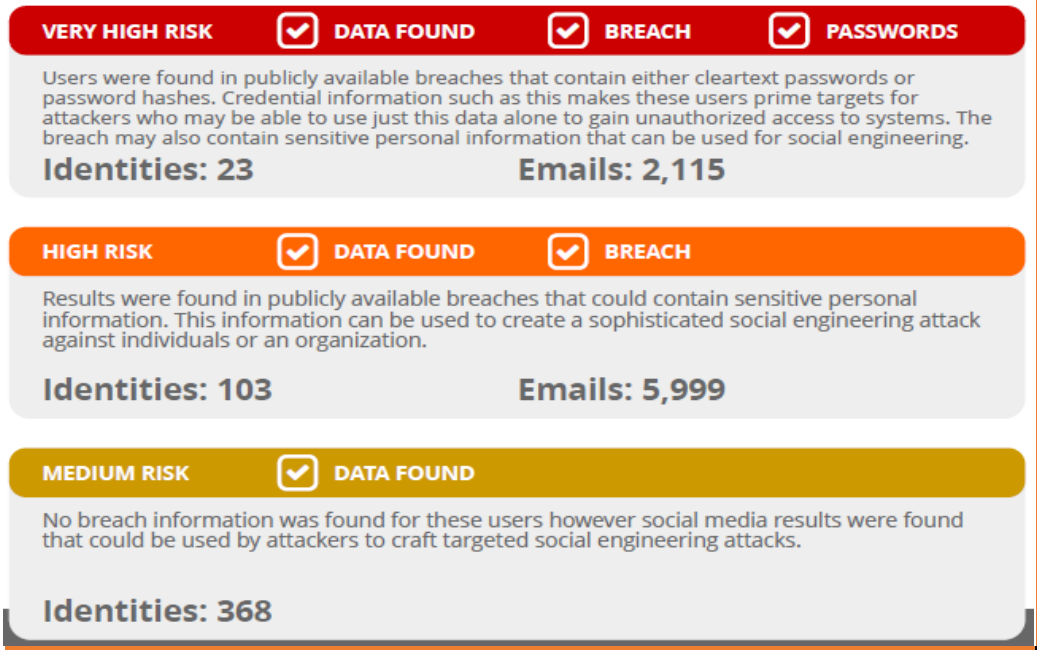

UTHSC G.U.A.R.D.

October 2017

IN THIS ISSUE

Do You Know if Your Email Address is Safe?

by Chris Madeksho, Information Security Coordinator

Recently, UTHSC's Information Security Team collaborated with a vendor (KnowBe4) and requested a report that determines how many of our UTHSC email addresses were found in known breaches and how much of a risk those emails present to our security.

KnowBe4 provided a report after searching known breaches for email addresses from "@uthsc.edu". They found 494 identities (email addresses) were found in 58 unique breaches. You read that right – **494 of our email addresses are part of known breaches** of information. A total of 8,114 emails were found that had anything from data that could be used in a social engineering attack to credential information just displayed there in the email.

The most critical of these finding is 23 identities that were found that had information, such as passwords, clearly identified in the emails. These users would be easy targets for attackers, as they do not need to do any more research or social engineering to get that user's credentials. Above is a breakdown of what they found.

What can you do to protect your information? First of all, do not use your UTHSC email address as your personal email. It is very easy to sign up for a free email address at Gmail, Yahoo or other sites that can be used for personal use.

You can check to see if your email has been reported as part of a breach. Visit https://haveibeenpwned.com and type out your email address. The results will show you if you are part of a breach, and if so, which breaches. This website is a free tool that can be used for any email address. Check all the email addresses your family and friends have. Without knowing where you are vulnerable, it is hard to protect yourself.

If you have been part of a breach, the best recommendation is to change your password and your security questions. For more information, please contact the Information Security Team at itsecurity@uthsc.edu or (901) 448-1880.

Data Breaches and Our Emails

Learn about how our UTHSC email address are part of data breaches and how to check your email address

Email Encryption is Here

Learn how to encrypt your UTHSC email message that hold sensitive information

Email Encryption at UTHSC

by Vikki Massey, Director Project Management Office and Chris Madeksho, InfoSec Coordinator

In the past, sending protected or confidential data via UTHSC email was prohibited for security reasons. However, you now can encrypt individual UTHSC emails and transmit sensitive information to anyone with the confidence that only the recipient(s) will be able to decrypt and read the message.

Encryption is easy to enable on a case-by-case basis. All you have to do is add the word **encrypt** anywhere in the subject line of an email sent from your UTHSC account, and you are set! No special interface or website is needed for sending, and the message notification goes directly to the recipient's inbox for easy retrieval.

In order to send an encrypted email using your uthsc.edu email account, add the word **encrypt** anywhere in the Subject line of your email, along with your regular Subject line information. (Words that contain "encrypt" in them, such as "encryption" or "encrypted" will not trigger the encryption process.)

Please note that encryption can be guaranteed only for UTHSC email sent via the UTHSC email router. Unless you have deliberately gone into your email software and changed the router for your UTHSC email, you are using the proper router that will allow for encrypted UTHSC emails.

Recipients of encrypted emails will receive a message in their UTHSC email inbox notifying them of the encrypted email and stating the sender's email address. The notification will contain an attachment ("message.html") that provides instructions for accessing the actual encrypted message.

People with a Microsoft account (whether personal or business/academic) will use those credentials to sign in and access the message. (That means UTHSC and UTK members will use their NetID and password.) People without a Microsoft account must choose the option to receive a passcode, which is delivered to their email inbox.

If the recipient chooses to respond to an encrypted message, encryption will continue to be enabled on the entire email thread as long **as the recipient replies from the screen where the encrypted message is displayed**. This applies even if the Subject line is changed. Other recipients of the email will use the same process to view the encrypted information as described above.

For more information about email encryption in the UTHSC email environment, visit https://uthsc.edu/its/information-security/email-encryption.php or contact the Information Security team at itsecurity@uthsc.edu or (901) 448-1880.