The summer season is here, which often means for some of us vacation and travel. When we are on the road, it is not uncommon to “check in” from your remote location. Traveling with digital devices, including laptops, cell phones, smartphones, or tablets, is often necessary in order to stay connected while you are away from the office or home. Connecting to the Internet and checking email over a wireless network are day-to-day tasks often handled on the road that can make your personal information, the College’s data, and your physical devices vulnerable. Even innocent tasks such as posting pictures on social media can make you susceptible. This month’s security awareness will focus on some reminders and tips for you to follow as you partake in your “checking in” activities whether work related or just for fun. Finally, the “In the News” section will keep you informed about some security breaches and events that have made recent headlines.

Have a wonderful summer,

Patty

While on the Road

Network Security

- If you are checking email on a public computer that is shared by others (i.e. hotel lobby), be sure to remember to logout when you are finished. Although the computer may have a “time out” feature after a period of inactivity, the length of time before it activates may be too long allowing the next user to have access to your information. Also, be cautious about the data that you access on these public computers as they may not be secure.
- Do not enter sensitive information (credit cards, bank accounts, passwords, online shopping) while connected to wireless hotspots or other unsecured networks.
- Do not install any software updates or patches while you're away from a known, secure network—updates could be malware in disguise.
- Be sure to disable broadcast services including Bluetooth, WiFi, and GPS if they are not needed. These services can be used to potentially launch attacks against your device, and can be used to locate and introduce malware.

Data Security

- Set secure passwords, codes, or screen locks for all devices so information can’t easily be accessed if the device is lost or stolen.
- Create new passwords on accounts you will need to access before you leave, and change those passwords when you get back. Avoid accessing banking or other financial sites during your trip when possible.
- Keep your data only on a University server and access it only through a secure VPN connection. Alternatively, storing documents in the cloud with services like Google Docs, DropBox, etc., to facilitate sharing and collaboration maybe a better option.

Social Media

- Be careful about what you post on social media leaving you as an open target for intruders.
- Be suspicious of emails that claim to come from social media sites. These can easily be spoofed.
- Be cautious of suspicious links or potential scams posted on social media sites. Bad guys use social media to spread their own attacks. Just because a message is posted by a friend does not mean that message is really from them.
- Most social media sites provide mobile apps to access your online accounts. Make sure you download these mobile apps from a trusted site and that your smartphone is protected with a strong password If your smartphone is unlocked when you lose it, anyone can access your social media sites through your smartphone and start posting as you.
- limit what you post. Yes, privacy options can provide some protection. However, they are often confusing and change frequently without your knowledge.
- For more information visit http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201507_en.pdf

And In the News……

- As many as 4 million people may have had their personally identifiable information compromised in a breach of IT systems at the Office of Personnel Management (OPM). OPM detected the data breach in April, but waited until June 4 to announce it publicly. http://www.federaltimes.com/story/government/cybersecurity/2015/06/04/opm-hack-intrusion-cybersecurity/28495819/
- Attackers have targeted the Canadian government's networks with a distributed denial-of-service (DDoS) attack, rendering the sites intermittently unreachable and email access sporadic. A group claiming responsibility for the attack said it was conducted to protest new laws that pave the way to increased surveillance. http://www.softwaresecured.com/2015/06/19/the-canadian-government-cyberattack-and-raising-profiles-of-simples-attacks/
- Hackers will put Internet-connected embedded devices to the test. Routers, network storage systems, cameras, HVAC systems, refrigerators, medical devices, smart cars, smart home technology, and TVs – “if it is IP-enabled, we're interested." http://www.computerworld.com/article/2918985/security/the-internet-of-things-to-take-a-beating-in-defcon-hacking-contest.html

Patricia Kahn, PhD