WKU IT Security Bulletin

The IT Security Bulletin is sent to inform the WKU community of IT security issues and best practices. If you have any questions, please contact the IT Helpdesk at 270-745-7000, via online chat at http://www.wku.edu/it/chat, or submit a request online at http://www.wku.edu/it/helpdesk/.

Windows XP - End of Life April 8, 2014

The IT Security Office advises anyone running Windows XP to upgrade immediately. On April 8, 2014, Microsoft will end support for XP and no longer provide security patches for this operating system. Without security updates, computers running Windows XP will be vulnerable to malware and can pose a threat to other University systems.

To protect WKU IT resources, computers running Windows XP after April 8th will be removed from the network. If you have a computer currently running Windows XP, please contact the IT Help Desk now using one of the methods above.

IT Policies

All users of WKU Information Technology Resources (including but not limited to all employees and students) should read and understand WKU's IT Policies. Failure to understand and abide by these policies could not only result in disciplinary action but expose the University or you personally to various liabilities. These policies were recently updated and are found at: wku.edu/it/policies

Email Scams / Phishing Attacks

Email and Phishing scams are a way of life in the digital world we rely so heavily on today. While WKU's email filters catch and block a large number of these types of emails, they cannot all be blocked. The best defense is user knowledge and wariness. The simple rule is "Do not respond to, download files from, or click on links within any unsolicited email from a sender you do not know". If you are unsure about any email to which you are tempted to respond, contact the IT Help Desk for help verifying authenticity. Recently, there have been a number of email scams sent to WKU email users which promise money for "work from home" or "acting as a secret Walmart Shopper", etc. These typically want you to send money after they have sent you a fake check or counterfeit money order payment. These are scams that you should delete.

Phishing scams try to lure you into giving up your username, password, or other sensitive information by masquerading as someone you know and trust. They may ask you to click a link, open an attachment, or reply with your personal information.

The most common phishing attack we see is an attempt to steal WKU usernames and passwords. The email may claim to be from the IT Helpdesk and even include a WKU logo to appear more convincing. It may insist you "update" your account by clicking a link, which actually leads to a malicious login page.

If an attacker can convince you to enter your username and password, they can gain complete control of your account. They can then read your email, send malicious messages posing as you, and potentially access other University systems using your identity.

Is it Phishing?

- Be suspicious of email that is “Urgent” or requires “Immediate Action”.
- Be suspicious of attachments and only open those that you were expecting.
- Be suspicious of email from a friend or colleague that looks odd or out of place. If their email account has been compromised by an attacker, it could be used to send phishing email.
- Examine from “From:” email address. Often the “Display Name” will say something that looks familiar, but the underlying email address (with the “@” sign) is obviously foreign or nothing you recognize.
- Examine the underlying URL on any links. Regardless of how the link is labeled in the email, the underlying link on a Phish email will usually not be a “wku.edu” address.

If you receive a phishing email, you should delete it. To notify IT, you can forward the email to phish@wku.edu.

Note: If WKU IT sends out any email about IT Accounts, we will always instruct you to call the IT Help Desk if you have any doubts about the authenticity of the email and we will never directly ask for User IDs or passwords.

Example of a Recent Phishing Scam

==========

Subject: Microsoft Outlook 2014 Update
From: WKU Help Desk
Attention: Helpdesk Service Center requires your immediate re-activation of your Email account. This is to upgrade email account to Microsoft Outlook 2014. Inability to complete this procedure will render your account inactivate. Activate by completing the survey procedure. CLICK HERE to activate your account.

IT-Helpdesk Service.

==========