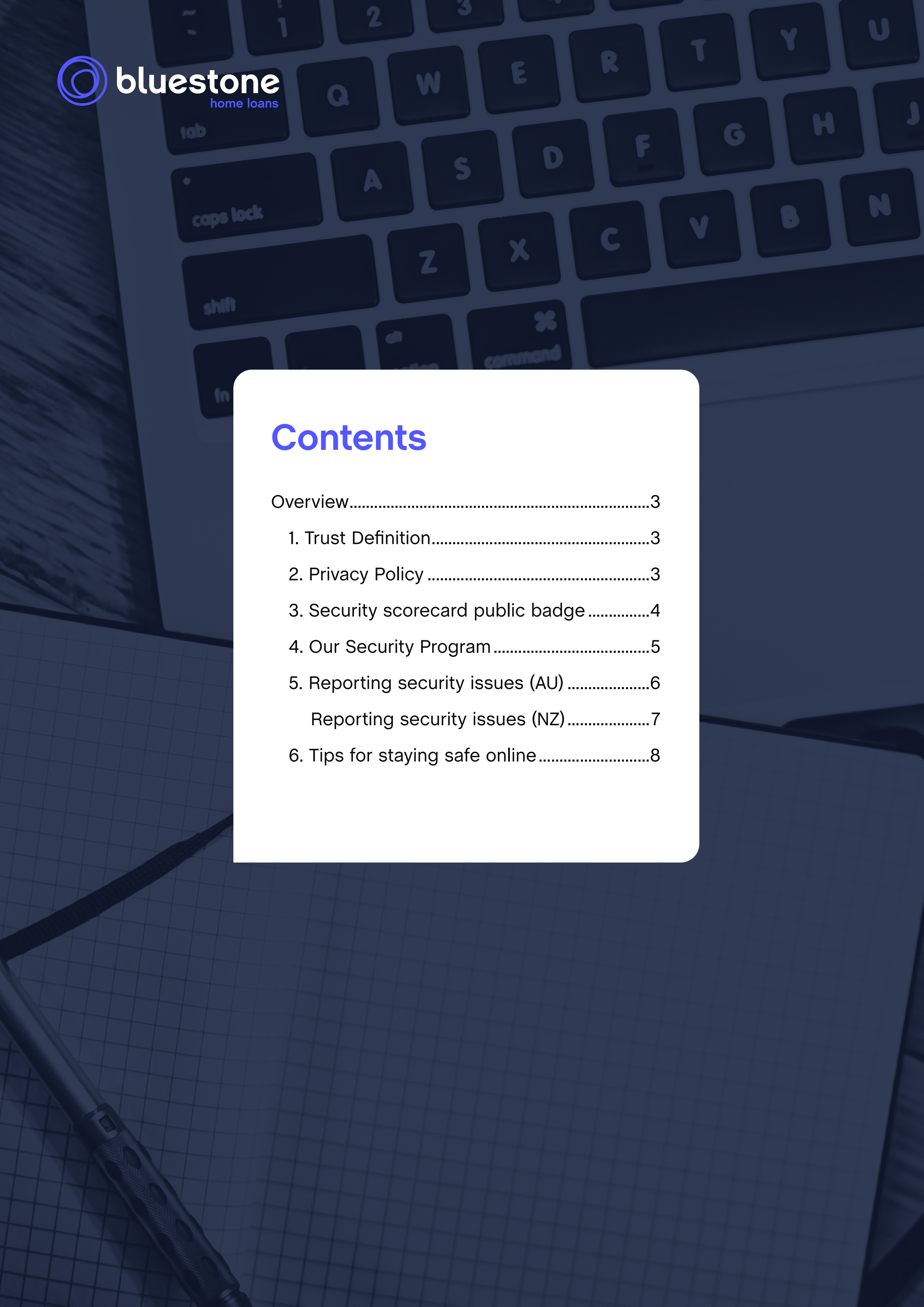
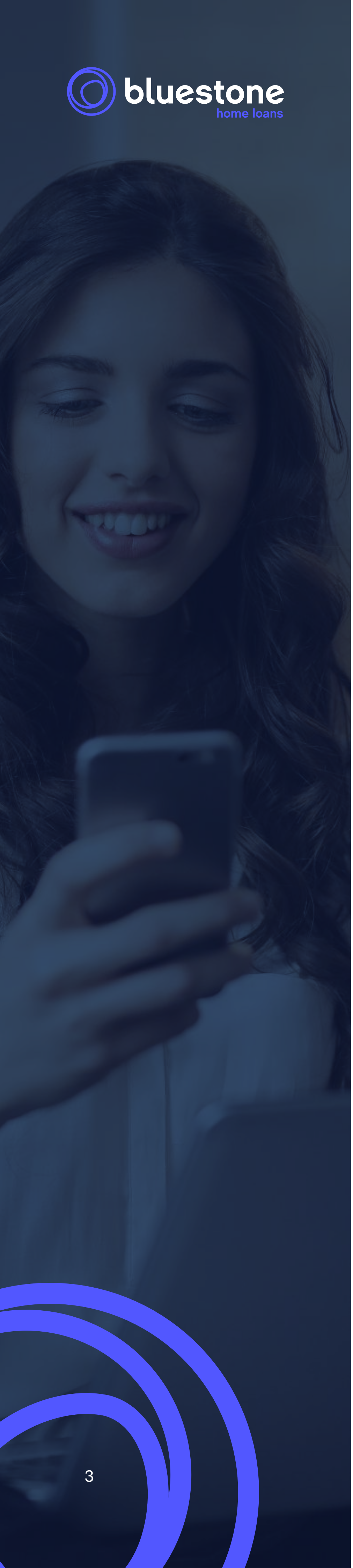
bluestone
home loans

