Preparing and Securing Your Computer for Use at Lehigh

Your personal computer is an essential tool for completing coursework and vital to your success at Lehigh. The following nine topics offer guidelines on how to reduce your risk from viruses/malware, keep your computer physically secure, and protect it from catastrophic data loss.

• 1. Update your operating system
• 2. Update key applications and utilities
• 3. Practice good password management
• 4. Install anti-virus software
• 5. Enable your firewall
  ▶ Making Sure Windows Firewall Is Enabled
  ▶ Making Sure Mac OS Firewall Is Enabled
• 6. Extend your warranty
• 7. Plan and practice data backup
• 8. Physical security
• 9. Consider encryption

1. Update your operating system

Both Apple and Microsoft continually publish updates to their operating systems that strengthen weaknesses in the security of Windows and Mac OS. They also both have auto-update features built in, so if you are prompted to install updates, install them. Do not postpone them as they may be very important. To manually check for updates, follow the instructions below. You must be connected to the Internet when checking for and downloading updates.

• In Windows, click on Start, then click on Settings, then click on Update & Security, and click on the button, follow the prompts for downloading and installing updates.
• In Mac OS, go to click the Apple Menu at the top left corner of the menu bar, then click on Software Update, and it will check for updates. You'll be presented with a list of available updates, or a notice informing you that your software is already up-to-date.

Both of these features allow you to both get the current updates and to set your computer to automatically check for and download those updates in the background, which is a good choice for most users.

2. Update key applications and utilities

Many viruses and security threats today take advantage of vulnerabilities/defects in common third-party applications/utilities that almost everyone uses on their computers. These applications include:

• Adobe Acrobat Reader
• Browser (Chrome, Safari, Firefox, Edge)

As a result of these on-going threats, the companies that maintain these applications/utilities release frequent updates. **It is imperative that you run ALL updates for these applications AS SOON AS PROMPTED.** Many viruses and other malware specifically target outdated versions of these applications. You can significantly reduce your computer's risk of becoming infected ten-fold simply by always running updates when prompted.

3. Practice good password management

Not having a passwords set on your computer is a lot like not keeping your front door locked. To keep your data and personal information secure on your computer and web accounts you should get into the habit of using unique/strong passwords. Follow the guidelines below to reduce your risk of having your personal information stolen.

• Use unique passwords and usernames whenever possible.
  It is never a good idea to reuse the same username and password for multiple sites. If your username/password gets compromised on one site it makes your other sites vulnerable as well.
• Use strong passwords.
  Avoid using short/simple passwords (i.e., “password”, “12345”, etc.), they can be cracked in milliseconds (and most reputable online services will not even allow such passwords to be set in the first place). When creating passwords avoid dictionary words. The strongest passwords are those that use upper and lower case letters, avoid dictionary words and include numbers or special characters.
• Change your password regularly.
  It is good practice to periodically change your passwords especially on important sites such as those related to credit cards and banking.
• NEVER share your password.
  Never share your password with anyone and especially not in an email message. Beware of email phishing messages that attempt to trick you into providing your username/passwords.

**NOTE:** Lehigh University will NEVER ask you to provide your password via email or over the phone.

Following the above guidelines will go a long way toward keeping your confidential information and important data safe. To make managing your multiple username and passwords easier you may want to consider using some type of password management program/service such as: LastPass, RoboForm, or KeePass.

4. Install anti-virus software
Viruses, spyware, and other malware continue to pose a threat to users of any computer/platform. Using your computer at Lehigh is no exception. Having a good, up-to-date antivirus program is essential to minimizing the risk of your computer becoming infected and/or having your data and other personal information vulnerable to related threats. LTS recommends several antivirus packages that are free for personal use. Whichever program you choose to install on your machine, it is crucial to keep it up-to-date and run updates whenever prompted to do so. Since new threats are released almost on a daily basis, the anti-virus programs recommended by LTS all have automatic update features which you should always take advantage of.

It is important to note, especially if you are using an anti-virus program that you paid for (or came with your computer as a free trial), that these programs typically only include update subscriptions for a set period of time (i.e. 1 year, 2 years, etc.). When this period runs out you will need to either renew the subscription or switch to another program.

5. Enable your firewall

Besides anti-virus software, another important thing you can do to keep harmful software off of your computer is to make sure your firewall is enabled. A firewall is a networking feature that blocks portions of your network traffic so that only network communications of the types you want are getting through it. The built-in firewalls for Windows and Mac OS, work well, are already configured correctly for most users by default, and can simply be turned on or off.

**Making Sure Windows Firewall Is Enabled**

1. Go to the Control Panel (Start > Control Panel), click on Windows Firewall.
2. If the Windows Firewall state is set to On (shown in the screenshot below), then you are already good to go and you can close the window.
3. If the Windows Firewall state is set to Off, then click on Turn Windows Firewall on or off from the left menu pane.
4. Check each button next to Turn on Windows Firewall. By default, only Notify me when Windows Firewall blocks a new program should be checked. In any case, make sure that option is the only one checked. Once you have turned Windows Firewall on, you may close the window.

