THE FACTS: PROTECTING PERSONALLY IDENTIFIABLE INFORMATION

What are some ways I can protect my personally identifiable information (PII) online?

• Many social networking sites, chat rooms and blogs have privacy settings. Find out how to use these settings to restrict who can see and post on your profiles. Check periodically for updates to privacy settings and policies for sites you use often.

• Limit your online friends to people you actually know.

• Learn about and manage location-based services. Many phones and cameras have GPS technology, and there are applications that let you find out where your friends are — and let them to find you. Set your privacy settings so that only people you know personally can see your location. Think about turning off location-based services when not needed. Ask yourself, "Does this app need to know where I am?"

• Trust your gut if you feel threatened or uncomfortable because of something online. If necessary, report your concerns to the police and others who can help.

• Treat information such as your Social Security number, bank account and credit card numbers like valuables – because they are.

• Limit personal information including ranks, full names, street addresses, schedules and routine activities. Be aware of the content in photos as well -- elements such as house numbers, vehicles, license plate numbers and work locations are often overlooked, but could provide personal details or indicate an affiliation with important individuals or high-value targets.

• Passwords should be "long and strong." A combination of symbols, number, and upper- and lowercase letters is usually the best option. Do not use birth dates, family names or other easily guessed information. Never share your passwords, write them down, or store them near your computer.

• Don't reply to text, email, or pop-up messages that ask for personal information, even if a message looks like it's from a friend, family member or company you know, or threatens that something bad will

happen if you don't reply. These may be fakes, sent to steal your information.

• Protect your computer with security and antivirus software and keep it and your web browser up to date. If your applications offer the option to download updates automatically, consider enabling it.

• Be cautious about opening attachments or clicking on links. They may contain viruses or spyware.

• Sometimes free stuff such as games, ring tones or screen savers can hide viruses or spyware. Don't download free stuff unless you trust the source and scan the file with security software first.

• Don’t leave laptops, tablets or phones unattended in public — even for a minute. If they go missing, everything on them, such as data, messages and photos, may fall into the wrong hands.

• If you download apps, you may be giving their developers access to your personal info — maybe even info unrelated to the app. For example, you download a game, but the company that made the app gets access to your entire contact list and can share it with marketers or other companies. You can try to check what information the app collects — if it tells you — and check your privacy settings. Think about whether getting that app is really worth sharing the details of your life. Find out what application components such as cookies, Active-X controls and multimedia players do before downloading.

Some helpful links:
Federal Trade Commission online protection tips:
http://www.onguardonline.gov/articles/0033c-protection-connection
U.S. Computer Emergency Readiness Team (US-CERT) tips for publishing information online:
https://www.us-cert.gov/ncas/tips/ST05-013
US-CERT safe social networking information:
https://www.us-cert.gov/ncas/tips/ST06-003

Follow ARCYBER on
(click the images to visit our pages)

ABOUT US: United States Army Cyber Command directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.

As of 2 March 2016