IT Security Bulletin

The IT Security Bulletin is sent on a semiannual 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 http://www.wku.edu/it/contact.

Protecting Your Critical Email Password

Contributed by Dr. Mark Ciampa

Think for a moment about that password protecting your email account. Just how important is it? Most users would probably shrug their shoulders and say, "My email password is not really that important. Hey, if somebody wants to break into my email account and read my messages, then go ahead!" But your lowly email password has become very important today.

Consider for a moment your "digital footprint" on the Internet. For the vast number of online accounts that you have – social networks, school or work accounts, financial institutions, and e-commerce sites, just to name a few – increasingly they are using your email account as your username. In addition, that same email account is used if you forgot the password or want to change the password to one of these accounts: a password reset link is typically sent directly to your email account. If an attacker could get into your email account, she could then go to your online bank account, have a password reset sent to your email account, and then change the password to whatever she wanted. The attacker could then enter your bank account and transfer all your hard-earned money overseas. And she could do the same for all of your other accounts. So, if an attacker can uncover just your email account password, it could result in a digital disaster. Thus, your single email account "underpins the security" of your entire digital footprint.

OK, so our email password today is very, very important. What can we do to protect ourselves? There are two defenses. One defense is to use multifactor authentication: sign up to have a code sent to your cell phone whenever you log into an account that must be entered along with the password. The second defense is to use a password manager to store and retrieve strong passwords for all of your accounts.

If you have any questions about account or password security, please contact the WKU IT Helpdesk.

Alteryx Data Breach

It seems that every few months we learn about new data breaches. In December, Alteryx left an unsecured database exposed to the Internet, and about 123 million records were stolen. These records did not contain social security or credit card numbers, but they did contain addresses, demographics, income/financial information, and even information about children living in the household. Information

from this breach alone is probably not enough to steal someone's identity, but when added to information already leaked from other major breaches, it may be enough to enable a criminal to steal someone's identity.

It is important to check your credit regularly for abnormalities. You can do so via www.annualcreditreport.com. If you believe that you're a victim of Identity Theft, follow the steps outlined by the FTC at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

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.

New to WKU?

Be sure to check out all of the Information Technology resources at WKU including a Helpdesk, Knowledge Base, and information about phishing and IT security on our website at http://www.wku.edu/it/. Also follow us on Twitter @wkuIT.

Spam

Spam is unsolicited bulk email, typically sent to a large number of recipients. Spam can be harmless (albeit annoying) marketing emails, or it can be of a malicious nature. Phishing is a type of spam that encourages the recipient to give up their account credentials so that a malicious actor can gain access to various resources. Some spam may also include attachments that contains viruses.

At WKU, we utilize Barracuda Spam Firewalls that block most spam and viruses, but no spam filter is 100% effective. If you receive an email and question its legitimacy, you can check the Phish Bowl or contact the WKU IT Helpdesk. You can also forward any email that you think may be a phishing attempt to phish@wku.edu. You can learn more about phishing scams at http://www.wku.edu/it/security/sc-phishing.php.

University Policy

All users of WKU Information Technology resources 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 at http://www.wku.edu/it/policies/.