UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

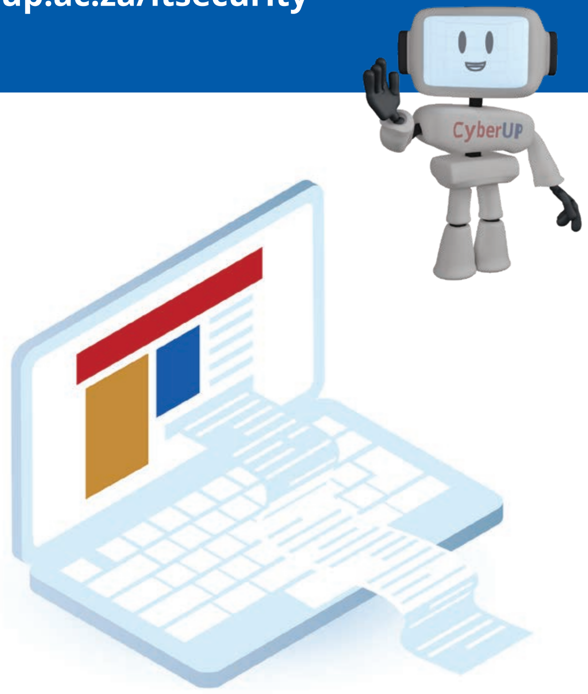
Information Technology Services

Information and Cybersecurity Awareness

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

Two-factor authentication (2FA)

'Make your home a haven for online safety'



Millions of users' login credentials have been exposed on the dark web. In addition, phishing is currently the most common cybercrime. Preventing exposed credentials from being used to access your accounts is important and not that difficult.

What is two-factor authentication?

Two-factor authentication (2FA) adds a layer of security to online authentication by requiring a second form of identity verification in addition to a password. The second factor often requires access to a cell phone or another specialised device. 2FA is offered for online products like Apple ID, Google, Facebook, Twitter, WhatsApp, banking apps and many more.

How does two-factor authentication work?

After logging in to your account with a password, you are asked to verify your identity using a verification app or by entering a security code provided in a text message, email, push notification, or physical key, depending on the 2FA method employed.

The second factor is usually more difficult to present than a password. This is because it requires something to which the real owner has physical access, like a smartphone with a particular authenticator app installed, a linked phone number for a push notification or SMS authentication code, or a hardware security key, which leaves a hacker unable to access the account even if they have the correct password.

SEE MORE

▶ Watch the video on 2FA and its features

READ MORE

How to switch on 2FA for Google accounts

DO MORE

Consider enabling 2FA on your Google and social media accounts

Why does two-factor authentication matter?

2FA is currently the most effective way of preventing access by criminals or anyone else in possession of valid credentials for your online accounts.

How safe is two-factor authentication?

Nothing is completely secure, and that includes 2FA. Two-factor systems have been hacked in the past, but the biggest risk is not the 2FA technology. The biggest risk is social engineering, which can bypass even the most secure of systems.

How do I start using two-factor authentication?

2FA is available for most online accounts and often only requires that you enable the option.

Start by checking each of your online accounts to see whether 2FA is offered as a service. This is usually found under the account settings and/or security features.

If 2FA is not available for an important account, take care to change its password regularly.

HOME-2 • Graphic sourced and adapted from freepik.com