



FACT SHEET

U.S. Army Cyber Command and Second Army

The Nation's Army in Cyberspace

www.arcyber.army.mil

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.
- 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.
- Protect your information, particularly things such as your Social Security number and family financial information such as bank account or credit card numbers.
- Passwords should be "long and strong." The longer they are, the harder they are to crack.
- 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 software and keep it up to date.
- Be cautious about opening attachments or clicking on links. They may contain viruses or spyware.

ABOUT US: United States Army Cyber Command and Second Army 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

- 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.

Source: <http://www.onguardonline.gov/articles/0033c-protection-connection>



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



ABOUT US: United States Army Cyber Command and Second Army 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