Information Security Newsletter

Issue 2, October 14, 2015

Follow this and additional works at: https://digitalcommons.georgiasouthern.edu/infosecnews
Part of the Computer Sciences Commons, and the Higher Education Commons

Recommended Citation
https://digitalcommons.georgiasouthern.edu/infosecnews/6

This newsletter is brought to you for free and open access by Digital Commons@Georgia Southern. It has been accepted for inclusion in Information Security Newsletter by an authorized administrator of Digital Commons@Georgia Southern. For more information, please contact digitalcommons@georgiasouthern.edu.
5 Threats To Your Security When Using Social Media

By Elli Bishop from SafeWise.com

Social networking has changed the way we interact with friends and associates. While social networks, like Facebook, Twitter, YouTube, FourSquare, and Google+, play a significant role in our lives, they are also a high risk for security threats.

With hundreds of millions of users online, these tools not only attract friends and family wanting to stay in touch, but they also attract people wanting to know about you for the wrong reasons. Be aware of the top five security threats currently out there to help you stay safe online.

1. Having Your Identity Stolen

Identity thieves gather personal information from social media sites. Even if you have your account on the highest security settings, there are still ways for an identity thief to get your information. Most social network sites have information that is required, such as email address or birthday. It’s common for an identity thief to hack an email account by using social information. For example, a common technique to get personal information is by clicking on “forgot password” and trying to recover the information through email. Once the thief has access to your email account, they then have access to all information on your social networking sites.

So what can you do to protect yourself? You don’t have to
Cyber Security
Awareness Class
For all Employees

During the month of October, GSU highlights our local training for Cyber Security. Each employee must complete the general cyber security awareness training course contained in BuildingABetterU by December 31st. For instructions, please visit http://its.georgiasouthern.edu/infosec/cyber-security-awareness-course-instructions/

When you use social networking sites, you are posting personal information. Once information is posted online, it’s no longer private and can fall into the wrong hands. The more you post, the more vulnerable you become to those who may wish to harm you. Even with the highest security settings, friends, associates, and even the brands you “like” on your networking sites, can inadvertently leak information about you. The websites you subscribe to, the apps you download, and the games you play on social networking sites all contain personal information about you. Every time you browse a website, companies

- Have a strong password. The stronger your password, the harder it is to guess. Use special characters like symbols and capital letters when creating your password. Also, don’t use “common” passwords, like your birthday or your child’s name.
- Be careful with your status updates. Often, we innocently post status updates that would give an identity thief information they need to steal our identity. For example, you may post “Happy birthday to my mother!” and then tag her in the post. Likely, your mother’s maiden name will be associated with that tag now. A popular security question is “What is your mother’s maiden name?” and if you share that online, you run the risks of identity thieves getting the answer to this commonly used question.
- Don’t reveal your location. You can use a fake location or make one up from another city and state. You may even be able to leave this information blank. Be cautious and never use a city and state where you live.

2. Getting Your Computer Or Social Profile Hacked
Hackers love social networking, going right to the source to interject malicious code. The code hackers use can steal your identity, inject viruses to your computer, and obstruct

bank account information, to name a few. Shortened URLs, such as those created on bit.ly, are especially susceptible to hackers. Shortened URLs can trick users into visiting harmful sites where personal information can be compromised because the full URL is not seen.

The best advice is to never click on a link until you are sure of the source. To tell if a link is safe, you can:
- Hover over the link. If you hover over a link without clicking, you’ll see the full URL in the lower corner of your browser. If this is a website you recognize, go ahead and click.
- Try a link scanner. A link scanner is a website that lets you enter the URL of a link you suspect might be suspicious to check for safety. Try URLVoid or MyWOT as possible options.
- Check shortened links. A shortened link is popular on sites like Twitter where character length matters. Some shortened link sites include bit.ly, Ow.ly, and TinyURL. Use a service like Sucuri to determine if the real link is secure.

3. Inadvertently Letting Stalkers Find You

- Delete all your social profiles or hide from the real world; just take these precautions.
can put invisible markers on your computer called cookies. In theory, no two cookies are alike. When you are online, these cookies track your activity as you move from site to site.

To keep sites from tracking your activity, click on the “Do Not Track” feature. Most websites have an option for you to opt out of tracking. You can also clear the cache and cookies on your browser regularly to help prevent any problems.

4. Letting Burglars Know Your Whereabouts
Telling the online world where you’re going and when you aren’t at home is inviting burglars to your house. Did you know that a run-of-the-mill burglar can break into your home in less than 60 seconds and spend less than 10 minutes stealing your possessions? By telling the world you are on vacation in Europe, you're letting potential thieves know where you are, how long you'll be gone, and where you live. Burglars are fond of constant updates, especially about your travel plans. You wouldn’t stand up in the middle of a crowd and announce you’re going on vacation for a week, would you? Of course not, but that’s what you do when you post your vacation pictures and plans online.

When you go on vacation:

- Avoid posting specific travel plans. Never post when, where, or how long you'll be gone.
- Wait until you are home to post pictures to a vacation album.
- Use highest privacy control. Only let certain groups, like a family group, view your photos.
- Be selective with the status updates. You can use an audience-selector dropdown menu on Facebook to choose certain groups to see your status updates.
- Stay offline. You’re on vacation, after all. Relax and forget about the online world for a few days.

5. Becoming Overconfident
One of the biggest threats to online security is overconfidence. Whether at home or at work, many users believe as long as they have a firewall and an antivirus installed, there is no threat to security. Many people also believe that they don’t have anything worth hacking so there’s no need to worry about security. With today’s technology, we are more connected to each other than ever before. When you neglect security, you not only put yourself at risk, but others are at risk as well.

To keep yourself and your information safe, pay careful attention to your online activity. Avoid posting information including:

- Travel plans (see point 4)
- Bank account information
- Your full address and birthdate
- Your children’s’ names, school, and birthdates
- Location information, such as the name of your workplace
- Your daily schedule

You can still use social networks for all they were meant to accomplish, but you need to take extra precautions to make sure your personal information doesn’t get in the wrong hands. Know what threats you are most vulnerable to and take steps to protect yourself and your networks.

Resources for more information:

National Cyber Security Alliance
www.Staysafeonline.org

Stop.Think.Connect
www.dhs.gov/stophinkconne ct
The Office of Information Security promotes a secure environment for the university to meet its mission of academic distinction in teaching, scholarship, research, and service.

Michael Fox, Chief Information Security Officer, Georgia Southern University
Email: security@georgiasouthern.edu    Web: GeorgiaSouthern.edu/infosec