UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0401

SMS SCAMS TARGETING NEW ZEALANDERS

DATE ISSUED: 16th August 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

New Zealanders are being targeted by a text message phishing scheme that uses a distressing situation involving family members. The messages falsely state that a recipient's relative or child has encountered phone damage and includes a new mobile number for communication.

BREAKDOWN

In New Zealand, a text phishing campaign is underway, targeting people with messages pretending to be from family members, stating their phone is broken. They ask for contact through a new mobile number. Scammers then request bank or credit card info to supposedly buy a new phone. Getting an unexpected text message purportedly from a family member doesn't automatically put you in danger. While just receiving the message is generally safe, responding could increase the risk.

REMEDIATION STEPS

- Avoid replying to unexpected messages. Reach out to your family member using their usual number first to verify. If you can't reach them normally, consider asking a close friend to confirm the situation.
- If you receive a fraudulent message, send it at no cost to 7726. This service is managed by the Department of Internal Affairs.
- Report a fraudulent mobile number to CERT NZ either on their website or contact them at 0800 CERTNZ.
- Multi-Factor Authentication (MFA): Implement MFA on your bank accounts. Even if a hacker gets your password, they can't access your account without the second authentication factor.
- Refer to our Smishing Defence Strategy Guide for more information and tips.

REFERENCES & RESOURCES

CertNZ https://www.cert.govt.nz/individuals/alerts/mum-i-dropped-my-phone-sms-scam-targeting-new-zealanders/

CyberMaterial https://cybermaterial.com/new-zealanders-targeted-by-family-phone-scam/