THE FACTS: SOCIAL NETWORKING BASICS

Facebook, Twitter, Google+, YouTube, Pinterest, LinkedIn and other social networks have become an integral part of our online lives. They're a great way to stay connected with others, but you should be cautious about posting personal information.

What are some basic strategies for safe social networking?

-- Learn about and use the privacy and security settings on social networks. They are there to help you control who sees what you post and manage your online experience in a positive way. Know that some sites will share your information, including email addresses and user preferences, which can increase spam. Consider hiding your email address or changing the settings so that only a few people you trust can see it. Also, check out the site's referral policy so you don't unintentionally sign up your friends to get spam.

-- Once posted, always posted: Protect your reputation. What you post online stays online.
Think twice before posting things you wouldn't want your parents or future employers to see. One Microsoft study found that 70 percent of job recruiters rejected candidates based on information they found online.
-- On the other hand…Microsoft also found that job recruiters respond to a strong, positive personal brand online. So show your smarts, thoughtfulness, and mastery of the environment.
-- Keep personal info personal: Be cautious about how much personal information you provide on social networking sites. The more you post, the easier it may be for a hacker or criminal to use that information to steal your identity, access your data, or commit crimes such as stalking.
-- Know and manage your friends: Some of the fun of social networks is creating a pool of friends from many aspects of your life. But that doesn't mean all friends are created equal. Use a site or group's tools to manage the information you share.
-- Be honest if you're uncomfortable: If someone posts something about you that makes you

uncomfortable or you think is inappropriate, let them know. Likewise, be open-minded if a friend tells you something you've posted about him makes him uncomfortable.
-- Know what action to take: If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator.
-- Be wary of strangers. The Internet is full of weirdos and people misrepresenting themselves. Consider limiting who you allow to contact you on social media, and be cautious about what info you reveal.
-- Be skeptical. Don't believe everything you read online. There is a lot of false and misleading information out there, so try to verify details before taking any action.
-- Use caution with third-party applications. They might be fun, but they often require a lot of your personal information. Be wary of any that seem suspicious, and modify your settings so you limit what information they can access.
-- Use strong passwords.

SOURCE: National Cyber Security Alliance Cyber Threat Resources booklet, November 2012; DoD release, October 2015

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 26 April 2016