The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Overview
- Privacy
- Security

Social Networking Safely

GUEST EDITOR

Ted Demopoulos is the guest editor for this issue. He is a longtime security consultant and has been teaching SANS courses for a decade, including SEC401/501 and MGT414/512. Learn more about Ted at http://demop.com.

OVERVIEW

Social networking sites such as Facebook, Twitter, Google+, Pinterest and LinkedIn are powerful, allowing you to meet, interact and share with people around the world. However, with all these capabilities come risks; not to just you, but your family, friends and employer. In this newsletter we will discuss what these dangers are and how to use these sites more safely.

PRIVACY

A common concern about social networking sites is privacy protecting your personal information and the sensitive information of others. Potential dangers include:

- **Impacting Your Future:** Many organizations search social networking sites as part of background checks. Embarrassing or incriminating posts, no matter how old, can prevent you from getting hired or promoted. In addition, many universities conduct similar checks for new student applications. Privacy options may not protect you, as these organizations can ask you to "Like" or join their pages prior to the application process.
- **Attacks Against You**: Cyber criminals can harvest your personal information and use it for attacks against you. For example, they can use your information to guess the answers to your "secret questions" to reset your online passwords, create targeted email attacks called spear phishing or apply for a credit card using your name. In addition these attacks can spill into the physical world, such as identifying where you work or live.
- **Harming Your Employer:** Criminals or competitors can use any sensitive information you post about your organization against your employer. In addition, your posts can potentially cause reputational harm for your organization. Be sure to check with your organization's policies before posting anything about your employer.

Social Networking Safely

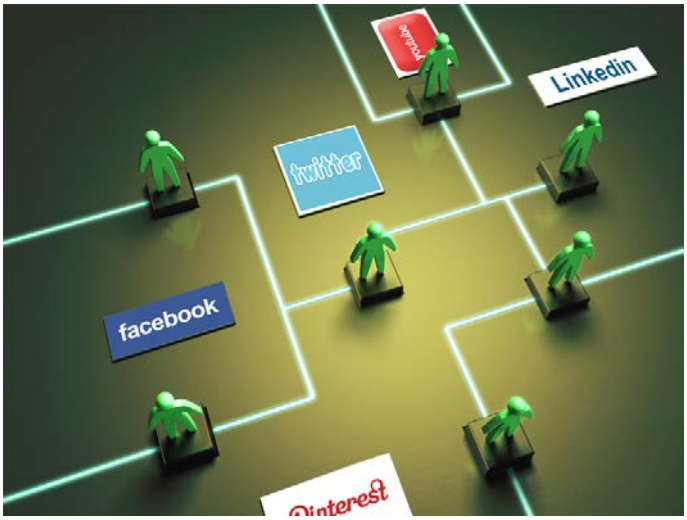
The best protection is to limit the information you post. Yes, privacy options can provide some protection; however, keep in mind that privacy options are often confusing and can change frequently without you knowing. What you thought was private could become public for a variety of reasons. In addition, the privacy of your information is only as secure as the people you share it with. The more friends or contacts you share private information with, the more likely that information will become public. Ultimately, the best way to protect your privacy is to follow this rule: if you do not want your mother or boss to see your post, you most likely should not post it.

Also be aware of what information friends are posting about you. It can be just as damaging If they post private information or embarrassing photos of you. Make sure your friends understand what they can or cannot post about you. If they post something you are not comfortable with, ask them to take it down. At the same time, be respectful of what you post about others.

SECURITY

In addition to privacy concerns, social networking sites can be used by cyber criminals to attack you or your devices. Here are some steps to protect yourself:

- **Login:** Protect your social networking account with a strong password and do not share this password with anyone or re-use it for other sites. In addition, some social networking sites support stronger authentication, such as two-step verification. Enable stronger authentication methods whenever possible.
- **Encryption:** Many social networking sites allow you to use encryption called HTTPS to secure your connection to the site. Some sites like Twitter and Google+ have this enabled by default, while other sites require you to manually enabled HTTPS via account settings. Whenever possible use HTTPS.
- **Email**: Be suspicious of emails that claim to come from a social networking site; these can easily be spoofed attacks sent by cyber criminals. The safest way to reply to such messages is to log in to the website directly, perhaps from a saved bookmark, and check any messages or notifications using the website.



Social networking sites are powerful and fun, but be careful what you post and whom you trust.

Social Networking Safely

- **Malicious Links/Scams**: Be cautious of suspicious links or potential scams posted on social networking sites. Cyber criminals can post malicious links and if you click on them, they take you to websites that attempt to infect your computer. In addition, just because a message is posted by a friend does not mean it is from them, as their account may have been compromised. If a family member or friend has posted an odd message you cannot verify (such as they have been robbed and need you to send money), call them to confirm the message.
- **Apps**: Some social networking sites give you the ability to add or install third-party applications, such as games. Keep in mind there is little or no quality control or review of these applications; they may have full access to your account and private information. Only install apps that you need, that are from well-known, trusted sites and remove them when you no longer need them.

Social networking sites are a powerful and fun way to communicate with the world. If you follow the tips outlined here, you should be able to enjoy a much safer online experience. For more information on how to use social networking sites safely or report unauthorized activity, be sure to review the security pages of the sites you are using.

RESOURCES

Some of the links have been shortened for greater readability using the TinyURL service. To mitigate security issues, OUCH! always uses TinyURL's preview feature, which shows you the ultimate destination of the link and asks your permission before proceeding to it.

11 Security Tips for Online Social Networking:
http://preview.tinyurl.com/b28a525

FB Security:
https://www.facebook.com/safety

Your FB Security Settings:
https://www.facebook.com/settings?tab=security

Common Security Terms:
http://preview.tinyurl.com/6wkpae5

SANS Security Tip of the Day:
http://preview.tinyurl.com/6s2wrkp

BECOME A SECURITY PROFESSIONAL

Become a certified security professional from the largest and most trusted security training organization in the world at SANSFIRE. Over 40 security classes taught by the world's leading experts. 14-23 June in Washington DC. http://www.sans.org/event/sansfire-2013

OUCH! is published by the SANS Securing The Human program and is distributed under the Creative Commons BY-NC-ND 3.0 license. Permission is granted to distribute this newsletter as long as you reference the source, the distribution is not modified and it is not used for commercial purposes. For translating or more information, please contact ouch@securingthehuman.org.

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner

© The SANS Institute 2013