# Cybercrime Prevention Flyer

CPF 00015-2022-CID361-9H 26 May 2022

## Operations Security (OPSEC)

OPSEC is a pretty common term to those affiliated with the military, but what does it mean for day to day life? Simply put, OPSEC just means being careful about what is communicated to others. A person's online activity and conversations, whether a service member or civilian, says a lot: who they are, where they are, what they do, family members and friends, likes and dislikes, and personal and professional affiliations to say the least. Always remember anything posted online is permanent.

Be cautious providing information to unknown persons. If a close friend cannot be trusted with the information, it should not be told to a stranger. Criminals, nation state actors, and terrorists often use social media to gather information on people, places, and activities or events. This can be both personal and professional information. Even if you think posting just one thing is okay, it is not. Information can be aggregated to form a complete profile of a person, event, or location.

Below are some general guidelines to follow for OPSEC.

### OPSEC Guidelines

- Change social media account settings for additional layers of security as the default settings are normally set to public. Allow only family and friends to view social media profiles and posts.
- Do not accept social media requests from unknown persons.
- Do not post specific information regarding deployments, military graduations, private ceremonies, or other significant events. This includes information such as times, dates, places, names, units, or office information.
- Do not post specific information relating to vacations, home address, or employment.
- Do not post photos revealing military unit information, location, and capabilities. Photos can be easily exploited by enemies searching for landmarks or unit patches that may be in the photo.

**Report a crime to U.S. Army Criminal Investigation Division**

Cyber Directorate
27130 Telegraph Road
Quantico, Virginia 22134

Email

Cyber Directorate Web Page

CID LOOKOUT
ON POINT FOR THE ARMY



"Do What Has To Be Done"

# Cybercrime Prevention Flyer

- Be cautious posting personal photos, interior home photos, photos of children, and vacation photos while on the vacation. Photos are often revealing, providing insight into family life and potential intelligence to scammers, predators, and other criminals.
- Do not check-in or geotag any social media posts as it will give away the location of where the post was made.
- Be aware that smart watches and fitness trackers are able to track movement. Ensure smart device settings are not public.
- Be cautious when downloading or using third party applications. Always verify what information those applications have access to.
- Do not post or discuss sensitive information, including classified and controlled unclassified information.
- Do not post information commonly used in general security questions, i.e. first car, mother's maiden name, first pet, or other personal information not typically known by non-family members or close friends. This information can be used to compromise most online account security questions.
- Do not click suspicious links as they can sometimes lead to malicious downloads. Always verify where a link may come from.

## Resources:

Social Media Protection

Social Networking Safety Tips

CISA Guidelines for Publishing Information Online

Security and Safety During Deployment

Internet Social Networking Risks

*To receive future Cyber Directorate Cybercrime Prevention Flyers, send an email to:* Subscribe CPF