WKU IT Security Bulletin

About this Bulletin
The IT Security Bulletin is sent to inform the WKU community of IT security issues and best practices. If you have any questions about this bulletin, call the IT Help Desk @ 745-7000 or email ITSecurity@wku.edu.

Security is Everyone's Responsibility
While WKU IT strives to provide secure and safe IT computing resources and services, it is the responsibility of everyone to keep current with safe computing best practices and to conduct business in a secure and vigilant manner. Visit the IT Security website at wku.edu/it/security for more information and read these IT Security Bulletins when issued.

Sensitive Information Handling
All University employees are required to understand their responsibilities for handling and protecting sensitive information. Please refer to the IT Sensitive Data Protection Policy for further information: http://wku.edu/it/policies/documents/sensitive-data.pdf .

Safe Computing Tips – Downloading files
Download files only from trusted sources. Files from untrusted sources may contain viruses or other malicious programs. "Free" software hosted on file-sharing programs and untrusted websites often contain spyware and may have adverse effects on your computer.

Phishing Attacks
Because so many people use and depend on email, phishing has become one of the primary attack methods used by cyber criminals. Phishing messages try to lure you into giving up your username, password, credit card details, or other information by masquerading as someone you know or trust. They often request that you click on a link, open an attachment, or reply to the email with your personal information.

Phishing email can look very convincing and appear as if it were sent from a friend, your bank, or an online store. It may even impersonate official WKU email and link to a fake WKU login page. In fact, WKU passwords have been the target of multiple phishing attacks.

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 with significant grammar and spelling mistakes.
- 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. You can also 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: Email Security Update

From: WKU Help Desk

Attention: There has been an automatic security update on your email address. CLICK HERE to complete the update. Please note that you have 24 hours to complete this update or you may lose access to your Email Box.

==========

In the News

Salem State University Says Database Was Breached

The Boston Globe reports that the personal data of 25,000 current and former staff members and student workers at Massachusetts' Salem State University may have been compromised after a virus accessed a university human resources database.

http://bostonglobe.com/metro/2013/03/15/virus-accesses-salem-state-university-database-containing-personal-information-for-thousands/S7AJvP1k7Zb7lLzSqhm7pN/story.html

If you have any questions, please contact the IT Help Desk at (270) 745-7000