Public information security policy

NOVEMBER 2023



Contents



Overview

Bluestone recognises it has a responsibility to provide safe and secure systems for customers to transact on. We want to demonstrate that we take the security and privacy of your information seriously. We want to earn and maintain your trust and to that end, we provide the following information and tips for staying safe online.

1. Trust definition

1. to have confidence in somebody; to believe that somebody is good, sincere, honest, etc. (Oxford);
2. to believe that something is true or correct or that you can rely on it (Oxford);
3. to believe that someone is good and honest and will not harm you, or that something is safe and reliable (Cambridge).

2. Privacy policy

bluestone.com.au/privacy-policy/ (AU Site)

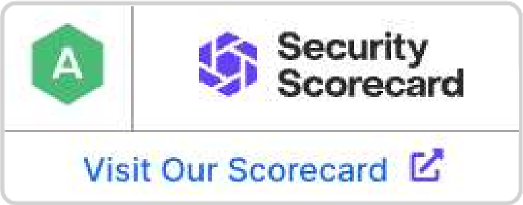
bluestone.net.nz/privacy-policy/ (NZ Site)

3. Security scorecard public badge

We use a 3rd party platform to assess and score our public security posture. Cybersecurity ratings are similar to financial credit ratings. In the same way that a poor credit rating is associated with a greater probability of default, a poor cybersecurity rating can be associated with a higher likelihood of sustaining a data breach or other adverse cyber event.

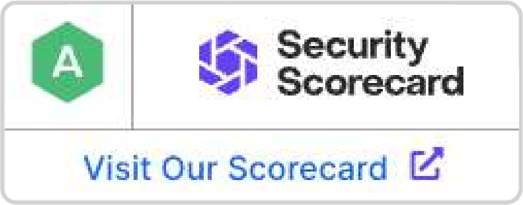
The total score consists of an easy-to-understand letter grade A (100) to F (0) based rating.

Bluestone AU Scorecard



securityscorecard.com/security-rating/badge/bluestone.com.au

Bluestone NZ Scorecard



securityscorecard.com/security-rating/badge/bluestone.net.nz

4. Our Security Program

Our security program is regularly reviewed, tested and improved based on industry frameworks and best practices. Internal and external audits are conducted annually to validate the program's effectiveness.

ISO 27001 is an Information security management standard that structures how businesses should manage risk associated with information security threats; including policies, procedures and staff training. Bluestone is independently audited and ISO 27001 certified.

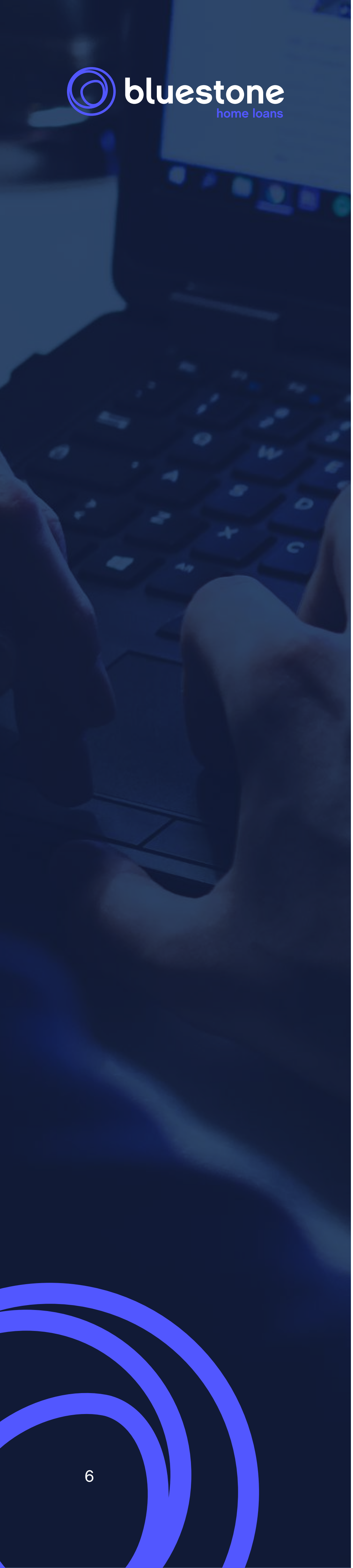
GLOBAL COMPLIANCE CERTIFICATION GCC ISO 27001 Certified

