15-Apr-15
15-015

Sir or Ma'am,

Terrorist groups recently used information publicly available on the internet and social media to release a list of 100 service members, their photographs and other personal information, and encouraged supporters to target these members.

We all have a responsibility to protect ourselves and our military community by reducing vulnerabilities through active and vigilant monitoring of personal information available on the internet and social media. Practical tips follow.

Social media privacy settings and usage guidelines:

- Change social media privacy settings to allow only friends to see personal information. The default settings for many social networks allow your private information to be viewed by the public
- Verify the identity of those with whom you correspond
- Do not share private information, such as where your children go to school, home addresses, phone numbers, times and locations of events you plan to attend, or other similar information
- Never share information such as unit movements, deployments, personnel rosters, weapons information, or other command critical information.
- Resources for learning to use social media safely can be found at the following DoD and FBI websites:
    - Http://www.defense.gov/socialmedia/education-and-training.aspx/
    - Http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks

Geotagging/tracking:

- Many mobile devices and applications can track your physical location, providing your exact whereabouts at any given time
- Review your device settings for geotagging/tracking features and disable
- Turn off your device's GPS when not actively using it to navigate
- Disable apps that track your approximate location based on your cell phone signal
- Digital cameras, cell phones, tablets, and other mobile devices with GPS capability embed the coordinates for your physical location in the metadata of photographs. Turn this feature off

Internet use safeguards:

- Protect your home wireless network with a unique network name and password
- Limit who has access to your private network
- Ensure your personal computer has up-to-date antivirus, anti-spyware, and firewall software installed
- Use encryption when transmitting personal information and avoid using public file sharing services
- Always assume mobile apps and public networks are unsecure
- Hackers can "spoof" your phone, causing it to connect to their wireless network. To avoid this, regularly clear your phone's memory of networks and turn off the Wi-Fi when not in use

The bottom line is BE ALERT. Always maintain good situational awareness and report all suspicious activity to the appropriate authorities.

Thank you for taking the necessary precautions to protect yourself, your family and your Air Force.

John Sotham, Colonel, USAF
IMA to the Commander, HQ Individual Reservist Readiness and Integration Organization

Connect with HQ RIO online
HQ RIO Website
Facebook
Twitter
YouTube

**Previous ARCNet messages are located in the Resources section of our website**