WHEN THE CYBERTHREAT GOES MOBILE

KEY THREATS

VISHING - "VOICE PHISHING"

- Scammers use phone or voicemail to pose as bank, service or other staff
- Aim is to get people to provide their credentials to a "trusted" caller or to take action over the phone

SMISHING - "SMS PHISHING"

- Scammers send text messages prompting you to make payments or click on specific links
- Aim is to harvest credentials, elicit payments or embed malware on the device.

SPOOFING - "TRUSTED CALLER"

- Scammers use real phone numbers, maybe even yours, to scam others
- Aim is to use a local number / caller ID that you are likely to trust, and therefore answer

www.maxsum.com 1300 629 786

MAXSUM CONSULTING

WHAT TO DO

VANQUISH THE VISH

- Hang up - Block the number if you can
- Never take any action over the phone
- Never provide any personal information over the phone
- If unsure, call the organisation to verify and confirm

SQUISH THE SMISH

- Be on the lookout for telltale fakes - Strange links, unusual domain names, spelling mistakes etc.
- Do not click on any links in SMSs to take action
- Do not enter any credentials via SMS links
- If unsure, call the organisation to verify and confirm

STAMP OUT THE SPOOF

- Report to your Telco provider asap
- Turn on 'Silence Unknown Callers' on iOS Devices*
- Turn on 'Spam and Call Screen' on Android devices*
- Avoid giving out your phone number, especially online, wherever possible

*Seek technical guidance first for corporate or managed devices.

www.maxsum.com 1300 629 786

MAXSUM CONSULTING