**Making Sure Mac OS Firewall Is Enabled**

1. Go to System Preferences (can be found on the dock or by going to Apple menu > System Preferences), and click Security.
2. In the Security section, click on the Firewall tab.
3. If necessary, click the lock icon on the lower left, and enter your OS admin password to allow changes to be made.
4. If not already set by default, Select Set access for specific services and applications so that the listed services are allowed through the firewall.

6. Extend your warranty

See computer purchase and warranty recommendations for information on purchasing the appropriate warranty coverage.

7. Plan and practice data backup

Backing up the important data (documents, music, pictures, etc) is absolutely essential for every student. With most students using laptops, the chances of data loss from hard drive failures increases greatly. Having your important files backed up onto another source ensures that you will not lose everything in the event of a disk failure, stolen laptop or accidental deletion. The options below will give you some options as to how the average student can protect their data.

- **Lehigh H: drive space**: Each student is given 5 GB of Lehigh network drive space. This data can be accessed from Windows and Mac computers as well as public site computer labs. The data is backed up regularly by Lehigh.
  - **Pros**
    - Data is backed up by Lehigh nightly
    - Assistance is available from Lehigh staff with accessing the space from personal computers and also, if necessary, with file restoration from backups
  - **Cons**
    - Maximum of 5GB of space available
    - Requires the use of the Lehigh VPN in order to access the space from off-campus
- **Google Drive App**: As part of a student’s Lehigh Google account, Google Drive cloud storage space is available. Using Google’s Drive app a student can have the important files on their computer automatically backed up to their Lehigh Google Drive space. The instructions and app can be found at [https://www.google.com/drive/](https://www.google.com/drive/)
  - **Pros**
    - Fast, backups run automatically
    - Must have Internet access to use, only 30 day retention on deleted files.
- **External hard drive**: In addition to manually copying files from your computer to your external hard drive, current operating systems typically offer some sort of backup feature that works by automatically backing up data at regular times to an external drive - Mac OS Time Machine is an example of such a backup feature.
  - **Pros**
    - Very fast/easy to backup files
    - No ongoing costs beyond the purchase of the hard drive
- **Cons**
  - Backups can only be done when the drive is connected to the laptop
  - The user must be proactive in doing the backups otherwise backups get out-of-date

- **Online backup services**: Internet services such as Crash Plan, or Carbonite offer automated backup services and online storage at a per gigabyte cost. Services such as these will automatically back up the data on your main computer to their cloud storage servers.
  - **Pros**
    - Backups are done automatically without the user needing to do anything
    - Large amounts of data can be backed up for a relatively low monthly cost
  - **Cons**
    - Internet access is required to do backups
    - Large amounts of data can take a while to back up

- **Online cloud storage**: Services such as Google Drive, Dropbox, Box.com, OneDrive, Amazon Cloud, etc. These services provide you with storage space in the Cloud (Internet) that you can access from multiple devices (laptop, tablet, phone, etc).
  - **Pros**
    - Data stored on the cloud service is available from any device (web, laptop, phone, tablet, etc)
    - Files can be synced onto different devices making it possible to work on the same set of files from different computers
  - **Cons**
    - Monthly cost for storage is much higher than for online backup service
    - Cloud storage is not a substitute for backups. If a file is accidentally deleted or changed in most cases it is not possible to recover it

A good backup strategy includes elements of all of the above. The external hard drive is great for fast backups and restores, the online backup service, while slow, will provide protection in the event you forget to backup to the external drive or if your laptop and hard drive gets stolen or destroyed. Finally, storing your data on an online cloud storage service can be made much safer by having your data also backed up to your external and/or online backup service.

8. **Physical security**

Protecting your computer from loss or theft is something all students should be concerned with. Below are some options you may want to consider:

- **Laptop Lock**: Also known as a Kensington lock. This type of lock will secure your laptop using a steel cable connected to an immovable object such a table or desk thereby preventing someone from casually walking away with your laptop

9. **Consider encryption**

Whole disk encryption is something students may want to consider to protect the sensitive data on their computer. Disk encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. If your computer is ever lost or stolen disk encryption ensures that the data on it will be inaccessible to anyone but the owner. Both major OS platforms provide built-in full-disk encryption schemes:

- Bitlocker (Windows)
- File Vault (Mac)

Things to consider before using encryption on your hard drive:

- You must know/have access to your encryption keys. It will be impossible to recover your data without them if your system becomes unbootable.
- Data recovery from a failing hard drive is more difficult if the drive is encrypted
- Having backups of your data is essential if your drive is encrypted
- There could be a decrease in performance on computers with encrypted drives

Individual students must decide for themselves if the data on their own computers is important enough that disk encryption is needed.

There are no related labels.