How many times have you updated the Operating System (OS) on your device this year? A number of security incidents are caused by flawed operating systems. Others caused by not updating applications. As these issues are revealed, vendors release patches, or fixes, to protect security holes: by updating your operating system you ensure it has been properly updated.

Updating your OS is perhaps the most critical and simplest of all the methods for securing your computer. Nearly all modern operating systems have some easy method to make sure you have the latest version of all of your operating system software. Make sure to enable automatic updates whenever possible.

Standardization is achieved when a common based-structure is implemented for the University, faculty, staff and students. Selected from specific vendors, the base hardware platform and software suite can be modified to fit particular needs by building on the common base. Standardization does not require every faculty, staff, administrator and student to have the exact same equipment.

Standardization brings about a seamless, streamlined structure for Information Technology Services. It gives ITS entities like the Help Desk, IT Security, and Systems an advantage when remediating computer issues and addressing your individual computing concern. With computer standardization, your workday could flow more efficiently, saving you time and frustration.

IT personnel are trained to troubleshoot issues based on a particular operating system. Once a single issue is remediated, that particular solution can be used for all similar operating systems thereafter; eliminating confusion and long wait time for computer fixes.

Some may attempt to avoid updating their OS, so their current applications can function properly. ITS understands your concerns and will accommodate those who need special exceptions regarding OS standardization.

ITS will be rolling out the standardization in upcoming months. All UTHSC faculty, staff, and student body will be notified in a timely fashion. ITS will provide continuous communications, details, timelines, and all other pertinent information. UTHSC ITS is transparent in its functioning roles. The UTHSC community are welcome to ask questions regarding any ITS issue or decision.

Do you still have questions about computer standardization? Contact the IT Security Team at (901) 448-1579 or itsecurity@uthsc.edu.
Using your UTHSC email with a third party account or a non-UT email account can open the door for SPAM/Phishing. Phishing is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords, credit card numbers and Social Security numbers. Your email address is directly linked to your UTHSC Net ID. Your University NetID is exclusive to the usage of only the internal university systems.

Using your UTHSC email to gain student access to commercial merchant sites such as Amazon.com, and other sites that give student incentives ONLY if the student uses their uthsc.edu account, is not against university policy but it is recommended that you should set up different log in credentials for each of your other online accounts, such as banking, shopping, or email accounts.

Unfortunately, some plan to their NetID as their username, or their UTHSC email (which includes their NetID) for the non-university related web sites.

In December of 2010, gawker.com had around 1.3 million passwords (including corresponding usernames and email accounts) compromised.

Here are some tips and risk reminders when using your university NetID or your UTHSC email to gain access to external and third-party sites:

- Never reuse your UTHSC password for another online account.
- If your NetID and/or NetID password is stolen, the entity that retrieved this information can access any of your university-related portals.
- Technical journals and other licensed UTHSC Library resources can be accessed, putting the university at risk of being blocked from using the resources or having the university license revoked.
- Your personal university information can be accessed, putting you at risk for identity theft.
- Depending on your job function at the university, sensitive or confidential information about other members of the community could be exposed to unauthorized individuals (HIPAA).
- No one from the external or third-party site, where you use your UTHSC email, should ever ask you for your NetID password – not in email, not on the phone, not in person.
- Using your NetID password for other services, such as online banking, shopping, or discussion forums, increases the chances that it may be stolen, because these services may not transmit the password securely or could experience a security breach.
- Using the same password for most online accounts, hackers immediately begin attempts to access your university email accounts using the exposed password and NetID information.
- This statement can never be repeated enough: Avoid using your NetID as your login or account name for any non-UTHSC services!

If you have questions regarding the use of your UTHSC NetID or email, contact the IT Security Team at (901) 448-1579 or itsecurity@uthsc.edu.

Common UTHSC applications that require your UTHSC Password

- UTHSC’s Exchange email and calendar service, accessed via Outlook, Entourage, Outlook Web Access
- MyUT – The campus web portal
- iLogin
- UT VPN – The campus Virtual Private Network service
- Xythos
- Blackboard – Course information and materials
- Other web-based applications that use UT Web Login
