How do I update my university Windows computer to make sure it is not vulnerable to the Peyta Ransomware attack?

Tell Me

If a Windows computer has the latest security updates, the computer is not vulnerable. If a Windows computer has been turned off or not on the university network for some time, it may be at risk.

To manually install security updates - follow these steps. If off-campus, connect to the VPN first.

Windows 7

1. Open the Control Panel
2. Click System and Security

Windows 10

1. Type Control Panel in the search box in the bottom left toolbar
2. Click on Control Panel
3. Click System and Security

Adjust your computer's settings

- System and Security
  - Review your computer's status
  - Save backup copies of your files
  - Backup and Restore (Windows 7)
  - Find and fix problems

- Network and Internet
  - View network status and tasks
  - Choose homegroup and sharing options

- Hardware and Sound
  - View devices and printers
  - Add a device
  - Adjust commonly used mobility

- Programs
  - Uninstall a program
  - Get programs

4. Click Configuration Manager at the bottom of the window.
3. Click **Configuration Manager** at the bottom

4. Click **Action** tab

5. Click **Action** tab

6. Click **Machine Policy Retrieval & Evaluation Cycle**, then click **Run Now**.
5. Click **Machine Policy Retrieval & Evaluation Cycle**, click **Run Now** and then **OK**

6. This message will show click **OK**

7. Let the scan run, it will identify the updates that are needed

8. Follow the prompts to install updates, install immediately

---

Related FAQs

- How do I request my University computer to be upgraded to Windows 10?
- How do I fix a shortcut to a Google Drive shared folder?
- How do I know what operating system I am running?
- How do I find information about my computer like the computer name?
- How do I install Adobe PDF printer on my University Windows computer?