IT Security Bulletin

The IT Security Bulletin is sent on a quarterly basis or as needed 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

Sensitive data such as credit card numbers, social security numbers, and driver's license numbers should never be sent via email, even for business purposes. Also, please do not store sensitive data on local storage devices or on the WKU shared drives and ***never*** on a web server. We regularly scan the S: drive for certain types of sensitive information and move any such data to a quarantine area. If you discover your files have been quarantined, please contact the WKU Helpdesk via one of the methods above. If you believe you have a need to store sensitive data or securely share access with a limited number of faculty/staff at WKU, please contact the Helpdesk to discuss potential options for doing so including the use of the U: drive.

All university employees are required to understand their responsibilities for handling and protecting sensitive information, but this is particularly important for employees who handle or process information or documents that contain personally identifiable information (PII – SSN, birthdate, etc.). Please regularly review any stored sensitive data and delete it when it is no longer needed. The recent Anthem data breach is an unfortunate example of damage to a company and other impacted individuals that can result from a breach of sensitive data. Security is everyone's responsibility. Please stay vigilant and informed.

IT Policies

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

MyStuff

Some changes are being made to further secure your personal and shared files, available through MyStuff. Now, rather than the system relying solely on NetID and password credentials, you will be asked to provide additional information to verify your identity. Since MyStuff is accessible anywhere on the Internet, these measures will help ensure that our users' files remain protected even if their NetIDs and passwords have been compromised.

Windows Server 2003 EOL (End of Life)

After July 14, 2015, Microsoft will no longer release security patches for Windows Server 2003 because the operating system has reached its End Of Life (EOL). WKU IT will decommission all Server 2003 servers from the datacenter by this date, but there may be some on WKU's network that IT does not manage. If you operate a server that runs Windows Server 2003, please make plans to upgrade it before July 14. After July 14, IT may deny network access to machines running Windows Server 2003. If you have any questions, please contact the IT Helpdesk.

Malware

Malware, short for malicious software, is an umbrella term for spyware, adware, viruses, worms, ransom-ware, and Trojan horses. Malware can be used to disrupt computer operation, gather data including account credentials, gain access to a computer system, attack a remote system, or distribute email spam.

Malware is generally installed by executing a downloaded file or by visiting a website with malicious code via Java, ActiveX, etc.

All WKU-owned computers have Symantec Endpoint Protection installed, and it is managed from a central server. This software helps to protect computers from malware, but no endpoint protection is 100% effective. Computer users at WKU should follow some basic guidelines to reduce the risk of installing malware on WKU-owned and personally-owned computers.

- Do not click on links or open attachments in email that is from someone you don't know. Even if you do know the sender, do not click on or open anything that seems out of the ordinary.
- If you follow a link and you are asked for logon information, do not enter your information. For example, if you receive an email from you bank that contains a link to logon to your account, don't do it. Go directly to your bank's website and logon there.
- Do not browse to websites that contain illegal content such as pirated software, movies, and music.
- Do not install software from untrusted sources.

If you have any questions or concerns about software, files, or attachments that you have downloaded or plan to download, please contact the IT Helpdesk.

Phishing Scams

Members of the WKU community sometimes receive email from outside entities who pose as a legitimate companies or organizations (like PayPal, Anthem, or even the IRS) in order to obtain your login credentials or personal information. Phishing scams are a persistent threat to our own WKU email as well, as hackers try to obtain your WKU login credentials so that they can use your account for further phishing activity. IT is able to filter an overwhelming majority of phishing attempts before they reach your WKU or Topper mailboxes, but once a WKU account is compromised the messages become much more difficult for IT to block. An example of this is an email that went out recently from a compromised WKU email account (hyperlink has been removed):

> **Dear Webmail User,**
>
> **We hereby announce to you, that your email account has exceeded its storage limit. You will not be unable to send and receive mails and your email account will be deleted from our server. To avoid this problem, you are advised to fill the form: click HERE**
>
> **Web Provider.**

In the message, a click-able link directs you to a site that asks for your login information. Such sites often contain WKU logos in order to appear legitimate. Use caution whenever you are directed to enter your WKU credentials after following a link in an email. WKU will never send an email of this type without providing a way for you to verify its authenticity, and if you ever have a question about the origin of a message you may always forwarding the email to itsecurity@wku.edu. It is never advisable to login to a website that you reached from a link in an email. It is far better to type the address into a browser and then login. You can find additional tips for spotting phishing attempts at http://www.wku.edu/it/security/sc-phishing.php.