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 IT Support via one of the methods listed at www.wku.edu/it/contact.

Securing the Human

WKU now has SANS Securing the Human (StH) training available to all faculty, staff, and student employees. StH training can be beneficial to any WKU employee that is required to use a computer. To find out more about the training, visit http://www.wku.edu/it/security/training.php.

Incident Response

Do you know how to report an IT security incident? Check out the IT Security site (http://www.wku.edu/it/security) for the new "Report an Incident" link so you will be prepared if you need to report an incident in the future. It is important to report IT security incidents as soon as possible.

Credit Card Merchants

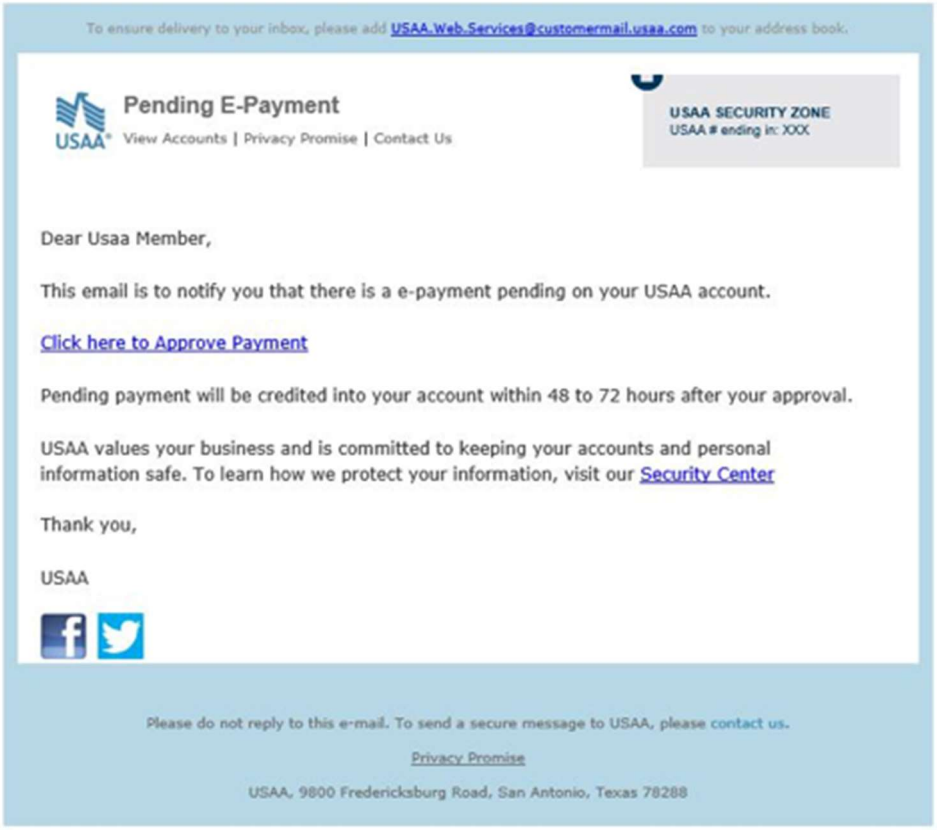
If your department or organization accepts credit cards, you are responsible for familiarizing yourself with WKU policies and PCI standards. WKU policy 3.3101 directly discusses credit card merchants. PCI standards can be found at https://www.pcisecuritystandards.org/.

Phishing

Phishing scams continue to be a security threat to WKU as well as other organizations. Scammers attempt to collect your username, password, or financial information by directing you to a link from an email message or by calling you on the phone. WKU IT will never ask you for your password. A common tactic employed by scammers is to make their email message appear to be from WKU IT and warn you of a problem with one of your accounts, such as that your mailbox is full, has been compromised, or is being moved. Still other scams appear to be from companies with whom many people have accounts, such as PayPal, eBay, Amazon, or large financial institutions. Be wary of any link you are asked to click in an email that directs you to a web form asking for login credentials or other personal information. If you suspect an email may be phishing, please forward it to phish@wku.edu.

Example of recent phishing scam:

From: "USAA" <mons@umit.maine.edu>
To: "Recipients" <mons@umit.maine.edu>
Subject: USAA: Pending E-Payment
Date: Wed, May 11, 2016 7:49 PM



You can learn more about phishing scams here: http://www.wku.edu/it/security/sc-phishing.php

Spam

WKU IT's SpamControl system blocks many millions of messages containing harmful or unwanted content. Classifying spam is complex, but the process is based on rules such as whether a message is from a specific sender address or domain, contains certain keywords or content, contains certain types of attachments (including viruses), etc. Based upon these rules, messages are assigned a score which determines whether or not they are blocked (4.5 or above), allowed with a [??SPAM??] subject tag (under 4.5 but at or above 2.5), or allowed (under 2.5). Any message's score may be seen by viewing the Internet headers of the message in your email client.

You can adjust your own spam settings, whitelist or blacklist certain senders, or adjust your account's spam scoring threshold by creating an account on https://spamcontrol.wku.edu. Your spam scoring settings are located in the Spam Settings area

under Preferences. If you have any questions about how to access SpamControl, contact the IT Helpdesk by one of the methods listed above.

Spam stats since March 1, 2016:

	Blocked: Spam	Blocked: Virus	Allowed: Tagged	Allowed
March	3,285,745	28,731	63,793	2,038,705
April	3,736,151	5,356	83,027	2,556,558
May	5,127,081	5,608	71,952	2,220,416
Total	**12,148,977**	**39,695**	**218,772**	**6,815,679**

University Policy

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/