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/.

Sensitive Data Protection - Storage

Sensitive data should be stored in as few places as possible and duplicated only when necessary. Unless absolutely necessary, data should be stored on central administrative systems only.

Do not store sensitive data on mobile or external storage devices such as CD, DVD, floppy disks, laptops, USB drives, PDAs, cell phones, or any other device that can easily be lost, stolen or compromised.

Do not send, receive, or store sensitive data using email. Email is convenient, but it is not a secure method of sharing sensitive data. If it is necessary to transfer a file with sensitive information, use the WKU Send Files Application. http://www.wku.edu/it/security/send_files.php

Do not store sensitive data such as credit card or social security numbers on departmental shared drives.

If you have a need to store sensitive data, please contact the IT Helpdesk to request a secured network drive.

For more information on protecting sensitive information, please refer to the Information Security Plan found at http://www.wku.edu/it/policies.

Email Scams & Phishing Attacks

Phishing scams try to lure you into giving out 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 may even include a WKU logo to appear more convincing. It may state that you must "update" your account by clicking a link, which actually leads to a malicious login page. Please see an example of such a message at the bottom of this bulletin.

If an attacker can convince you to enter your username and password, the attacker can gain complete control of your account. The attacker 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 you are expecting.
- Be suspicious of email from a friend or colleague that seems odd or out-of-place. If his/her email account has been compromised by an attacker, it could be used to send phishing email.

- Examine the “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 not something you recognize.
- Examine links in the email that you are asked to click. Links in a phishing email will usually direct you to a site other than “wku.edu”.

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 an email concerning IT Accounts, we will always instruct you to call the IT Help Desk if you have any doubts about the authenticity of the email. We will never directly ask for user IDs or passwords.

Example of a Recent Phishing Scam

==========

Subject: : IMPORTANT - A Warning Regarding Password Security
From: WKU IT Division

WKU IT Division

Attention:

Due to the recent Virus attack on our database, we are currently upgrading our database and all email accounts need to be verified. “IT HELP DESK” will automatically upgrade to the latest anti-spam version. You are required to complete upgrade within the next 72 hours so that your account can be upgraded or have your account deleted from our database to stop the spread of this virus.

To ensure your email(s) remain active, please confirm the email address and password we have for you is accurate in the link below form.

http:// CLICK HERE

Thank you for your time.

Western Kentucky University IT Division

==========