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

Don't let your smart device outsmart you —Part 2: steps to protect yourself and your smart device

'Make your home a haven for online safety'

Your smart devices have valuable information stored on them.

Introduction

Any electronic device that connects to the Internet to share data can be classified as a smart device.

So, what can I do?

1. **Secure your desktops.** Be responsible and aware of all your device security configurations. Setting group policies can allow you to set configuration details for Windows and other programs like Internet Explorer.
2. **Give your router a name.** The router comes standard with an easy name to find. The name the manufacturer gave it can reveal the make or model. This information allows hackers to easily find admin-level access. Choose an uncommon name that does not identify you or any of your private information.
3. **Check the settings of your devices.** Your Internet of things (IoT) devices come with default privacy and security settings. Consider changing them as soon as possible as these are default vulnerable points of entry.
4. **Use strong encryption for Wi-Fi.** This is easier than it sounds. In your router settings, choose a strong encryption method, like WPA2 for Wi-Fi. This will help keep your network, IoT devices and their connections secure.
5. **Set up a guest network.** Try to keep your main Wi-Fi account private. Others can log into a separate network that does not connect to your IoT devices.
6. **Change default usernames and passwords.** Cybercriminals probably know the default password that comes with your device. Change the default password as soon as possible.
7. **Use strong, unique passwords.** For Wi-Fi networks and device accounts, avoid common passwords that are easy to guess, such as 'password' or '123456'. Consider using a password manager to support your security.
8. **Disable features you may not need.** IoT devices come with many services, such as remote access, often permitted by default. If you don't need it, disable it.
9. **Audit IoT devices** already on your home network. You can check if newer models might offer stronger security or if software updates are available to fix security breaches.
10. **Use two-factor authentication.** See our 2FA article for this feature. It can keep your accounts safe.

SEE MORE

Cybersecurity 101

READ MORE

How you can protect your smart devices from cyberattack

DO MORE

10 ways to prevent computer security threats from insiders