IT Security Bulletin

The IT Security Bulletin is sent on a quarterly basis or as needed to inform the WKU community of IT security issues and best practices. If you have any questions, please contact IT Support via one of the following methods:

- IT Helpdesk Phone: 270-745-7000
- Live Chat: http://www.wku.edu/it/chat
- Knowledge Base and Service Catalog: http://td.wku.edu/TDClient/Login.aspx
- Website: http://www.wku.edu/it
- In Person: Mass Media & Technology Hall, 3rd Floor Technical Support Services Windows

Scam Alert

Scammers Pose as IRS and FBI Agents:

Scammers are making phone calls posing as IRS and FBI agents, demanding payment for taxes. They threaten to arrest you, get you kicked out college, fired from your job, and threaten deportation of international students. The scammers demand that money be loaded on a prepaid card or sent through a wire transfer service like MoneyGram or Western Union.

The callers who commit this fraud often:

- Make the caller ID information appear as a IRS or FBI number.
- Know the last four digits of your social security number or birth date.
- May give fake badge numbers, or claim to forward you to a supervisor.
- Follow up with another call claiming to be the police or other government agency.

If you receive a call like this you can simply hang up the phone and ignore it. If you would like to report it, you can file a formal complaint with the Federal Trade Commission at www.ftc.gov/complaint. If you need to reach the IRS, you can contact them at 800-829-1040 or go to www.irs.gov.

Mobile Device Security

Mobile devices such as smart phones and tablets make it convenient to keep up with email, appointments, social media, etc. while you're out of the office.   Since mobile devices are portable, they can also be lost or stolen easily. With that in mind, you can take the following steps to help protect your mobile device:

- Protect your device with a PIN, password, pattern, etc. If someone does get your mobile device they will not be able to use it without your credentials.
- Encrypt your device. Apple iPhones and iPads are encrypted as soon as you protect them with a PIN. http://apple.co/1hCeTWk . Android devices require you to go into the settings and activate encryption. http://bit.ly/10luMYF
- Use a device locating service such as Apple iCloud's Find my iPhone, or Lookout for Android. These programs allow you to potentially find your device if it is lost or stolen and remotely wipe the data from your device.

Malware

All WKU owned computers have Symantec Endpoint Protection installed, and it is managed from a central server. This software helps to protect computers from malware, but is not 100% effective. Computer users at WKU should follow some basic guidelines to reduce the risk of installing malware on WKU owned and personally owned computers.

- Do not click on links or open attachments in email that is from someone you don't know. Even if you do know the sender, do not click on or open anything that seems out of the ordinary.
- If you follow a link and you are asked for logon information, do not enter your information. For example, if you receive an email from your bank that contains a link to log on to your account, don't do it. Go directly to your bank's website and logon there.
- Do not browse to websites that contain illegal content such as pirated software and movies/music.
- Do not install software from untrusted sources.
- Keep Windows, Adobe Acrobat, Adobe Flash, and any other software that you have installed up to date. If there is a message in your system tray reminding you to install updates, do so as soon as possible.
- If you believe that your computer has been infected with Malware, please contact the Help Desk as soon as possible. If your WKU-owned computer becomes infected with malware, it is likely that IT will perform an operating system refresh (OSR). All of your data will be transferred, but any software that you have installed yourself will have to be reinstalled and configured.

University Policy

All users of WKU Information Technology resources, including but not limited to WKU employees and students, are required to read and understand WKU's IT policies. Failure to understand and abide by these policies could not only result in disciplinary action but could expose the University or you to various liabilities. IT policies, like technology in general, evolve over time, so it is a good idea to review them regularly for changes. Please see the IT policy web site for more information:

http://www.wku.edu/it/policies/