

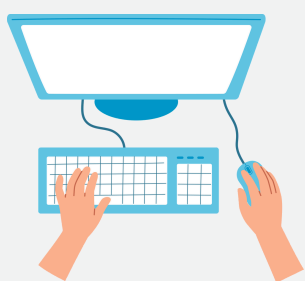


CYBER EMERGENCY RESPONSE GUIDE

7 STEPS WHEN THINGS GO WRONG

STEP 1 - STOP & DISCONNECT

- STOP what you're doing - don't click anything
- DISCONNECT from internet (unplug WiFi)
- TAKE PHOTOS of suspicious messages/screens
- WRITE DOWN what happened and when



STEP 2 - SECURE YOUR MONEY

- CALL your bank if money is involved
- CHANGE passwords on a different device
- ENABLE two-factor authentication
- CHECK recent login activity

STEP 3 - CHANGE ALL PASSWORDS

- USE a different device (phone/tablet)
- CHANGE passwords for email, banking, social media
- UPDATE work account passwords
- ENABLE two-factor authentication everywhere



STEP 4 - CHECK THE DAMAGE

- CHECK email sent folder for unknown messages
- ASK friends if they got strange messages from you
- REVIEW all recent purchases and transactions
- REMOVE unknown apps and permission

STEP 5 - CLEAN YOUR DEVICES

- RUN antivirus scan on all devices
- DELETE suspicious programs and browser extensions
- UPDATE all software and operating systems
- CLEAR browser cache and saved passwords



REPORT

STEP 6 - REPORT & DOCUMENT

- FILE police report if money stolen
- REPORT to local cybercrime authorities
- CONTACT identity theft support services
- DOCUMENT everything - screenshots, emails, transaction IDs

STEP 7 - GET EXPERT HELP

Send an email to us at hello@remaleh.com.au with subject "EMERGENCY" and include what happened and when. Expect a response within hours and get professional help with recovery.



hello@remaleh.com.au



www.remaleh.com.au

Cybersecurity Protection for everyday people