Lander UNIVERSITY

Information Technology Services
http://www.lander.edu/its
help@lander.edu
864.388.8234

Tips and Reminders for Lander University Computers

ITS offers the following tips and reminders to help ensure that Lander's computer resources are functioning to their best ability and meeting the needs of faculty and staff members in supporting Lander's mission.

Individual Computers assigned to Faculty and Staff Members:

- To ensure that Lander network computers remain up-to-date with security patches, antivirus definitions, and operating system updates, please ensure that office computers remain on overnight during the workweek. Optimize power savings by turning off external monitors and peripheral equipment overnight.
- To allow Lander network computers to apply operating system updates and clear temporary memory caches, please restart your Lander network computer at least twice a week. The recommended schedule is Tuesday and Friday afternoons.
- When stepping away from your computer, please take a second to lock the computer by simply hitting the ***Windows Key + L*** on windows computers or ***Control + Shift + Power*** on most newer Mac computers. When you return to your computer, you can quickly re-enter your password and pick up right where you left off.
- For laptop computers: When packing your computer away in a bag to transport home or to another location, consider shutting the computer off to minimize the chance of damaging or overheating the drive while in transit.
- Report damage to or problems with your Lander owned computer should be reported to Lander University's Information Technology Services Help Desk (extension 8234) for repair or resolution as soon as possible. Computers purchased for Faculty and Staff members include system warranties and accidental damage protection (for mobile computers) and can be repaired at no expense if damage is reported promptly. In most cases, a loaner computer can be immediately assigned to you while your computer is being repaired.

In general:

- Make it a habit to back-up your computer and important files regularly. You are solely responsible for backing up your essential data. Find basic instructions here: http://www.lander.edu/docs/default-source/its-documents/onedrivebackupwin10.pdf?sfvrsn=4 and look for periodic Tech Tuesday sessions covering this topic in more detail. If you or your department have specific concerns about backup strategies, you can request a consultation to discuss your unique needs and receive targeted recommendations from ITS hardware and security team members.
- Practice safe computing by maintaining and periodically changing strong passwords. Consider using a passphrase (multiple words that make up a phrase or sentence). Never share your password with anyone.
- Install software selectively: If you did not go looking for it, do not install it. If you install it, keep it up to date. If you no longer need it, uninstall it. Avoid pirated or cracked software.
- Avoid using special characters other than underscore or dash in your file names.
- If you notice something 'weird' or 'off' about your computer such as unsolicited popup windows, large numbers of email bounce-back messages, browser windows that redirect you to sites other than your home page, etc.; do not hesitate to contact ITS for assistance.
- Be suspicious of email scams or phishing attacks. If you think you have fallen victim, contact ITS immediately.

- If you think you have fallen victim to a phishing attack or your account has been otherwise compromised, change your password immediately.
    - If you are on campus on a Lander network computer, you can simply hit ***Control + Alt + Delete*** and choose the option to change your password.
    - If you are not on campus, you can change your password by logging in to MyLander, opening your Lander email account by clicking on the link in the upper right corner of the screen; (alternately – portal.office365.com and sign in with your Lander account); clicking on the My Account option; choosing Security & Privacy; then choosing Password. Note that if you change your password on your computer, you will be asked to log back in to Windows and to update your Outlook account password. You may be prompted to update your Bearcat Wireless credentials. You will also need to update the password on your mobile phone and any other mobile devices that you receive email on (such as an iPad). If you do not update your account password in all these places, your account will lock once the old (incorrect) password has been entered a few times.