

Virus and Threat Protection at Wharton

Last Modified on 04/29/2025 3:51 pm EDT

The University of Pennsylvania offers threat protection and antivirus software solutions for faculty, staff, and students for both managed and unmanaged computers.

How To Protect Yourself Against Viruses

Be Aware of Sites & Attachments

As computers become more networked and standardized, it gets easier and easier to catch computer viruses. You can get viruses from downloads over the internet, from opening e-mail attachments, or from another infected system or device.


Many self-propagating viruses will mail themselves to you before the original sender has discovered that his/her machine is infected. Be suspicious of any attachments, but be extra vigilant about inappropriate subject lines and attachment titles (for example, if someone you barely know sends you an e-mail called **ILOVEYOU**).

Back Up Data Frequently

Some viruses are so damaging that they will render your files useless or unrecoverable. In that case, your only hope of recovery is with back-ups made prior to infection.

Update, update, update!

Microsoft & software developers frequently release patches to fix known issues for their services. These fixes include known security issues that may leave your computer or program vulnerable to viruses and other attacks. To

manually update, press the Windows key + S ( + s), type **check for updates**, and then click the **Check for Updates** setting.

Antivirus Protection

Antivirus software recommendations at Wharton differ depending on whether you are faculty, staff, or student and whether Wharton manages your computer.

Unmanaged Computers

Student computers and some personal computers owned by faculty and staff are "unmanaged" – they are not part of the Wharton-managed computing environment. These computers should have antivirus protection installed – we recommend Sophos Home (for Macs) or Windows Defender (for Windows 10).




Managed Computers

Wharton uses the CrowdStrike software to protect faculty and staff machines that are managed by Wharton. (Student computers are not managed by Wharton.)

Choosing Your Antivirus Software

There are several conditions that will determine which steps you take to install the appropriate antivirus software: who you are, and what kind of computers you are using.

	Faculty/Staff	Student
Unmanaged Mac	Sophos Home	Sophos Home
Managed Mac	Crowdstrike	N/A
Unmanaged Windows	Sophos Home	Windows Defender
Managed Windows	Crowdstrike	N/A

MacOS	Windows 10	Windows 10 (if Defender is not an option)
 Sophos Home	 Windows Defender	 Sophos Home

Sophos Home FAQs

What if I already have antivirus software?

Why should I switch to Sophos Home?

Will I get technical support if I switch to Sophos Home?

Virus Removal

If your personal computer has a virus, use the steps below to try removing it on your own.

Faculty and Staff should NOT attempt to remove viruses on any Wharton-managed machine.

If you suspect you have a virus, disconnect your computer from the network, power it off, and contact your **Wharton Computing Representative** or the **Information Security Office** right away for assistance.

Before You Start:

- Back up your computer's data to an external hard drive or other source not attached to your computer to prevent any loss of important data.
- Make sure you're comfortable downloading and installing software on your computer.

Windows/PC

The procedure below is simplified for your convenience and remedies most situations.

Virus Removal Procedure (Mac)

The steps for removing viruses from Macs are fairly straightforward.

Questions?

For more information regarding security threats and antivirus software, you can also contact the Wharton Information Security Office at security@wharton.upenn.edu.
