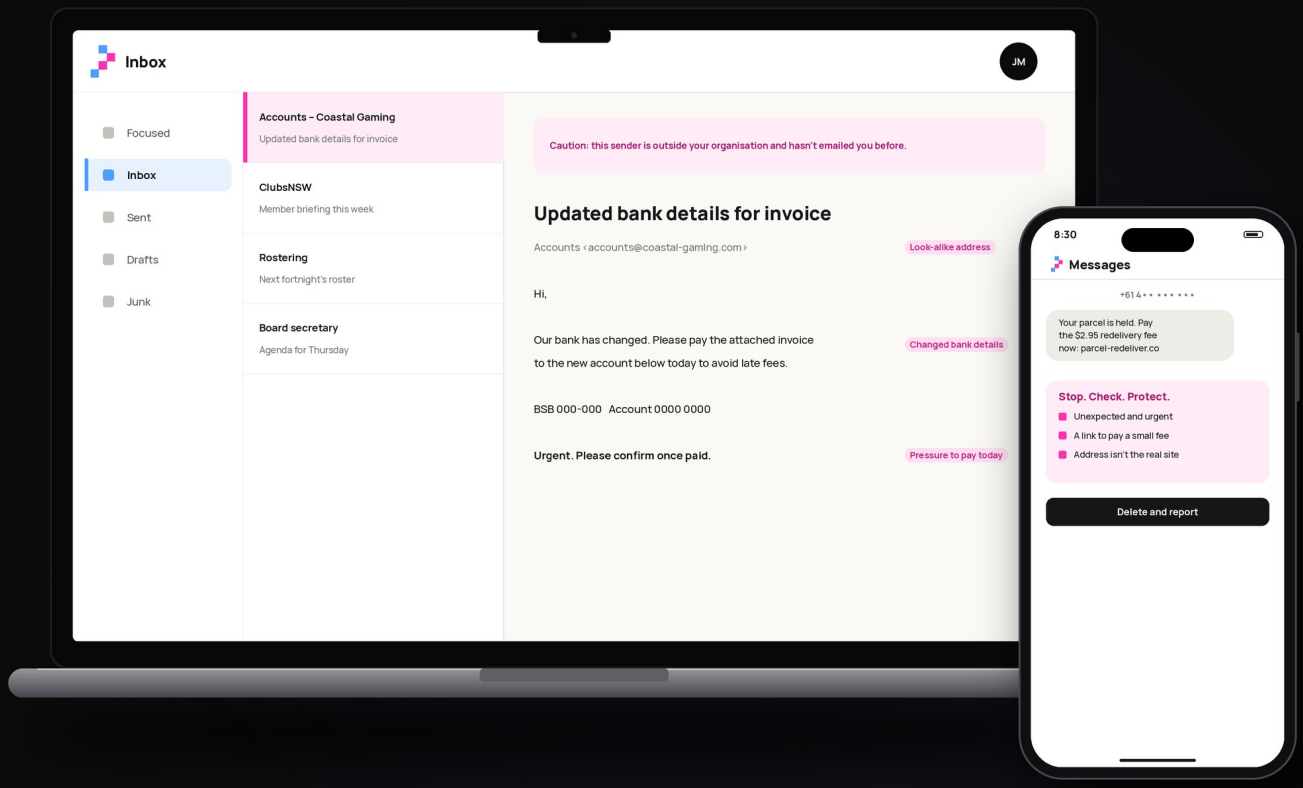


CYBER SECURITY · AS OF NOVEMBER 2026

Cyber basics. Simplified.

The habits that stop most scams and break-ins, and how to spot a phishing email or a fake invoice before it costs you.

John Morgan · Initial Technology · November 2026

THE ONE THING TO KNOW

Scammers don't hack in. They get invited in.

Most attacks on clubs start with a convincing email, text or call. A fake invoice, a changed bank account, a 'quick favour' from the CEO. Good habits stop most of it, and a phone call stops the rest.

SIMPLIFIED

Updates on. Multi-factor on. Backups tested. Staff pause before they click. Phone before you pay.

FIVE HABITS AT A GLANCE

01

Keep everything updated

Phones, laptops, routers, apps.

02

Use strong sign-in

Passkeys or app approval.

03

Back up, then test

If you can't restore it, it isn't a backup.

04

Teach staff to pause

Five seconds beats five figures.

05

Phone before you pay

Any change to bank details.

06

Report it

Fast reports limit the damage.