JAS-ANZ WWW.JAS-ANZ.ORG/REGISTER

We recognise that the security of our suppliers can also directly affect us. We have a strong supplier due diligence process in place ensuring that we choose the right partners and are able to continuously monitor their security posture.

Here are just some of the ways we look to protect you and gain your trust:

- Annual Business Continuity Planning (BCP) and Disaster Recovery (DR) testing;
- Centralised and logical access management system;
- Two-factor authentication, encrypted VPN access;
- Denial of Service (DDoS) mitigation;
- Active intrusion detection and prevention;
- Anti-malware software integration that automatically alerts Bluestone's cyber incident response team if potentially harmful code is detected;
- Third-party penetration testing.



5. Reporting security issues (AU)

Security contacts

Need assistance?

Call Customer Service on 13 BLUE (132 583) Monday to Friday **between 8:00am and 8:00pm** AEST to:

- Report a suspicious Bluestone message
- Report unusual activity or unauthorised use of your Bluestone account
- Report identity fraud

You can also report unusual or suspicious activity by emailing us at fraud@bluestone.com.au

Additional Cyber security resources

There are a number of government and not-for-profit initiatives and resources that provide information and updates about cybersecurity risks, trends and staying safe online.

- Australian Cybercrime Online Report Network (ACORN)
- Stay Smart Online
- Scamwatch

You may also want to consider registering for **Stay Smart Online Alert Service**, an Australian Government service designed to alert you of new online threats as they are identified.

5. Reporting security issues (NZ)

SECURITY CONTACTS

Need assistance?

Call Customer Service on 0800 668 333 Monday to Friday **between 8:00am and 5:00pm** NZST to:

- Report a suspicious Bluestone message
- Report unusual activity or unauthorised use of your Bluestone account
- Report identity fraud

You can also report unusual or suspicious activity by emailing us at nzcustomerservice@bluestone.net.nz

Additional Cyber security resources

There are a number of government and not-for-profit initiatives and resources that provide information and updates about cybersecurity risks, trends and staying safe online.

- New Zealand Police - Cybercrime and the Internet
- CERT NZ
- Netsafe

You may also want to consider subscribing to updates on the **Computer Emergency Response Team (CERT)** site, a New Zealand Government service designed to alert you of new online threats as they are identified.

6. Tips for staying safe online

Here are some of the ways you can be cyber safe:

- Never reuse passwords (or passphrases) for different services and websites;
- Create a strong password (or passphrase) and change it if you believe it may have been compromised;

Configure two-factor (2FA) or multi-factor (MFA) for your vital accounts. See **www.cyber.gov.au/mfa** (or in NZ **netsafe.org.nz/2-factor-authentication/** or **www.cert.govt.nz/individuals/guides/two-factor-authentication/**)

- Regularly install device and application updates and patches;
- Keep your digital devices backed up;
- Install and regularly update anti-virus software to reduce the risk of malware being installed;
- Know how to identify spam and phishing emails so you can avoid clicking on those dodgy links.

What is Phishing?

Phishing is a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick you into revealing sensitive information to the attacker or to deploy malicious software (like ransomware) on your device.

How to spot phishing emails?

- Look for incorrect spelling, grammar and other inconsistencies in the email that don't align with the organisation's branding;
- Before you click on the link, hover over it to view the actual address that you will be taken to;
- Don't be fooled by emails that threaten you or seem too good to be true;
- If you're not expecting a message from a person or business, don't click on the links or open the attachments in an email. Reach out to the person or business via other legitimate means;
- Use a spam filter to block suspicious messages from reaching your inbox in the first place;
- Keep in mind that Bluestone will never ask you for your password or codes via email.

www.cyber.gov.au/emailsecurity (AU)

www.cert.govt.nz/individuals/common-threats/phishing/ and **netsafe.org.nz/phishing/** (NZ)

bluestone
home loans

Public information security policy

NOVEMBER 2023