**What you should do as the HSC Information Security team works to protect data**

**News for team members** University of North Texas Health Science Center **Tue, Mar 10, 2020**

**Your HSC Information Security team is taking new steps to protect your data.**

Guiding the process is the HSC Information Technology Steering Committee, composed of high-level institutional leadership.

This mission is more critical than ever as we strengthen our partnerships with research agencies including those administered by the federal government, and with additional health-oriented organizations.

Often, these agencies and organizations require strict access control.

Security enhancements incorporate best practices, and some will require your cooperation while others will be invisible to users.

**HSC’s new steps include:**

* A return to a 90-day password expiration period, rather than the current 365 days. You will not be asked to change your password immediately. As in the past, you’ll receive notifications as your password expiration date nears. Once changed, your password will expire every 90 days.
* Changes in the baseline security configurations of our workstations. These will be done automatically, with some noticeable and others not.
* Changes in HSC network configurations – already under way.

**What you need to do:**

* **Please leave your workstation and/or laptop powered on.** Security-related updates are set to download while your workstation is turned on and available on campus. If an update is distributed when your computer isn’t available, it will run the next time your device is turned on.
* **Some updates will force your computer to reboot.** Don’t be alarmed if you are prompted to log in from scratch when you turn on your computer after an overnight or similar “off” period.
* After updates, you may notice that some programs or software are not available. **Please contact the HSC Helpdesk,**[**helpdesk@unthsc.edu**](mailto:helpdesk@unthsc.edu)**, for assistance.**

**More tips to help you protect your digital data:**

* **Avoid phishing attacks:** <https://www.unthsc.edu/Information-technology-services/wp-content/uploads/sites/55/Phishing2018.pdf>
* Please do not use your UNTHSC email address for personal business. Such use increases our accounts’ vulnerability to hacking.
* **Prevent identity theft:** <https://www.unthsc.edu/Information-technology-services/wp-content/uploads/sites/55/IdentityTheftandInternetScams2018.pdf>
* **Create a Cyber Secure Home:** <https://learnhsc.bridgeapp.com/learner/courses/07d402a4/enroll>
* **Additional tips and training:** <https://www.unthsc.edu/Information-technology-services/information-security/training-and-awareness/>

***Please send questions to [ email addresses ]***