**1. How do I secure my computer?**

Even if you aren't a security expert, there are a few basic steps you can take to secure your computer. Read the [**Secure UD Essentials for computers**](https://www1.udel.edu/security/essentials.html#computer) for more information.

* [**Install and run anti-virus software**](https://www1.udel.edu/security/bestpractices/avs.html) on your computer to detect and remove malware.
* [**Back up your computer's data**](https://www1.udel.edu/security/bestpractices/backups.html) to protect yourself and the University from data loss or corruption.
* Enable your computer's [**firewall**](https://www1.udel.edu/security/bestpractices/firewalls.html) to block potentially harmful traffic.
* [**Encrypt sensitive information**](https://www1.udel.edu/security/bestpractices/encryption.html) to protect it from being read or misused if it's lost or stolen.
* [**Password-protect your computer**](https://www1.udel.edu/security/bestpractices/passwords.html) to prevent others from logging in and using your system and files.
* Regularly [**patch your computer's software and firmware**](https://www1.udel.edu/security/bestpractices/patching.html) to protect against the newest vulnerabilities.
* [**Physically secure your computer**](https://www1.udel.edu/security/bestpractices/physical.html) in a locked office when possible. Never leave laptop computers unattended in public locations.
* Configure your computer to [**automatically lock**](https://www1.udel.edu/security/bestpractices/sessions.html) after fifteen minutes of inactivity.

If you're a faculty or staff member, talk to your local support provider or contact IT for more information about the University's [**computer management tool**](https://www1.udel.edu/security/bestpractices/computermanagement.html), which automates security tasks like patching, anti-virus scanning, and more. It can be administered by either your unit or IT, and it's never used to spy on you or your files.

**2. How do I secure my mobile device?**

Mobile devices like smartphones and tablets present unique security challenges because of their portability and simplicity. Read the [**Secure UD Essentials for mobile devices**](https://www1.udel.edu/security/essentials.html#mobile) for more information.

* [**Back up your mobile device's data**](https://www1.udel.edu/security/bestpractices/backups.html) to protect yourself and the University from data loss or corruption.
* [**Encrypt your mobile device**](https://www1.udel.edu/security/bestpractices/encryption.html) with whole-disk encryption to protect its data from being read or misused if the device is lost or stolen.
* [**Password-protect your mobile device**](https://www1.udel.edu/security/bestpractices/passwords.html) to prevent others from accessing its data and apps.
* [**Regularly patch your mobile device's software and firmware**](https://www1.udel.edu/security/bestpractices/patching.html) to protect it against the newest vulnerabilities.
* [**Physically secure your mobile device**](https://www1.udel.edu/security/bestpractices/physical.html) in locked offices or cabinets when possible. Never leave mobile devices unattended in public locations.
* Configure your mobile device for [**remote management**](https://www1.udel.edu/security/bestpractices/remoteprotection.html). Enable it to automatically erase data after ten failed password entries in a row and to be remotely locked, located, or erased at your request.
* Configure your mobile device to [**automatically lock**](https://www1.udel.edu/security/bestpractices/sessions.html) after five minutes of inactivity.

**3. Can IT help me manage my computer's security?**

Yes; both IT and your unit's IT staff can help you manage your computer. If you're a faculty or staff member, talk to your local support provider or contact IT for more information about the University's [**computer management tool**](https://www1.udel.edu/security/bestpractices/computermanagement.html), which automates security tasks like patching, anti-virus scanning, and more. It can be administered by either your unit or IT, but your unit may also offer its own computer management solution that is more suited to your particular data needs.

The computer management tool is used only to help secure your computer. It is not used to read or record your personal files or spy on your computing activity.

**4. What is malware and how do I get rid of it?**

Malware is short for *malicious software*—software used by hackers to impair your device's function, steal your device's data, or even gain control of your device itself.

Typically, malware is downloaded unknowingly when an unsuspecting user opens an infected file or visits an infected website. Once it's on your computer, it launches a specific kind of attack based on its design. For example, keyloggers record each keystroke and report it to hackers, who look for usernames, passwords, and other sensitive credentials. Trojans masquerade as useful or benign software—often as fake anti-virus software or games—to trick users into opening them and granting them access to system files or the ability to download more malware.

You can protect your computer against malware by installing [**anti-virus software**](https://www1.udel.edu/security/bestpractices/avs.html) and running routine scans. IT provides a University-licensed copy of [**McAfee VirusScan**](http://udeploy.udel.edu/software/mcafee-virusscan/) free of charge to all students, faculty, and staff. Any faculty or staff member whose computer processes sensitive University information should contact the [**IT Support Center**](https://www.udel.edu/it/help/request) to get a copy of Cylance advanced anti-virus software.

If your computer is running slowly or taking unusual actions (such as "reminding" you to download strange software), it may be infected with malware. Run an anti-virus scan to check for, identify, and remove malware from your device.

**5. What should I do if I want to dispose of a device that was used for University activities?**

If the device in question is a University-owned IT device, then check with your unit's IT staff first. Your unit may have its own procedures for securely disposing of IT devices. If your unit doesn't have its own procedures, then you should use central IT's [**secure device disposal service**](https://www1.udel.edu/security/bestpractices/disposal.html).

If the device in question is your personally-owned device and was used to conduct University-related work, then you should follow this basic process:

1. [**Back up**](https://www1.udel.edu/security/bestpractices/backups.html) any files that you need to retain.
2. [**Securely erase**](https://www1.udel.edu/security/bestpractices/disposal.html) the device's memory. If you don't plan to sell or donate the device, you can physically destroy its storage media.

Dispose of the device by using an electronics recycling center or by selling or donating it.