



Fort Bliss Antiterrorism/ Force Protection Program

Risks of Social Media Use

Internet Social Networking Risks

Social networking sites have created a revolution in social connectivity. However, con artists, criminals, and other dishonest actors are exploiting this capability for nefarious purposes. Humans are a weak link in cyber security, and hackers and social manipulators know this. They try to trick people into getting past security walls. They design their actions to appear harmless and legitimate.

Once information is posted to a social networking site, it is no longer private. The more information you post, the more vulnerable you may become. Even when using high security settings, friends or websites may inadvertently leak your information.

Personal information you share could be used to conduct attacks against you or your family. The more information shared, the more likely someone could impersonate you and trick one of your friends into sharing personal information or downloading malware. Predators, hackers, and hostile actors troll social networking sites looking for information or people to target for exploitation.

How To Avoid Being a Victim

- *Always use high security settings on social networking sites, and be very limited in the personal information you share.*
- *Do not click on links in email messages from unknown sources.*
- *Disable Global Positioning System (GPS) encoding.*

Report any suspicious incidents or activity on social networking sites to IT personnel immediately.

For more information, go to <https://www.bliss.army.mil/iWATCH/>