Haselhoff, Brent

From: Hackbarth, Greg
Sent: Thursday, August 31, 2017 2:50 PM
To: Faculty-All; Staff-All
Subject: WKU Official Email: IT Security Bulletin

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

Contributed by Dr. Mark Ciampa

Ransomware is malware that prevents your computer from fully functioning until a fee is paid. The ransomware embeds itself on your computer in such a way that it cannot be bypassed, and even rebooting just causes the ransomware to start again. Recent variations of ransomware encrypt all your user files--documents, spreadsheets, photos, etc.--so that none of them can be opened. A screen appears telling you how to pay the ransom to receive the key to unlock them. However, often after paying the ransom a key to unlock the files is never sent or the key is useless. Although most ransoms for personal users range about $300, recently one business paid a million dollars to have their files unencrypted.

There are two defenses against ransomware: prevention and protection. To prevent ransomware be sure that your computer is updated with the latest security updates (called "patches"). Several recent ransomware versions have taken advantage of known vulnerabilities, and it only infected computers that had not been recently updated. Another prevention is to not open email attachments unless you were expecting them from a specific person. If you receive an unsolicited attachment, pick up the phone and call the sender to see if he or she did indeed send the document. Also, do not click on links in emails that you receive, even if it appears that it came from your bank or a known sender.

The second defense is protection. Regularly backup your computer files and store the backups offline (not attached to your computer). If your computer does become infected you can reinstall the files from the backup. If you use an online storage service like Dropbox or OneDrive, check with your provider to see if it has a "version" feature so that any infected files stored there can be "rolled back" to a previous state. This is important because a ransomware infection will not only encrypt files on your local hard drive but also on any other storage device to which your computer is attached.

If your computer is infected with ransomware or other malware, please contact the WKU IT Helpdesk.

Securing the Human

WKU has online security training from SANS, called “Securing the Human” (StH), available to all faculty, staff, and student employees. StH training is beneficial to any WKU employee that uses a computer. To find out more about the training, visit http://www.wku.edu/it/security/training.php.

New to WKU?

If you’re new to WKU, whether a student or an employee, be sure to check out all of Information Technology’s online resources at http://www.wku.edu/it/. There you’ll learn about the Helpdesk, Knowledge Base, and information about phishing and IT security. Also follow @wkuIT on Twitter for important system notices and phishing examples.

Phone Scams

Some scammers have been using the telephone to target victims and extort money. They often fake or “spoof” the caller ID information to imitate a trusted caller. Two common examples are the IRS scam and Computer Support scams:

- **IRS/FBI Scam -** The caller claims to work for the IRS or FBI and says you have unpaid taxes. They insist payment be made immediately through wire transfer or prepaid gift, and even threaten you with arrest.
- **Computer Support Scam –** The caller claims to be IT/computer support, says your computer has a virus or that you need to visit a website to “test the network”. Their goal is to infect your computer with actual malware, take control of your files, or access your financial information.

What to do – If you receive a suspicious call, simply hang up. You should not attempt to call the number back. Consider blocking the number in your phone settings, and if you would like to file a complaint, contact the FTC at: https://www.ftccomplaintassistant.gov.

Phishing

People are becoming increasingly aware of the dangers presented by suspicious emails that pretend to be from a trusted source (your bank, the government, a friend, or even WKU) and lure you into providing your credentials or financial information. Scammers have responded to this heightened awareness by creating more convincing, customized messages that target individual users. The FBI estimates that in the last three years more than $3 billon may have been lost to this type of scam.

If you receive an email that you are unsure of, 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.

SMiShing

SMiShing is short for “SMS phishing.” SMiShing is very similar to a phishing, but it exclusively targets mobile device users. SMiShing scammers send text messages to mobile users containing URLs or links. When a user visits the link, the device may download a Trojan horse or other virus program. The link may also present a login page that attempts to trick you into giving the scammer your credentials. If you receive a text message from an unknown user, never visit any links in the message, and do not reply. More detailed information about SMiShing can be found at https://us.norton.com/internetsecurity-emerging-threats-what-is-smishing.html.

Handling Sensitive Data

Did you know that WKU has a policy that addresses the handling of sensitive data? Sensitive data including social security numbers and credit card numbers should not be should not be sent via email or stored on the S: or P: drives. If sensitive data must be stored, it should be stored in a folder on the U: drive. If you need a folder set up for this purpose, please contact the WKU IT Helpdesk.

There is a new annual training requirement for employees who handle sensitive data. Employees with access to sensitive information in Banner, Advance, and some other central IT systems can expect to be contacted soon regarding this requirement. The new requirement helps WKU comply with our audit and cybersecurity insurance best practices. IT's full Information Security Plan can be found here.

University Policy

All users of WKU Information Technology resources 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.