

Operating system and software updates are required to keep computers healthy, up-to-date, and protected from outside threats. It is ITAC's recommendation that university computers connected to the network remain powered on, as appropriate, to receive important updates. In addition, Texas State-owned computers require an increased level of security when storing confidential information or during instances when laptops are taken off-campus.

Keeping the Software Connected and Accessible

For Microsoft Office and Windows software to remain active and accessible, computers must be connected to the Texas State network (physically or virtually) and communicate with the servers once every 180 consecutive days (three consecutive hours at a time). However, to ensure that your computer remains up-to-date with security patches and software updates, Technology Resources (TR) recommends connecting to the network every 30 days.

If you have a Windows environment on your Mac, the Windows environment must also follow the same connection rules as a regular Windows computer. Also, laptops must be hardwired on-campus or connected via the Texas State [Virtual Private Network \(VPN\)](#) service to synchronize with newly created passwords. Contact the [IT Assistance Center](#) to request VPN service.

There are three ways to connect to the Texas State network for security updates and software activation:

- Desktops and laptops physically on-campus: Hardwired Ethernet connection
- Laptops physically on-campus: Wi-Fi connection to the secure, encrypted network ([TexasStateWPA](#))
- Laptops off-campus: Using any Internet connection (wired or wireless) and connecting to the Texas State VPN
 - Note: Contact the [IT Assistance Center](#) to request VPN service.

Updating Windows Software

Texas State-owned Windows computers must have [Software Center](#) installed to receive monthly campus-released updates. To receive updates, establish an active Internet connection for a minimum of three consecutive hours at least once every 30 days.

Note: Some department Technical Support Personnel (TSP) configure computers with maintenance windows or specified windows of time where updates must occur. If your computer is on a maintenance window, the computer will need to be connected to the Texas State network using one of the connection methods outlined above during that specific period of time to receive its updates.

Protecting the Computer against Viruses and Malware

Follow these best practices to maintain a healthy, virus and malware-free workstation:

- Perform a full virus scan at least once per week. Virus and malware definition files are released daily. To receive these updates, the computer must have any active Internet connection.
 - Note: To receive virus and malware updates, the computer must be connected to any Internet connection (not necessarily connected to the Texas State network).
 - If you do not use the computer often, be sure to power it on and establish an Internet connection weekly to allow the virus scan to run and the definitions to update.
- If you miss a scheduled virus scan, your computer will scan the next time it is turned on.

Accessing On-Campus Resources from an Off-Campus Computer

- Remotely connect to your office computer using the [Remote Desktop Setup](#) service.
- Alternately, connect your Texas State-owned laptop to the Texas State network from any Internet connection when away from campus by using the Texas State [Virtual Private Network \(VPN\)](#).
 - Note: Contact the [IT Assistance Center](#) to request VPN service.