



UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Information Technology Services

Information and Cybersecurity Awareness

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



Know when you're secure

'Think before you click, like or share'

The Web is the Wild West of the twenty-first century. However, you can do much to ensure your own safety when traversing this virtual environment.

Introduction

Cybercriminals have ways and means to intercept or redirect your internet traffic. Their objective is financial gain, and they would love to get hold of your personal information and banking details.

Below are a few things you can do to confirm that you are safe online before logging in to a site, performing private transactions or entering your personal and financial details on a website.

How to protect yourself

Always check the URL in the address bar at the top of the screen before entering any personal information.

- Ensure that you know your service provider's web address, for instance, your bank's address, and check that the address displayed is what you expect it to be.



- Check that a locked padlock is displayed to the left of the URL. If not, it means that the connection is not encrypted and that information typed in can be intercepted. Note that legitimate websites may be insecure for general public pages, but could switch to secure mode when you are required to enter sensitive information. Also, being secure does not indicate that the site is not fraudulent, only that its traffic is encrypted. Therefore, you need to do the checks below as well.
- Clicking on the padlock should show you more security details confirming the website's security and validity.
- Read the website's Privacy Policy, generally found at the bottom of the page. The policy should clearly communicate how your data is collected, used, and protected by the website.

In addition, take note of the following:

- Be aware of danger signs like an overload of advertisements and pop-ups, or the absence of contact details for the website.
- Refrain from installing web plug-ins (also called add-ons and extensions) which may contain malicious code or collect your information.
- Check the privacy options available for the browsers you are using on all your devices.
- Use a website safety-check tool to check if a URL in a link is safe before clicking the link.

SEE MORE



[Can you be secure on free Wi-Fi?](#)

READ MORE



[Secure your web browser for security and privacy](#)
[Does incognito browsing in Chrome increase your level of security?](#)

DO MORE



[Check the safety of a URL using Google's safe browsing tool](#) or [VirusTotal](#)