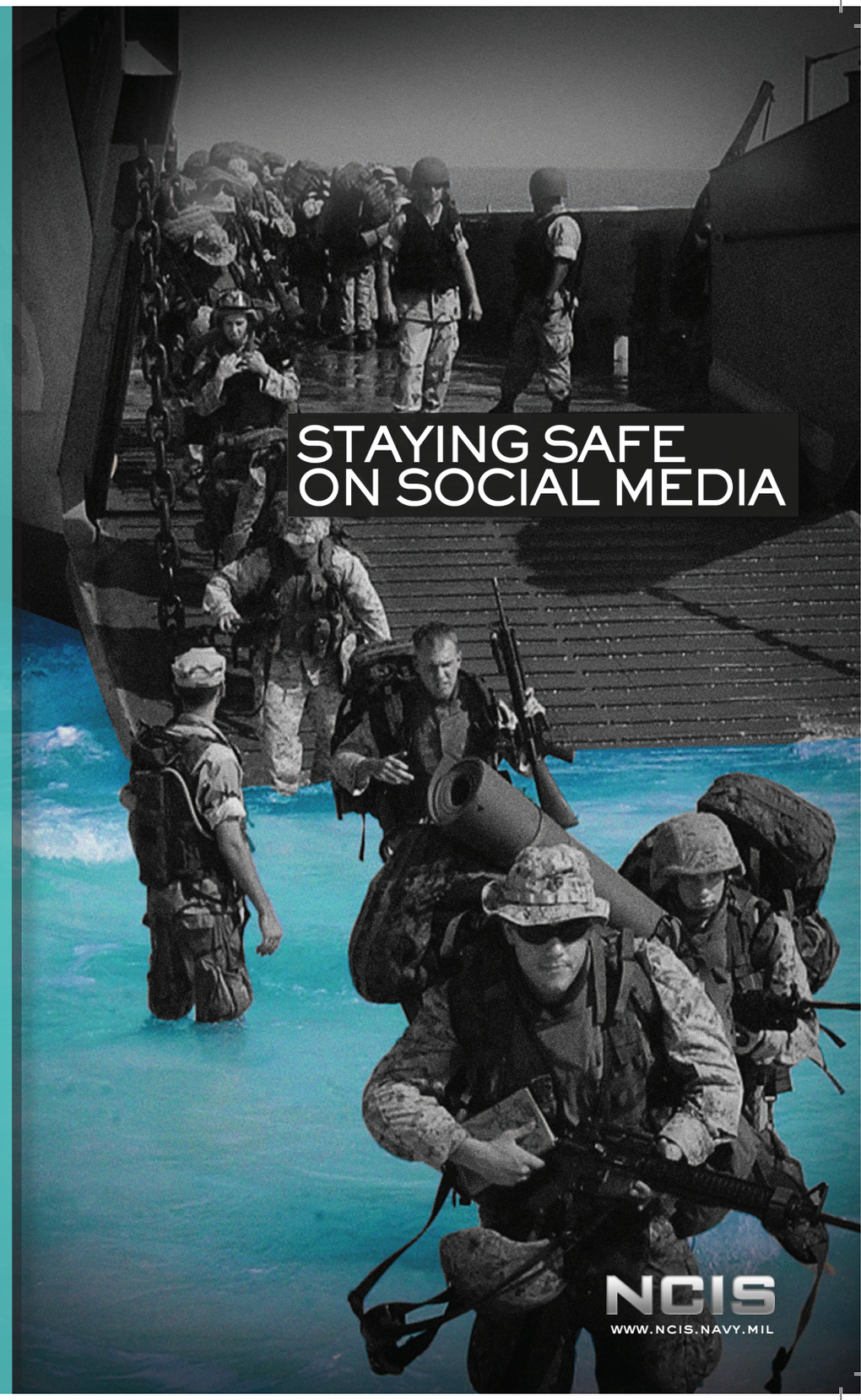
USE STRONG PASSWORDS & USE CARE WHERE YOU ENTER THEM.
Protect your account with passwords that cannot easily be guessed. Don't pick a word from the dictionary. Try to use a combination of at least eight letters, numbers, and symbols. Also, use different passwords for all of your online accounts. If your common password is compromised, you could lose access to all of your accounts at once, and someone may be able to access your accounts and pretend to be you. Be careful where you enter passwords. Just because a page on the Internet looks like Facebook or other sites you use, it doesn't mean that it is. If you have doubts about whether a link is real, simply type the website's URL (ex: https://www.facebook.com) into the browser's address bar. Facebook will never ask you for your password, except to log in. Never send your password in an instant message or an email. Lastly, add security questions to all of your online accounts that offer them, but don't use answers available on your profile (such as mother's maiden name or high school mascot). Security questions come in handy if you lose access and need to prove who you are.

