Center for Inclusive Design and Engineering (CIDE)
COLLEGE OF ENGINEERING, DESIGN AND COMPUTING
UNIVERSITY OF COLORADO **DENVER | ANSCHUTZ MEDICAL CAMPUS**

Cyber Security

Protecting Your Home Network

1. Change default password the router came with. (Lists of default passwords for pretty much every router are made readily available online.)
2. When possible, password protect every device in your home that is connected to the Internet (computers, laptops, gaming devices, TVs, refrigerators, tablets, and smartphones) – each with its own unique password.
3. Refuse to purchase devices that aren't set up for passwords.
4. Be wary of emails, especially those containing attachments or links, from unknown sources or even people you know whose accounts might have been hacked.
5. When asked by a company you do business with to "update your current information by clicking the link below" contact the company yourself to check.
6. Be wary of emails telling you to respond immediately or threaten that without an immediate response your account will be disabled.
7. Be aware that common uses of your personal computer that involve increased risks are social networks and peer to peer sharing.
8. Other activities that present a high security risk are accessing pornography and online gambling, both which should avoided or done on a separate computer limited to those functions.

Basic Security Precautions Suggested by the FBI’s Cyber Division

1. Keep Your Firewall Turned On – never set browser security setting below medium. Especially important if you have a high-speed Internet connection, like DSL or cable.
2. Install and Update Antivirus Software – prevents malicious software programs from embedding on your computer. They can be set up to update automatically, keeping up with the new viruses being created.
3. Install or Update Antispyware Technology – prevents others from peering into your activities on the computer. (Comodo Free Antivirus come with spyware protection built in.)
4. Keep Your Operating System Up to Date – periodically updated to in tune with technology requirements and to fix security holes.
5. Be Careful What You Download – never open an email message or attachment to an email from someone you don’t know.
6. Personal Information – only revel personal information such as social security and credit card numbers on secure websites. Secure, encrypted websites are identified by the “s” in the htttps:// at the start of an email address.
7. Turn Off Your Computer – “always on” renders computers always susceptible, turning the computer off puts it beyond the reach of the attacker. If you don’t need to be connected to the internet, then turn your router off.

Wireless Home Network

1. It is possible for attackers who are within range to hijack or intercept the wireless transmission.
2. Change Default Passwords – change the default password on router to make it hard for attackers to take control of your network.
3. Restrict Access – only allow authorized users to access your network. Each device connected to a network has a Media Access Control (MAC) address and you can restrict or allow access to your network by filtering MAC addresses.

4. Encrypt the Data on Your Network – every wireless network should enable encryption. Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) both encrypt information on wireless devices. WPA is more effective so specifically look for devices that support encryption via WPA.
5. Change SSID Name: The Service Set Identifier (SSID) is the name of your wireless network. Avoid using your family name, descriptive or functional names i.e. “Payroll” or “Accounting”.
6. Turn Off SSID Broadcasting – tells your wireless access point not to advertise its presence, (similar to having an unlisted phone number). The only way to connect to a WAP with SSID Broadcasting turned off is to know the SSIC name and password.
7. Install a Firewall – Ensure router’s firewall is turned on. For extra precaution, also install a firewall directly on each wireless device connected to the router (a host-based firewall).
8. Use a Decent Web Browser – Google Chrome is being called the most secure browser.
9. Don’t Trust Public Wifi – information is being sent over an unencrypted connection.
10. Never Leave Your Computer Unattended – don’t leave computer turned on if you aren’t around.

Secure Your Wireless Router

1. Change the name of your router
2. Change the pre-set password on your router – make sure your password is long and strong with a mix of numbers, letters and symbols. Use a password that is at least 8 charters in length and include a combination of numbers, letters that are both upper and lower case, and a special character. (A 6 character password with all lower case letters can be broken in under 6 minutes!) Don’t use a word that can easily be found in the dictionary.
3. Review security options – choose WPA2 if available or WPA – they are more secure than WEP option.

4. Create a guest password. – some routers allow for guests to use the network via a separate password.
5. Use a firewall – helps keep hackers from using your computer to send out personal information without your permission. Make sure firewall features are turned on.

STOP. THINK. CONNECT.

