October 2017 Cyber Security Awareness

Security risks to consider when using open wireless networks:

1. Use extreme caution when using the free open wireless networks available in hotels, airports, and restaurants, if the connection does not require a password then it is not secure and your data may be at risk.
2. When connecting to wireless services on campus make sure that you are using the universities encrypted wireless service known as “ulsecure”.
3. Always be conscious of your surroundings when logging to ensure that someone is not looking over your shoulder or using a phone to video your keystrokes.
4. If you want to check your university email while traveling, it is best to use your cellular data plan or connect to the university’s VPN client first.
5. **EMPLOYEES ONLY:** Before traveling, install the University’s **VPN client** and test it out so that you are familiar with how it works.
6. Validate the wireless settings on your devices and ensure that they are not automatically connecting to any available wireless network.
7. For more helpful information on wireless security, please check out this **video** by the Federal Trade Commission.

Installing regular updates is equivalent to putting gas in your car, if you do not do it regularly the device will stop working properly:

8. Make sure that you check the operating system of “all” of your mobile devices and ensure that they are updated regularly with the most current software version available. Developers resolve known vulnerabilities through the distribution of regular updates. These updates are imperative to maintaining the security of all computers and mobile devices for example, cellular phones, iPads, Nooks, and Kindle readers.
9. Also, verify frequently that the applications/apps installed on your devices are updated regularly. These updates are typically available within the app store.
10. If you think your credentials have been compromised, change your password immediately or call the IT HelpDesk for assistance at 852-7997.