ITS Security Bulletin, Fall 2018

The Information Technology Services (ITS) Security Bulletin is distributed semiannually or as needed to inform the WKU community of technology-related security news and best practices. If you have any questions, please contact ITS via one of the methods listed at www.wku.edu/its/contact.

New to WKU?

Please follow @wkuITS on Twitter and visit our website at www.wku.edu/its for links to major systems and to find out how to get support. If you need training, please visit our training site at www.wku.edu/its/training.

Password Extortion

A new email scam attempts to extort money from you by sending you one of your previously used passwords. On the dark web, scammers trade password lists from previously hacked sites like LinkedIn, Yahoo, etc. By showing you a familiar password, they hope to scare you into thinking that they know your current password and/or have compromising information or even a webcam video of you. The scammers then demand money, Bitcoin, or gift cards in exchange for not publicizing the information. Because hacked password lists are commonly distributed on the Internet, you should a different password for every site you visit. Never use the same password on two different sites, regardless of how strong the password is. If you need help remembering multiple passwords, investigate password management software such as LastPass or 1Password; there are many quality options. To see if your password may have been exposed in the past, you can check out https://haveibeenpwned.com/.

Facebook Messenger Scam

The FBI has released an article related to a current Facebook Messenger scam. The scam starts with a potential victim receiving a message through Facebook Messenger with a link to what is supposed to be a video of the victim. Sometimes the scammer claims that they have found a way to get money or other goods. It may be tempting to click on these links because they appear to be from a friend, but be aware that your friend's account may have been hacked, or someone may be contacting you that has your friend's picture and name. The full article can be found here: https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/fbi-tech-tuesday-building-a-digital-defense-against-facebook-messenger-frauds

