RISE
Enable • Protect
Research-centric Information Security Enablement Program

BSD
Information Security Office
Cybersecurity
Newsletter

May 2016 | SECURITY.BSD.UCHICAGO.EDU | Volume 2, Issue 5

Inside this Issue:

Socializing Securely

Common threats from the use of social networking include viruses, identity theft, third-party applications, and social engineering attacks. This article describes the possible threats and the implications of those threats as well as how to protect yourself by implementing security measures and following good practices when using social networking services.

What are social networking sites?

Social networking sites, sometimes referred to as "friend-of-a-friend" sites, build upon the concept of traditional social networks where you are connected to new people through people you already know. The purpose of some networking sites may be purely social, allowing users to establish friendships or romantic relationships, while others may focus on establishing business connections.

What security implications do these sites present?

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

1. The Internet provides a sense of anonymity;
2. The lack of physical interaction provides a false sense of security;
3. They tailor information for their friends to read, forgetting that others may see it as well;
4. They want to offer insights to impress potential friends or associates.

While the majority of people using these sites do not pose a threat, malicious people may be drawn to them because of the accessibility and amount of personal information that's available. The more information malicious people have about you, the easier it is for them to take advantage of you.

How can you protect yourself?

- **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 that the Internet is a public resource** - Only post information you are comfortable with anyone seeing. 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 the 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 people who are allowed to contact you on these sites. If you interact with people you do not know, be cautious about the amount of information you reveal or agreeing to meet them in person.

- **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 any information before taking any action.

- **Evaluate your settings** - Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile, but you can customize your settings to restrict access to only certain people. There is still a risk that private information could be exposed despite these restrictions, so don't post anything that you wouldn't want the public to see. Sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate.

- **Be wary of third-party applications** - Third-party applications may provide entertainment or functionality, but use caution when deciding which applications to enable. Avoid applications that seem suspicious, and modify your settings to limit the amount of information the applications can access.

- **Use strong passwords** - Protect your account with passwords that cannot easily be guessed. If your password is compromised, someone else may be able to access your account and pretend to be you.

- **Check privacy policies** - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam. Some sites will continue to send email messages to anyone you refer until they join.

- **Keep software, particularly your web browser, up to date** - Install software updates so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.

- **Use and maintain anti-virus software** - Anti-virus software helps protect your computer against known viruses, so you may be able to detect and remove the virus before it can do any damage. Because attackers are continually writing new viruses, it is important to keep your definitions up to date.

UCM Data Guardian Program for BSD Email Accounts

The next phase of the University of Chicago Medicine's Data Guardian Program to protect sensitive information sent via BSD email accounts launches June 20th. This will apply to all BSD departments, centers and institutes, including clinical, bridge and basic science departments.

Launched in March '16, the Data Guardian Program is a collection of tools aimed at helping you protect sensitive data – such as PHI and SSNs. The first phase of the Data Guardian program is to use a technology tool designed to catch emails with protected patient or employee information, but which did not carry #encrypt in the subject field, and automatically encrypt them before sending the emails out of our secure environment.

Users that fail to use the #encrypt indicator will get an email notification stating their email contained restricted information and was encrypted before being sent out or blocked from being sent with instructions on next steps.

Data theft is a growing threat. Underground rates for personal information can range from between $30 and $50 per record, making it increasingly attractive for hackers to try and infiltrate very enterprises and steal sensitive information.

What's important to note is that the software tool will not be able to read your emails. Instead, it will be searching for matches of various data points contained in our electronic medical records and email communications. Also, if you do not send protected health information, this will have no impact.

The following BSD email domains will now benefit from this program:

babies.bsd.uchicago.edu
bsd.uchicago.edu
bsdad.uchicago.edu
bsdadtest.uchicago.edu
cummings.bsd.uchicago.edu
cummings.uchicago.edu
dacc.bsd.uchicago.edu
dacc.uchicago.edu
drugs.bsd.uchicago.edu
familymedicine.bsd.uchicago.edu
founder.uchicago.edu
genetics.bsd.uchicago.edu
genetics.uchicago.edu
health.bsd.uchicago.edu
mbsd.uchicago.edu
mcdmail.uchicago.edu
medicine.bsd.uchicago.edu
moemail.uchicago.edu
neurology.bsd.uchicago.edu
pageit.uchospitals.edu
peds.bsd.uchicago.edu
radiology.bsd.uchicago.edu
radiology.uchicago.edu
radonc.bsd.uchicago.edu
radonc.uchicago.edu
radonc.uchospitals.edu
surgery.bsd.uchicago.edu
uhs.bsd.uchicago.edu
watson.bsd.uchicago.edu
yoda.bsd.uchicago.edu

Make sure to visit the UCM Information Security Office section of the UCM intranet for more information on this program and the Data Guardian Tip Sheet.

Thank you, and remember we are all Data Guardians.

What to do if you become aware of an information security incident? Contact the BSD ISO Team via email at security@bsd.uchicago.edu.