CCIT Cyber-Security Top Ten

The security of your online information and accounts starts with you. Here are some best practices for avoiding identity theft or worse.

1. **Never share your passwords with anyone**: whether your parents, girlfriend, boyfriend, BFF, soul-mate-for-life, random person who is totally fun to hang out with … anybody. Passwords are your keys into Mines’ systems where your identity resides (think: “Who am I at Mines?”). This includes essential personal information, your classes, your grades, your extracurricular activities, your GPA, your health records, and more. Keep it private.

2. **Do not download or upload copyrighted files that have not been legally purchased or licensed**. This includes (among other things) BitTorrent-sourced music, movies, TV shows, software, and ebooks. Such behavior always comes to the attention of Student Life in honoring the national Digital Millennium Copyright Act (DMCA) laws. Packaging malware as other kinds of content is a common way for criminals to take over your machine -- you can sometimes be grabbing more than just an illegal copy of Game of Thrones!

3. **Always run security software on your machines to offer greater protections**. Here at Mines we have Symantec Endpoint Protection software available for all students, faculty, and staff at no charge to you. Visit http://ccit.mines.edu/CCIT-Antivirus for more information.

4. **Keep your machines up-to-date** by ensuring that you have auto-updates enabled where possible. This does a good job in keeping your base operating system updated, along with your preferred web-browsers and any extensions you might use. Other packages – like iTunes, Microsoft Office, Adobe applications, and so on – have similar auto-update mechanisms. All should be enabled and used.

5. **Remember that large portions of the web attempt to track your online behavior** and where you visit. For better online privacy, recommended browsing extensions (available for the major web-browsers) include: Disconnect, Privacy Badger, and HTTPS Anywhere. These extensions keep tracking companies from piecing together your online activities.

6. **Make sure any external browser plugins you use are both truly needed and kept up-to-date**. If you don’t regularly use a plugin, set it to “Ask to Activate” or just disable it, or even uninstall it, altogether. Problematic plug-ins include packages like Java, Adobe Flash Player, Adobe Acrobat Reader (or other external PDF viewer), and Microsoft’s Silverlight, among others.

7. **When browsing email messages, instant messages, or other social-media postings, always apply common sense**. If something seems odd (a “bank” has sent this message to me from an @gmail.com address) or too good to be true (is someone really wanting to send me $25 million?), it is almost certainly an attempt to trick you. Ignore the message, delete it, and move on. This can also apply where someone you know sends you an unexpected link or attachment. Be cautious. Has this individual really sent this message or attachment to you, or has their email account been compromised by a scammer? Can you check with them via some other method of communication? Certainly, any message that asks you to “reply instantly, otherwise your account will be deleted,” or requests your username or password, is certainly a scam! CCIT will never ask for your credentials.

8. **Be careful what you share via social media**. Only post items that you truly would not mind sharing with everyone. For more private exchanges, ensure your privacy settings are configured correctly. If that post you just made ends up in front of your parents or (soon-to-be former) friend, is that okay? Items posted for everyone to see means that you could be sharing with identity thieves, who are extremely good at using and linking together all the information related to you. Identity theft is not something you want to deal with.

9. **Be careful when using shared data-sources**, like physical USB sticks, portable hard drives, and other storage devices, including cloud storage. Always have your security software running to be able to scan, and perhaps block, access to suspicious files.

10. **Don’t install random software on any of your computing devices**. Only use known software that is from a known reputable source – otherwise, who knows what extra “goodies” you’ve just installed?!

For more about cyber-security and how to keep yourself safe, visit us at http://ccit.mines.edu/CCIT-Security.