassing material
- Consider who you accept as a friend carefully 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

If you work with classified or sensitive material as a federal government civilian employee, military member, or contractor:

- Inform your security point of contact (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