Stellenbosch
UNIVERSITY
IYUNIVESITHI
UNIVERSITEIT

Cybersecurity toolkit

Be aware. Be secure. Be cybersmart.

Empower yourself to stay safe online

In today's digital world, protecting personal information is more important than ever. Stellenbosch University (SU) staff and students are encouraged to take note of and adopt the following simple and effective cybersecurity practices to stay safe online. Cybersecurity is everyone's responsibility.

Data breaches

A data breach happens when sensitive information - such as student records, research data or staff details - is accessed or disclosed without authorisation. Think of it as someone breaking into a locked room to steal confidential documents. In the digital realm, breaches can lead to identity theft and significant disruptions to university operations.

Report a data breach

Multi-Factor Authentication (MFA)

MFA adds an extra layer of security by requiring a secondary method to confirm your identity when logging into accounts. This typically involves entering a code generated by an authenticator app. With MFA, even if your password is compromised, unauthorised users cannot access your accounts.

How to enable MFA

Phishing

Phishing occurs when criminals attempt to deceive you into opening harmful links or providing personal information through emails, texts or phone calls. These messages often appear to come from trusted sources. Stay vigilant and report any suspicious communication.

Phishing red flags

Strong passwords

Weak passwords are like locking your door but leaving the key in the lock. They can be easily cracked by hackers. Using a password manager can help you create strong, unique passwords for each account and securely store them. This is one of the simplest ways to protect your sensitive information.

View SU's password regulations

Should you have any questions, please log a request on our **ICT Partner Portal**

#CyberSmartMaties