1. Keep security software current
2. Protect all devices that connect to the Internet
3. Plug & scan – USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.
4. Protect your $$ - when banking and shopping, check to be sure the site is security enabled. Look for addresses with "https://" or "shttp://" which means the site has taken the extra measure to help secure your information.
5. Back it up – protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely.

Social Media (Facebook, LinkedIn, Twitter, Google+, YouTube, Pinterest) – be careful about you share in your profile and posts.

1. Family members (with mother's maiden name)
2. Date of birth
3. Where they were born
4. Where they attend college
5. Compromise passwords
6. Malware
7. Change passwords regularly
8. Monitoring App – hack attempt monitoring (social media vault, LogDog
9. Install antivirus and security software
10. Keep business and personal social media accounts separated

11. Control you privacy settings - Even among friends, it's a good idea to avoid giving out personal details that could put your security at risk — you can't be totally sure of who has access to your posts. Set strong privacy limits on each social site, and don't add people as a friend if you don't know who they are. Don't forget to regularly check on those settings, too, and change them as necessary.
12. Be wary of public Wi-Fi – turn off network discovery and file sharing, deactivating wifi when you aren't actively using a connection, and enabling your firewall. Limit or avoid sensitive browsing – including entering passwords to your social accounts.
13. Don't engage with suspicious content - refrain from clicking any links you don't know the source of, as hackers are just as willing to pull a phishing scheme on social media as they are via email.
14. Companies mine the data we share to better market their products. Your posts, purchases, browsing history — these are tasty bread crumbs because they speak volumes about you.

Follow these tips to safely enjoy social networking:

1. **Privacy and security settings exist for a reason:** Learn about and use the privacy and security settings on social networks. They are there to help you control who sees what you post and manage your online experience in a positive way.
2. **Once posted, always posted:** Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research found that 70% of job recruiters rejected candidates based on information they found online.
3. **Your online reputation can be a good thing:** Recent research also found that recruiters respond to a strong, positive personal brand online. So show your smarts, thoughtfulness, and mastery of the environment.
4. **Keep personal info personal:** Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data, or commit other crimes such as stalking.

5. **Know and manage your friends:** Social networks can be used for a variety of purposes. Some of the fun is creating a large pool of friends from many aspects of your life. That doesn't mean all friends are created equal. Use tools to manage the information you share with friends in different groups or even have multiple online pages. If you're trying to create a public persona as a blogger or expert, create an open profile or a "fan" page that encourages broad participation and limits personal information. Use your personal profile to keep your real friends (the ones you know trust) more synched up with your daily life.
6. **Be honest if you're uncomfortable:** If a friend posts something about you that makes you uncomfortable or you think is inappropriate, let them know. Likewise, stay open-minded if a friend approaches you because something you've posted makes him or her uncomfortable. People have different tolerances for how much the world knows about them respect those differences.
7. **Know what action to take:** If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator.

Protect Yourself with these STOP. THINK. CONNECT. Tips:

- **Keep security software current:** Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats.

- **Own your online presence:** When applicable, set the privacy and security settings on websites to your comfort level for information sharing. It’s OK to limit how and with whom you share information.

- **Make your password a sentence:** A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, “I love country music.”). On many sites, you can even use spaces!

- **Unique account, unique password:** Having separate passwords for every account helps to thwart cybercriminals. At a minimum, separate your work and personal accounts and make sure that your critical accounts have the strongest passwords.

- **When in doubt, throw it out:** Links in email, tweets, posts and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.

- **Post only about others as you have them post about you.** The Golden Rule applies online as well.

For more information contact:

Center for Inclusive Design and Engineering
1201 5th St, Suite 240
Denver, CO 80204
303.315.1280 office
CIDE@ucdenver.edu
www.ucdenver.edu/centers/cide

This publication may be reproduced without the written permission of **Center for Inclusive Design and Engineering** provided that the source is appropriately credited.
Also available in: Braille, large print, audio tape, disk and Spanish formats
Made possible by NIDRR Grant #H224A40014 and
The Colorado Developmental Disabilities Council

Center for Inclusive Design and Engineering (CIDE)
COLLEGE OF ENGINEERING, DESIGN AND COMPUTING
UNIVERSITY OF COLORADO **DENVER | ANSCHUTZ MEDICAL CAMPUS**