Information Technology Services

Information and Cybersecurity Awareness

Email ithelp@up.ac.za | **www.up.ac.za/itsecurity**

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Make today matter

Secure your macOS device

'Do your part – be cyber smart'

McAfee Computer Security has estimated that there are approximately 450 000 malicious programs aimed at macOS devices. As the Apple userbase grows, so does the number of targeted malware versions. As part of the University of Pretoria's Security Awareness Campaign, we aim to increase the security of macOS devices to protect them from these threats and reduce the likelihood of their systems being compromised or data exposed to unauthorised parties.

Secure your device by following the instructions below:

How to protect yourself and your macOS device

- **Require an administrator password for system changes:** To prevent malware from installing PUPs (potentially unwanted programs) and making changes to your system settings, configure your device to require an administrator password when installing programs and making changes to your system settings.
- **Regularly update macOS software:** Ensure that your operating system software is regularly updated to keep your system secure and running correctly. macOS updates improve the stability, performance and security of your Mac and include updates for Safari, iTunes and other apps that are part of macOS.
- **Install antivirus or malware software:** Since macOS devices are not immune to viruses and other malware attacks, you should beef up your device protection by installing antivirus software. You can install any antivirus or anti-malware software, but it is highly recommended that you install McAfee, which is the University's licensed antivirus software.
- **Turn on automatic updates:** By turning on automatic updates you can ensure that your macOS device will download and install apps from trusted sources only, such as Apple App Store.
- **Encrypt with built-in FileVault:** FileVault ensures that your files are encrypted. If your macOS device is ever lost or stolen, others will not be able to access your private data. Apple's built-in FileVault[1] full-disk encryption will encrypt the entire hard drive using a secure encryption algorithm.
- **Turn on firewall:** Using the built-in firewall on your macOS device will block incoming connections and prevent unauthorised applications, programs and services from accepting incoming connections. As an administrator, you can choose to allow only signed software to accept incoming connections.
- **Turn on Stealth mode:** If you are using your macOS device on public networks, it is essential to turn on Stealth mode[2], which will ensure that other devices and users will not be able to detect or connect to your macOS device. Using Stealth mode makes it difficult for hackers and malware to find your device.
- **Backup your data:** The importance of regularly backing up your macOS device cannot be overstated. Backups offer protection that can help you recover from unexpected data loss. It can be used to recover data after reinstalling macOS or when setting up a new device. Lastly, it can protect you in the event of a catastrophic disk failure.

SEE MORE

McAfee Labs Threats Report: 2021

READ MORE

10 Assumptions About macOS Security That Put Your Business At Risk

2022 Readiness: Mac Malware Awareness

Apple Built-in FileVault

Stealth Mode on Mac

DO MORE

Set up your Mac to be secure