USE CARE ON UNSECURE PUBLIC WIRELESS NETWORKS (WI-FI).
Be careful when accessing or sending information over an unsecured public wireless network. Don't send sensitive information if you can't verify that a Wi-Fi network is secure. Enable secure browsing by using "https" URLs. Select https in the account setting menu or type https://(thewebsiteyouwant) to access the site.

CHECK PRIVACY POLICIES.
Some sites may share information, such as email addresses and user preferences, with other companies. This may increase the amount of spam you receive. Try to find the policy for referrals to make sure you do not unintentionally sign your friends up for spam. Some sites continue to send email messages to people you refer until they join.

USE AND UPDATE SECURITY SOFTWARE.
Security software should include anti-virus, anti-spyware, and anti-phishing components and a firewall. Anti-virus software recognizes most known viruses and protects your computer against them, so viruses are detected and removed before doing any damage. Because attackers are continually writing new viruses, it is important to keep your software up-to-date. In addition, make sure you have an up-to-date web browser, such as the latest version of Internet Explorer, with an anti-phishing blacklist. And remember to set the preference on your operating system, such as Windows, to update automatically.



WHAT IS SOCIAL MEDIA?

Social media or social networking sites, sometimes referred to as friend-of-a-friend sites, build upon the concept of traditional social networks in which you connect to new people through people you already know to share information, ideas, personal messages, and other content (such as videos and pictures). The purpose of some networking sites is purely social, allowing users to establish friendships or romantic relationships, while others focus on establishing business connections.

Although social networking site features differ, they all encourage you to provide information about yourself and offer communication mechanisms (such as forums, chat rooms, email, and instant messenger) that enable you to connect with other users. On some sites, you can browse for people based on certain criteria; other sites require that you be "introduced" to new people through a connection you share. Many of the sites have communities or subgroups for people who share a particular interest.

WHAT SECURITY IMPLICATIONS DO THESE SITES PRESENT?

Social networking sites rely on connections and communication, so they encourage you to provide personal information. When deciding how much information to reveal, people may not exercise the same level of caution as they would meeting someone in person because:

- the Internet provides a sense of anonymity
- the lack of physical interaction provides a false sense of security
- information is tailored for friends, rather than for the other users who may see it
- insights are offered to impress potential friends or associates

While the majority of people who use these sites do not pose a threat, malicious people are drawn to them because they are easily accessible and offer vast amounts of personal information. The more information about you that malicious people have, the easier it is for them to take advantage of you. Predators form relationships online and then persuade unsuspecting "friends" to meet them in person, which could lead to a dangerous situation. Personal information is also used to conduct a social engineering attack. Using information you've provided about your location, hobbies, interests, and friends, malicious people can impersonate a trusted friend or convince you that they have the proper authority so you allow them access to other personal or financial data.

Additionally, because these sites are so popular, attackers use them to distribute malicious code. Sites that offer applications developed by third parties are particularly susceptible. Attackers create customized applications that appear to be legitimate, but they infect your computer without your knowledge.

COMBATING THE CYBER THREAT

LIMIT THE AMOUNT OF PERSONAL INFORMATION YOU POST.
Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also, be considerate when posting information, including photos, about your connections.

REMEMBER THE INTERNET IS A PUBLIC RESOURCE.
Post only information you are comfortable with everyone seeing. Be aware that other people may forward your information to others. This includes information and photos in your profile and in blogs and other forums. Also, once you post information online, you can't retract it. Even if you remove information from a site, saved or cached versions may still exist on other people's machines.

BE WARY OF STRANGERS.
The Internet makes it easy for people to misrepresent their identities and motives. Consider limiting the number of people who are allowed to contact you through these sites. If you interact with people you do not know, be cautious about the amount of information you reveal and about agreeing to meet them in person. Only "friend" people you know.

BE SKEPTICAL.
Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities. This is not necessarily done with malicious intent; it could be unintentional, an exaggeration, or a joke. Take appropriate precautions, though, and try to verify the authenticity of information before taking action. Be suspicious of email or messages that contain an urgent request or ask you to update or provide new information, as well as emails and messages with misspellings or bad grammar, especially from someone who is usually a good writer. In addition, don't click on links or open attachments that look suspicious. If it sounds off or too good to be true, it probably is.

EVALUATE YOUR SETTINGS.
Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile. You can customize settings to restrict access to certain people. However, there is still a risk that even this information could be exposed, so don't post anything that you wouldn't want the public to see. Also, be cautious when deciding which applications to enable, and check your settings to see what information the applications are able to access.