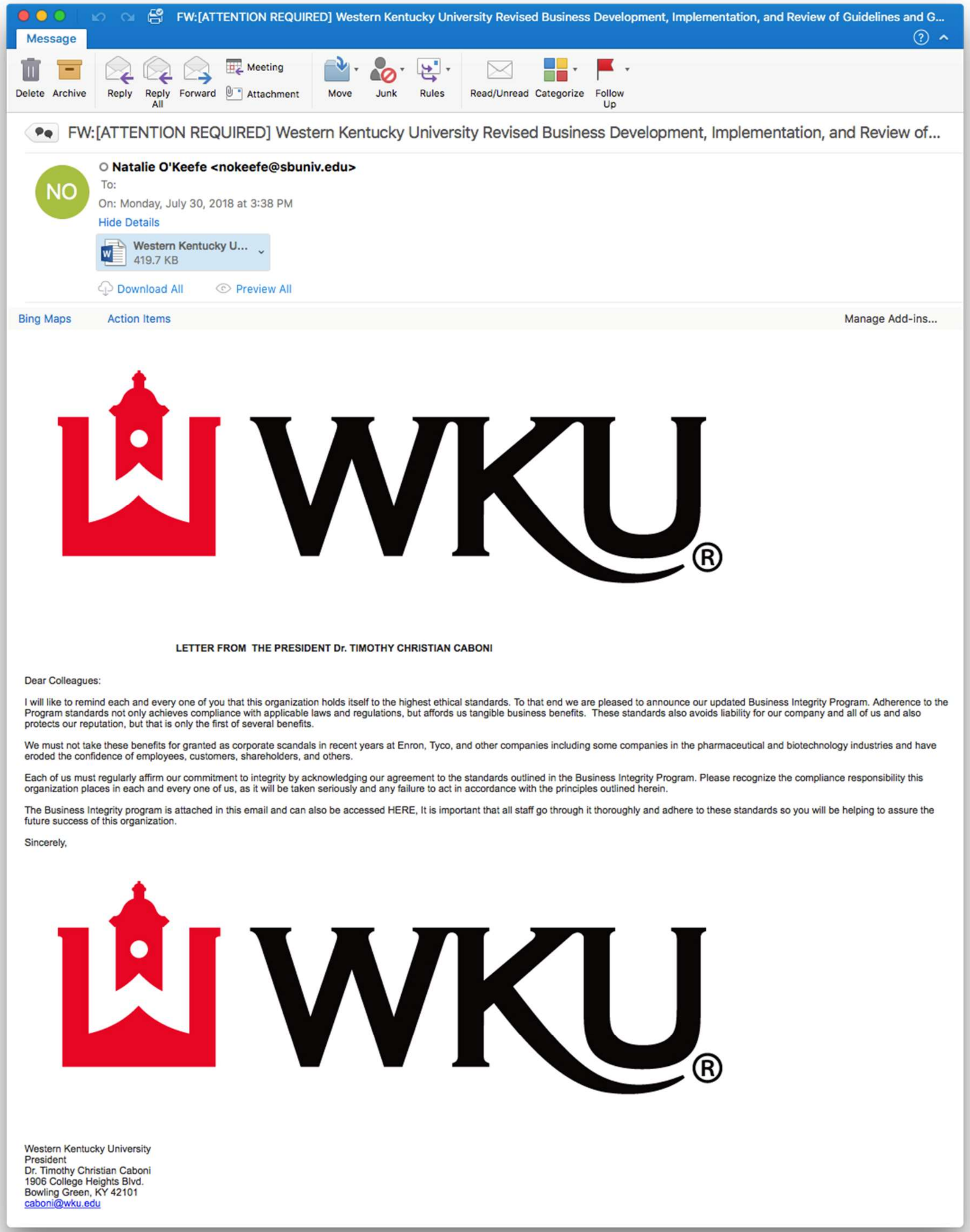
---

Privacy

Keeping sensitive information about students and employees of WKU private it extremely important. WKU is subject to several regulations including: FERPA and GLBA. Both of these regulations are covered in WKU's Information Security Plan.

Phishing

Phishing is a persistent threat to WKU and to organizations everywhere. Recent phishing campaigns targeting WKU have become much more sophisticated than those seen previously. For example, the email below appears to be from Dr. Caboni:



FW:[ATTENTION REQUIRED] Western Kentucky University Revised Business Development, Implementation, and Review of Guidelines and G...

FW:[ATTENTION REQUIRED] Western Kentucky University Revised Business Development, Implementation, and Review of...

○ Natalie O'Keefe <nokeefe@sbuniv.edu>
To:
On: Monday, July 30, 2018 at 3:38 PM

Western Kentucky U...
419.7 KB

LETTER FROM THE PRESIDENT Dr. TIMOTHY CHRISTIAN CABONI

Dear Colleagues:

I will like to remind each and every one of you that this organization holds itself to the highest ethical standards. To that end we are pleased to announce our updated Business Integrity Program. Adherence to the Program standards not only achieves compliance with applicable laws and regulations, but affords us tangible business benefits. These standards also avoids liability for our company and all of us and also protects our reputation, but that is only the first of several benefits.

We must not take these benefits for granted as corporate scandals in recent years at Enron, Tyco, and other companies including some companies in the pharmaceutical and biotechnology industries and have eroded the confidence of employees, customers, shareholders, and others.

Each of us must regularly affirm our commitment to integrity by acknowledging our agreement to the standards outlined in the Business Integrity Program. Please recognize the compliance responsibility this organization places in each and every one of us, as it will be taken seriously and any failure to act in accordance with the principles outlined herein.

