# Scam prevention checklist

Six practical checks to help protect business payments

**BUSINESS OR TEAM**

**DATE**

Tick each item as the policy is put in place. Add owners, follow-up actions or review dates in the notes field.

- [ ] **Verify with a contact you already had**

  Call the supplier using the number in your records or on the supplier website, never the number in the email or invoice. Follow the National Anti-Scam Centre advice: Stop. Check. Protect.

- [ ] **Treat changed bank details as unconfirmed**

  Do not update supplier details in accounting software or online banking until you have spoken to the supplier. After confirmation, consider waiting a day before making the first payment to the new account.

- [ ] **Use two sets of eyes**

  Have a second person approve new payees and changed bank details. In a small team, that might be you and your bookkeeper.

- [ ] **Agree a call-back rule for urgent requests**

  Confirm every urgent request to move money by calling back on a known number, including requests that sound like an authorised approver. Some businesses also use a team code word.

- [ ] **Lock down your email**

  Turn on multi-factor authentication for every account that handles invoices or payments. Keep backups, email security and software updates current.

- [ ] **Brief your team before your busiest weeks**

  Casuals and new starters may not know how the business pays suppliers, so take five minutes to walk the team through these rules.

**NOTES / ACTIONS**

prospa.co.nz/blog/how-to-detect-and-deflect-scams-targeting-your-business

For internal planning only. Always verify payment requests using trusted contact details.