Haselhoff, Brent

From: Hackbarth, Greg
Sent: Friday, April 7, 2017 10:16 AM
To: Faculty-All; Staff-All
Subject: WKU Official Email: IT Security Bulletin
Signed By: greg.hackbarth@wku.edu

IT Security Bulletin

The IT Security Bulletin is sent on a quarterly basis (semiannually to students) 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 methods listed at http://www.wku.edu/it/contact.

Ransomware

Ransomware is a special type of malware that takes your files hostage and threatens to destroy them unless you pay a sum of money. The ransom price can be hundreds or even thousands of dollars, and payment is usually requested in Bitcoin. Ransomware spreads like other malware, including infected email attachments and malicious websites. Once it infects your computer, it locates and encrypts files like documents and photos, making them inaccessible. The malware then tells you to pay a ransom in order to recover your files.

To avoid ransomware, practice safe computing. Do not open suspicious attachments, only visit legitimate websites, and back up your critical files. If your computer is infected with ransomware or other malware, please contact the WKU IT Helpdesk.

IRS Tax Return Scams

Tax time brings an increase in phishing scams targeting taxpayers. Some phishing emails claim to be from the IRS and tell you to click a link to receive a tax refund, respond to an IRS investigation, or make last-minute deposit changes or account updates. They may request personal and financial information, or request payment for unpaid taxes. If you receive an email that is questionable, you can check the Phish Bowl or contact the WKU IT Helpdesk. You can also forward any email that you think may be a phishing attempt to phish@wku.edu. You can learn more about phishing scams at http://www.wku.edu/it/security/sc-phishing.php.

Telephone Scams

In addition to phishing emails, scams can originate with a phone call. "Vishing" or voice phishing, is when a scammer attempts to get your personal or financial information over the phone. The scammer may also request or demand payment during the call. Two common examples are the Computer Support scam and the IRS scam.

Computer Support Scam – The scammer claims to be from a software or IT company and is calling to help with a problem on your computer. They may claim that your computer is infected with a virus and they are calling to help remove it. They may ask for payment or request that you download software that gives the caller access to your computer.

IRS/FBI Scam – The caller claims to be with the IRS or FBI and claims you have unpaid taxes. The scammer will then insist payment be made immediately or else you could be arrested. He/she will also threaten students that they will be kicked out of school or degree revoked if payment isn't made. The caller will usually request a wire transfer be made for payment.

What to Do – If you receive a suspicious call you can simply hang up the phone. To determine if the call was legitimate, you can visit the real website of the agency or company that called and contact the official telephone number. Do not call back any number given to you by the suspicious caller. You can also file a complaint with the FTC visiting https://www.ftccomplaintassistant.gov.

Faculty/Staff Email Upgrade

The faculty/staff email upgrade to Exchange 2016 is nearly complete. Soon, users will receive an official message about the migration of Mac users and the migration of public folder calendars. All official communication about the Exchange 2016 upgrade will either come from Gordon Johnson, Vice President for Information Technology, or Greg Hackbarth, Director of Enterprise Systems. If you receive email and question its authenticity, please contact the WKU IT Helpdesk.

Securing the Human Training

WKU now has SANS Securing the Human (StH) training available to all faculty, staff, and student employees. StH training teaches good computing and mobile security habits that can be beneficial to any WKU employee that is required to use a computer. To find out more about the training, visit http://www.wku.edu/it/security/training.php.

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

Please follow @WKUIT on Twitter.