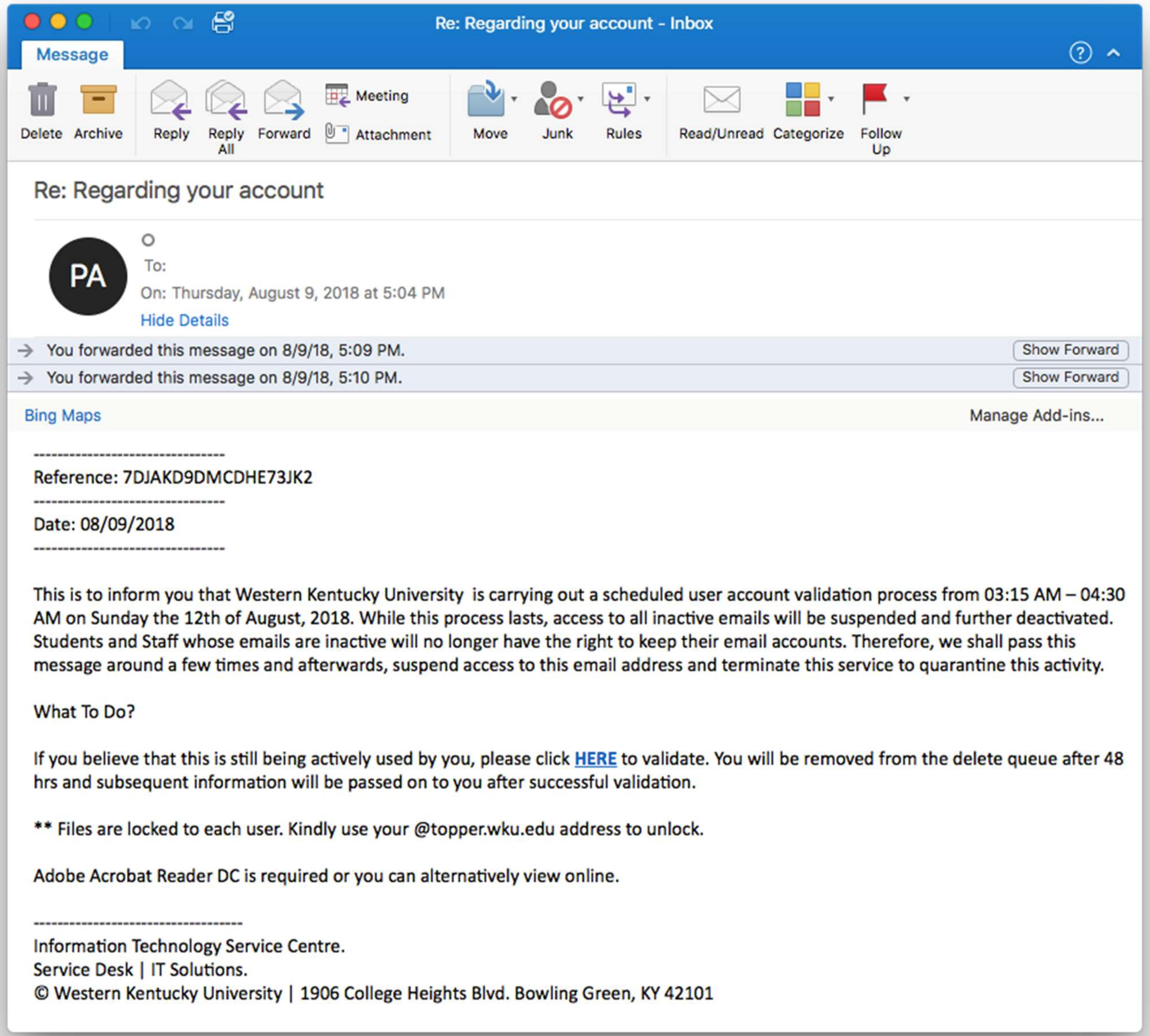
The Business Integrity program is attached in this email and can also be accessed HERE, It is important that all staff go through it thoroughly and adhere to these standards so you will be helping to assure the future success of this organization.