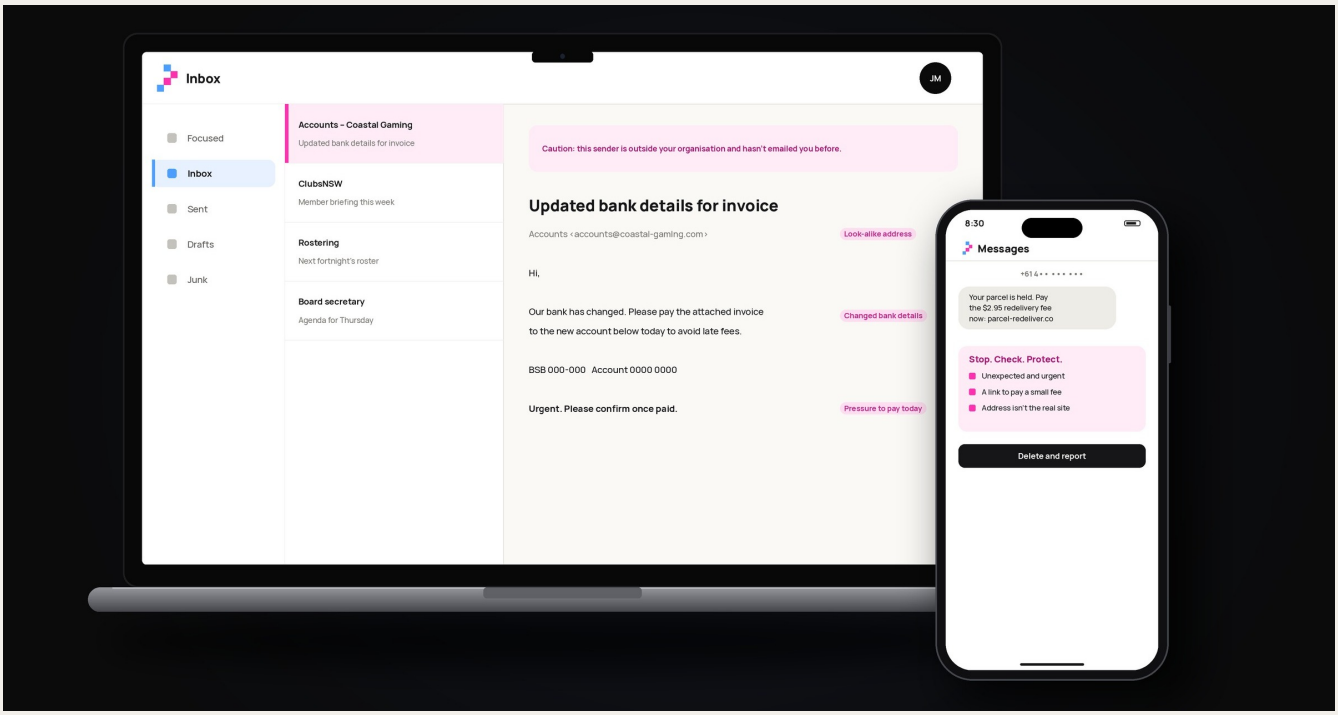


Illustration. Three warning signs in one email: a look-alike address, changed bank details, and pressure to pay today.

STEP 01

Spot a phishing message

Most have at least one of these.

- ☐ **It's urgent.**
  Pay today, act now, account suspended.
- ☐ **It asks for money or a sign-in.**
  Gift cards, bank changes, “confirm your password”.
- ☐ **The link doesn't match.**
  Hover or long-press to see where it really goes.
- ☐ **The sender is almost right.**
  One letter off, or a free email address.
- ☐ **It's unexpected.**
  An invoice you weren't expecting, a parcel you didn't order.
- ☐ **It's from “the boss”.**
  Unusual requests from senior people, often after hours.

HANDY TIP

Real banks, suppliers and the ATO won't mind you hanging up and calling back on a number you already have.

STEP 02

Stop fake invoices and bank changes

Business email compromise is the costliest scam for small businesses.

- [ ] **Phone to confirm any bank change.**
  Use a number from your files, never from the email.
- [ ] **Watch for first-time payees.**
  Your banking app can flag them.
- [ ] **Two people approve new payees.**
  Or any payment over a set amount.
- [ ] **If money's gone, call the bank now.**
  Minutes matter for getting it back.

HANDY TIP

Write your call-back rule into the finance procedure and tell suppliers about it. Criminals move on when it doesn't work.

WRITE IT DOWN

PAYMENTS OVER $ NEED TWO APPROVERS _____

BANK CHANGES CONFIRMED BY PHONE, BY _____

STEP 03

Make staff your best defence

Short, regular and kind beats long and annual.

- [ ] **Ten minutes, every quarter.**
  Real examples from your own inbox.
- [ ] **Make reporting easy.**
  One button in Outlook, or one email address.
- [ ] **Thank people who report.**
  Even when it's a false alarm.
- [ ] **No blame for clicking.**
  Fast reporting matters more than never clicking.

HANDY TIP

Bar and reception staff get scam calls too. Include them, not just the office.

STEP 04

Report it

Fast reports help you and everyone else.

- [ ] **Cyber attacks:** ReportCyber at cyber.gov.au, or ASD's hotline 1300 CYBER1 (1300 292 371).
- [ ] **Scams:** Scamwatch at scamwatch.gov.au.
- [ ] **Stolen identity details:** IDCARE, 1800 595 160.
- [ ] **Personal information exposed:** You may need to notify the OAIC and the people affected.

WRITE IT DOWN

OUR IT PROVIDER'S URGENT NUMBER _____

OUR BANK'S FRAUD LINE _____

Want a quick health check?

I'll look at your email security, sign-in settings and payment process, and give you a one-page list of what to fix. Plain English, fixed price.

0401 539 456 · info@initialtech.com.au · initialtech.com.au

THE SIMPLIFIED GUIDES

Free at initialtech.com.au/resources

01 Microsoft 365 security

02 Cyber basics and phishing

03 Ransomware readiness

04 Backup and recovery plan

05 Incident response

06 Working from home securely

07 Copilot readiness

08 Choosing an IT provider

09 Buying a major system

10 The board technology report

11 Copilot vs ChatGPT vs Claude

Sources, checked November 2026. ASD's ACSC: Small business cyber security guide; Protect your business from email fraud and compromise; ReportCyber and 1300 CYBER1. Scamwatch (ACCC). IDCARE. OAIC: Notifiable Data Breaches scheme. General information only, not legal, insurance or financial advice. Check current details with your IT provider before acting.