Remote Working Safety Guide

🔑 PROTECT YOUR NETWORK AT HOME

If you're using wireless access for remote work, ensure your home network is secure. Change the default administrator password of your router to prevent unauthorized access. Share your WiFi password only with trusted individuals and keep track of who has access to your network. Update devices connected to your network regularly.

💻 CREATE STRONG PASSWORDS

Never share your password, they are crucial for securing your information. For stronger security, choose complex combinations of letters and numbers. Consider using phrases instead of single words, and avoid reusing passwords. Password managers can help you manage multiple passwords effectively. Opt for two or multi-factor authentication when possible. These practices will significantly enhance your online security, protecting your sensitive data from potential threats.

UPDATES ARE KEY

Install updates for your computer, operating system, and software promptly. These updates often include security fixes and protect against cyber attacks. Don't postpone updates to ensure the security of your data and devices.

⚠ BE CAUTIOUS WITH EMAILS AND TEXT MESSAGES

Verify the legitimacy of every email you receive, especially urgent ones. Check the sender's email address, spelling and grammar, and message tone. When in doubt, contact the sender directly to confirm the request and avoid clicking on suspicious links or opening attachments.

For more information, visit *icts.uct.ac.za*

ICT
ICTS
Information and Communication
Technology Services