OUCH! | September 2011

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Overview
- Privacy
- Security

# Social Networking Safety

## GUEST EDITOR

Lenny Zeltser is the guest editor for this issue of OUCH! Lenny focuses on safeguarding customers' IT operations at Radiant Systems and teaches malware combat at the SANS Institute. Lenny is active on Twitter as @lennyzeltser and writes a security blog at blog.zeltser.com.

## OVERVIEW

This month we'll look at social networking sites, such as Facebook, Twitter, Google+ and LinkedIn. Sites such as these are powerful tools, allowing you to meet, interact with, and share with people around the world. However with all these capabilities come considerable risks, not to just you but your employer, family, and friends. In this newsletter we will discuss what these dangers are and how to use these sites safely.

## PRIVACY

A common concern about social networking sites is your privacy, the risk of you or others sharing too much information about yourself. These dangers of oversharing include:

- **Damaging Your Career**: Embarrassing information may harm your future. Many organizations search social networking sites as part of a new employee background check to see what has been posted about you. Any embarrassing or incriminating posts, no matter how old they are, may prevent you from getting that new job. In addition, many universities conduct similar checks for new student applications.

- **Attacks Against You**: Cyber criminals can harvest your information and use it for attacks against you. For example, they can harvest your personal information to guess the answers to "secret questions" that websites use to reset your passwords or perhaps apply for a credit card using your personal information.

- **Attacks Against Your Employer**: Criminals may gather information that you share on social networking sites when compiling competitive data or preparing for a cyber attack on your employer. Moreover, your actions online may inadvertently reflect badly on your employer. Be sure to consult your employer's social networking policy for

# Social Networking Safety

guidelines on how you are expected to safeguard your organization's data and reputation.

The most effective way to protect yourself against these dangers is to be cautious about what information you post about yourself. Consider whether the data you are sharing now could be used against you some time later. Also, tighten the privacy settings of your social networking profile to limit who can see the personal information you might share on the site. Keep in mind that your data may be inadvertently leaked by the website or your friends, so it is best to assume that any information you post will at some point become public knowledge. Also, be aware of what others post about you. If you have friends posting information, pictures, or other data you do not want made public, ask them to remove it.


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

## SECURITY

In addition to being the source of damaging information leaks, social networking sites can be used as a platform for attacking your system or conducting scams. Here are some steps to protect yourself.

- **Login**: Protect your social networking account with a strong password. (See OUCH May 2011) Do not share this password with anyone or use it for other sites. In addition, some social networking sites, such as Facebook or Google+, support features for stronger authentication, such as using one-time passwords when logging in from public computers or using your phone as part of the login process. Enable these features where possible.

- **Encryption**: Many sites, such as Facebook, Google+, and Twitter, allow you to force all communications with the website to be encrypted (called HTTPS). Whenever possible, enable this option.

- **E-mail**: Be cautious when clicking on links in e-mail messages that claim to originate from a social networking site. Instead, access the site using a saved bookmark and check any messages or notifications using the website directly.

# Social Networking Safety

- **Links**: Be careful of clicking on links posted on people's walls or public pages. Viruses and worms spread easily on such sites. If a link seems odd, suspicious, or too good to be true, do not click on it…even if the link is on your most trusted friend's page. Your friend's account may have been hijacked or infected and now be spreading malware.

- **Scams**: Criminals take advantage of the open nature of social networking sites to defraud individuals. Such scams sometimes use the pretext of an offer for a job or money that is too good to be true. Another common scam uses hijacked accounts to contact the victim's friends with requests for help, claiming that the person got robbed in a foreign country and needs money. Be cautious when approached by a friend or a stranger on a social networking site with a request for money or with an offer that's surprisingly good.

- **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 and they may have full access to your account and the data you share. Malicious apps can use this access to interact with your friends on your behalf and to steal and misuse personal data. Be careful, and only install apps that come from trusted, well-known sites. Once they are installed, make sure you keep them updated. If you are no longer using the app, then remove it.

Social networking sites are a powerful and fun tool; they allow you to communicate with the world. If you follow the tips outlined here, you should be able to enjoy a much safer online experience.

## RESOURCES

Some of the links shown below 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.

OnGuard Online: http://preview.tinyurl.com/5yjgjt
Microsoft: http://preview.tinyurl.com/3q4qzzr
US CERT: http://preview.tinyurl.com/df9f2d
Facebook: http://www.facebook.com/safety
Twitter: http://preview.tinyurl.com/3mb92rp

## LEARN MORE

Subscribe to the monthly OUCH! security awareness newsletter, access the OUCH! archives, and learn more about SANS security awareness solutions by visiting us at http://www.securingthehuman.org