UNITED STATES
EUROPEAN COMMAND

Social Media and Cyber Security

Whether on Facebook, Twitter, or any other social networking site, there are a few simple and proactive measures that can be taken to protect you and your Family's online information from those who wish to do harm.

Don't use a password that is easy to crack

Your password should consist of 20 characters and be generated either randomly or by using a combination of random words. Insert a few numbers and symbols to bolster your password strength.

When in doubt, throw it out

Links in e-mail, tweets, posts, and online ads are often the way cybercriminals compromise your computer. If something looks suspicious, even if you know the source, it is best to delete it or mark it as junk e-mail.

Limit access to your accounts

Minimize who can access your information and remember that you are never entirely alone when you are online. Allow access to your online accounts only if the need exists and be sure other users know how to safeguard your personally identifiable information. Also, review your privacy and security settings on a regular basis.

Think Operations Security (OPSEC)

Think before you post pictures, "check in" to a certain location, or post personal data. Consider who can see this information and how it could be misused.

Questions?
Need More Info?

Visit these websites:

United States Army Europe
Information Technology Training
Program

https://aeitt.ext.eur.army.mil

USAREUR G6
Cybersecurity Division (CSD)

https://intranet.eur.army.mil/hq/iassure/SitePages/Home.aspx

This publication is available at
https://aepubs.army.mil

AE MISC PUB 25-2D ● 19 JUL 18

SAFEGUARDING SOCIAL-MEDIA ACCOUNTS

Protect your Mission, Identity, and Life!

Headquarters
United States Army Europe
Wiesbaden, Germany

Headquarters
United States Army Installation
Management Command, Europe Region
Sembach, Germany

Two-Factor Authentication

USEUCOM Task Order

The United States European Command released a task order (TASKORD) that directs HQ USEUCOM and all USEUCOM components to implement two-factor authentication on DOD-managed, official-use, Internet-based capabilities (IBCs).

This TASKORD will ensure tightened authentication security for all Services to prevent unauthorized intruders from compromising DOD assets.

What is Two-Factor Authentication?

Two-factor authentication is a hardened cyber-access control that adds an extra layer of security to the login procedure. This procedure significantly increases the level of difficulty for an adversary to compromise social-networking services even if the user-name and password are known to the adversary. Two-factor authentication requires something you know (that is, your user-name and password) and something you have (that is, a mobile device, a computer, or another e-mail account).

Why Two-Factor Authentication?

Multiple adversaries continue to display capability and intent to compromise DOD-managed, official-use IBCs. IBCs include, but are not limited to, collaborative tools such as social-networking sites, social media, user-generated content, social software, web-based e-mail, instant messaging, and discussion forums (for example, YouTube, Facebook, Twitter, Google Apps).

SOMETHING YOU KNOW
+
SOMETHING YOU HAVE

There are great resources available for social media and for keeping your accounts secure:

"The United States Army Social Media Handbook"

http://www.slideshare.net/USArmySocialMedia/social-media-handbook32-38656179

"Guide to Keeping Your Social Media Accounts Secure"

http://www.eucom.mil/social-media

How to Enable Two-Factor Authentication to Social-Media Sites

Google Applications:
https://support.google.com/accounts/answer/185839?hl=en&t opic=1056283&ctx=topic

Facebook:
https://www.facebook.com/note.php?note_id=10150172618258920

Twitter:
https://blog.twitter.com/2013/getting-started-with-login-verification

LinkedIn:
http://blog.linkedin.com/2013/05/31/protecting-your-linkedin-account-with-two-step-verification/