Sincerely,

Western Kentucky University
President
Dr. Timothy Christian Caboni
1906 College Heights Blvd.
Bowling Green, KY 42101
caboni@wku.edu

At first glance, this email looks like an important message from Dr. Caboni, and his email address even appears in the text of the message, at the end. However, upon closer inspection, the “From:” field or message header reveals that the email is from “sbuniv.edu” (a hacked account at Southwest Baptist University), which is obviously not affiliated with WKU or Dr. Caboni. The message’s attachment contains a link to a so-called “secure document.” After clicking the link, you are prompted for your username and password. Once you provide this information, the phishers have your account information and can access everything that you can access with your NetID (Email, TopNet, Blackboard, etc.).

Another recent example actually originates from a compromised WKU email account, making detection more difficult. In this example the sender's WKU address has been redacted to protect the individual's privacy. The email looks like:



Re: Regarding your account

To:
On: Thursday, August 9, 2018 at 5:04 PM

You forwarded this message on 8/9/18, 5:09 PM.

You forwarded this message on 8/9/18, 5:10 PM.

Reference: 7DJAKD9DMCDHE73JK2

Date: 08/09/2018

This is to inform you that Western Kentucky University is carrying out a scheduled user account validation process from 03:15 AM – 04:30 AM on Sunday the 12th of August, 2018. While this process lasts, access to all inactive emails will be suspended and further deactivated. Students and Staff whose emails are inactive will no longer have the right to keep their email accounts. Therefore, we shall pass this message around a few times and afterwards, suspend access to this email address and terminate this service to quarantine this activity.

What To Do?

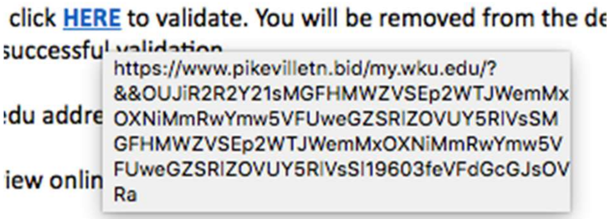
If you believe that this is still being actively used by you, please click HERE to validate. You will be removed from the delete queue after 48 hrs and subsequent information will be passed on to you after successful validation.

** Files are locked to each user. Kindly use your @topper.wku.edu address to unlock.

Adobe Acrobat Reader DC is required or you can alternatively view online.

Information Technology Service Centre.
Service Desk | IT Solutions.
© Western Kentucky University | 1906 College Heights Blvd. Bowling Green, KY 42101

The message looks convincing because it is "from" a wku.edu address. The easiest way to detect that this is phishing is to hover over the "HERE" link, where you'll see that it links to a site that is not affiliated with WKU:



click HERE to validate. You will be removed from the de
successful validation
edu addre
iew onlin

```
https://www.pikevilletn.bid/my.wku.edu/?
&&OUJiR2R2Y21sMGFHMWZVSEp2WTJWemMx
OXNiMmRwYmw5VFUweGZSRlZOVUY5RlVsSM
GFHMWZVSEp2WTJWemMxOXNiMmRwYmw5V
FUweGZSRlZOVUY5RlVsSl19603feVFdGcGJsOV
Ra
```

These links often lead to fake, look-a-like versions of our Outlook Web Access (OWA) or MyWKU pages.

If you receive a questionable email, here are some things to note:

- Check the WKU Phish Bowl at www.wku.edu/its/phishbowl. Many common phishing messages appear there.
- If you still have questions, please contact ITS at www.wku.edu/its/contact.
- If you accidentally respond or have reason to believe your email has been compromised, please reset your password immediately at www.wku.edu/its/accounts/manage and then contact ITS.
- ITS will never send you an email asking for your credentials. Be especially cautious when you receive messages from ITS claiming to be urgent, and contact us if you have questions.
- President Caboni and other administrators do not send "secure documents" to the WKU population. Be extremely suspicious of any email from the administration that contains a link or document that asks for a login.

If you've ever wondered why hacked email accounts are valuable to scammers, check out the following article: https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/

University Policy

Users of WKU technology resources are required to read and understand ITS 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. ITS policies, like technology in general, evolve over time, so it is a good idea to review them regularly for changes. Please see the ITS policy web site for more information at http://www.wku.edu/its/policies/.