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**

Passwords – your key to cybersecurity

'Do your part – be cyber smart'

How would you feel if your vehicle, home or office keys were lost or stolen? Do you use the same key for your car, safe, house, and office? In the digital world, your passwords are your keys that protect your information on all your devices and applications.

Introduction

Stolen or weak passwords are the most common reason for data breaches. Cybercriminals use of a variety of methods to obtain your login name and password, including phishing, spyware, buying passwords on the cybercrime market, using your personal information and automated password crackers.

A breached password can cause a domino effect of security compromises when the same password is used across different websites and platforms.

SEE MORE

WATCH: How to create a strong password

WATCH: Why password protection is important

READ MORE

UP Password Policy

Password best practices

Password managers

DO MORE

Test the strength of your password (or close replica) with Kaspersky's password checker

Test your password against compromised passwords

How to protect yourself

- Keep your passwords as secret as the PIN of your ATM card.
- Use strong passwords. More digits are better, as is a combination of upper- and lowercase letters, symbols and numbers. Avoid dictionary words, personal information and commonly used phrases such as 12345, qwerty, Password1 or 111111.
- Use different passwords for different sites – e.g. banking, email and social media – to limit your risk.
- Don't write down your passwords. Memorise them or use a password manager that requires you to remember only one very strong master password.
- Change your password regularly, e.g. every 60 days, and whenever you suspect that it might have been compromised.
- Use two-factor authentication whenever possible. This adds an additional level of security by requiring a PIN, fingerprint or another factor, in combination with your password for identification.
- Do not save passwords to browsers.
- Set up security questions or hints for remembering or resetting a forgotten password, but do not to use information that may be known to others.

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