AVOIDING TECH SUPPORT SCAMS

Beware of phone calls, popups and emails telling you there's a problem with your device!

POPUPS

If a window / banner appears on your screen while browsing, examine the message closely. Look for poor spelling and bad grammar. Verify phone numbers from known sources. Don't click!

ANTIVIRUS

Use reputable antivirus software. Antivirus software helps detect and deal with any malicious software that may come your way.

REMOTE ACCESS

If you receive a phone call or live chat request, where remote access to your device is requested, don't engage and hang up! Never give anyone remote access to your device.

PASSPHRASES

Passphrases are more secure than passwords. A passphrase contains random words, a mixture of upper and lowercase letters, numbers and symbols.

Example: Appl3$ky&ant5

CALLS

Beware of unsolicited calls requesting your personal information. This includes asking for access codes you may have been sent via your mobile as part of multifactor authentication.

EMAILS

Beware of scam emails designed to steal your personal information. Look out for generic greetings, suspicious links or attachments, poor spelling and grammar, threats or requests for payment.

If you are the victim of a cybercrime, make a report at cyber.gov.au/report or attend your local police station.

Disclaimer: This publication contains only general guidelines and strategies for dealing with scams, and no guarantees or representations are made concerning their effectiveness. SAPOL accepts no responsibility for any injury or loss resulting from the application of these strategies.

SOUTH AUSTRALIA POLICE
SAFER COMMUNITIES

Government of South Australia