**How to maintain Cyber Hygiene:**

**● Passwords:**  sometimes passwords are very easy to reuse from site to site, but it's important to make sure that one, you're using complexity, using the length in those passwords, and also make sure that those are unique from site to site. It is recommended to use a password manager. There's tools out there such as LastPass or Dashlane that make it very easy for you as an end-user to go and choose a very complex password, something that's very long, even you can choose 20-character passwords that are very complex, that you'll never remember, but your password manager will remember them for you.

**● System Updates:** We often see system updates. It's important to remember that the majority of those updates are because of security issues. For the most part, they only take about five minutes to install. Your computer typically then has to reboot or your phone has to reboot, and then you're off and running. You don't have to worry about that problem anymore.

**● Browsing the Internet:** When you're using your browser, it's not just the bad sites that you can go to, you could go to reputable sites that actually can expose you to malicious content as well. There are some things you can do to maintain security there. A lot of the active content that's on the Internet has been known to be utilized to exploit browsers, to push down malware down to people's systems, and compromise your own personal data or even your corporate data if you are working for a business.

**● Personal Firewalls:** In most operating systems, we can just enable a personal firewall and all inbound access is blocked so in this way we can avoid unwanted sites to be blocked.

**● Wi-Fi security:** All of us probably go to airports, even we sit on airplanes, and it's very important that we pay attention to the Wi-Fi network that we're connecting to. Maybe that it says that it's a public Wi-Fi or it's a restaurant's Wi-Fi and it has no password associated with it. Although when you connect, it's important to know that's still an untrusted network, and when you are browsing the Internet or anything you're doing on your computer, on your system, any information you're sending in the clear could be intercepted by whoever runs that network.

**● Internet of things:** Internet of things can be rather dangerous depending on what they are when they are plugged into an insecure Wi-Fi network, so everything sort of layers on top of each other. If your Wi-Fi network isn't secure in all the strong password associated with that network and you have something like a door lock or you have a camera inside your home or you have your thermostats connected to it, someone who connects to your Wifi could actually wreak havoc in your own personal lives.

**How to avoid Hacking: (Password Hygiene)**

1. Use lengthy passwords that are complex and that are not dictionary words

2. Don't repeat passwords. Maintain different passwords for different sites.

3. Use password services to stay more secure.

4. Don't maintain predictable security questions. The answers to security questions should be tricky.

**Some Social Media guide lines to be followed:**

1. **Personal vs. professional space:** Setting a clear boundary between the two spaces and knowing who will be exposed to your content can be helpful. Another thing to keep in mind is that posting inappropriate photographs or comments might cost you a job, as employers frequently research job candidates using social networking sites.

**2. Privacy:** Review your social media accounts, privacy settings and the people you’re interacting with. A good rule of thumb is to limit the number of acquaintances because they are, after all, simply acquaintances and shouldn’t have access to a lot of your personal information.

**3. Self-regulation:** Most people don’t reveal the ugly, vulnerable part of themselves on social media. As a result, lamenting about how your peers are living glamourous, perfect lives will only lead to self-pity and self-created suffering. Of course, reality checking and letting go of the illusions that dominate most social media platforms is easier said than done. Although you might absorb this information on an intellectual level, you may feel differently emotionally.

**4. Self-awareness:** social media can be a wonderful way to connect, share and reach out. However, as with anything else, there is a darker side and individuals who seek that side can indirectly put themselves in a harmful position.

**What is safe computing**:

As members of the campus community we are all responsible for the security of our shared resources. The best strategy for protecting university data is to take responsibility for your own security. Pay attention to security warnings and announcements and be aware of suspicious emails. Review the [Computing Policy](http://www.cmu.edu/policies/information-technology/computing.html) and follow the guidance below to exercise vigilance about patching, scanning your computer for viruses, and managing your password.

**Online Security:**

1. Computer and Mobile Security:

Computer Security: Update your software, Protect Personal Information, Protect passwords, **Consider Turning On Two-Factor Authentication, Give Personal Information Over Encrypted Websites Only.**

Disposal of old computers: You can ensure its hard drive doesn’t become a treasure chest for identity thieves

Disposal of mobile devices: It’s important to delete any personal information you stored on the device.

Laptop Security: A minor distraction is all it takes for a laptop to vanish. If it goes missing, all the valuable information stored on it may fall into the hands of an identity thief

Malware: Malware includes viruses, spyware, and other unwanted software that gets installed on your computer or mobile device without your consent

Online Tracking: Online Cookies

P2P File Sharing risks: To share files, like games and music, through a peer-to-peer (P2P) network, you download software that connects your computer to other computers running the same software – sometimes giving access to millions of computers at a time. This has a number of risks.

2. Networks:

Secure your Wireless Network: Taking basic steps to secure your home network will help protect your devices – and your information

VPN Apps: Wi-Fi network of your local coffee shop or airport poses some risk. Public networks are not very secure – or, well, private – which makes it easy for others to intercept your data. Some consumers have started using Virtual Private Network (VPN) apps to shield the information on their mobile devices from prying eyes on public networks.

Public wifi awareness: Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities, and other public places are convenient, but often they’re not secure. If you connect to a Wi-Fi network, and send information through websites or mobile apps, it might be accessed by someone else.

3. Common Online Scams:

* Hacked Emails
* Online Dating Scams
* Phishing
* Tech Support Scams

**What is Phishing?**

Phishing is when a scammer uses fraudulent emails or texts, or copycat websites to get you to share valuable personal information – such as account numbers, Social Security numbers, or your login IDs and passwords. Scammers use your information to steal your money or your identity or both.

**How to avoid Phishing:**

Be cautious about opening attachments or clicking on links in emails.

Do your own typing. If a company or organization you know sends you a link or phone number, don’t click.

Make the call if you’re not sure.

Turn on two-factor authentication

**How to use public computers:**

* Delete your Browsing History
* Don’t save files locally
* Don’t save passwords
* Don’t do online banking or enter credit card information
* Delete temporary files
* Remember to log out
* Pay attention to your surroundings and use common sense
* Browse in private: If you don’t want Google Chrome to remember your activity, you can browse the web privately in Incognito mode. Incognito mode runs in a separate window from your normal Chrome windows.