valse®

Business Security Quick Check

What you and your team can do today. No purchase, no project.

Email · Links · Browser · Payments · Laptop · Phone · Accounts · Domain

For Everyone in the Team

- [ ] Email **Read the real sender** before acting on any email about money, logins or urgent requests. In Gmail, open the arrow under the name and read `mailed-by` and `signed-by`. Other email apps show this in the message details. The domain should match the company it claims to be.
- [ ] Links **Read the link before you click.** Hover on a computer, or press and hold on a phone. In `yourbank.com.my.login-check.net`, the real site is `login-check.net`.
- [ ] Browser **Type the address yourself** for banking, payment and government sites. Skip the links in emails and messages.
- [ ] Browser **Treat the padlock as privacy only.** It shows the connection is encrypted. It does not show that the site is honest.
- [ ] Payments **Check the address bar on every payment page** before entering a login or card details. The address should be your bank's or the payment provider's own.
- [ ] Laptop **Paste nothing a web page asks you to.** A real captcha never asks you to press Windows + R, open Terminal or paste a command.
- [ ] Payments **Call back on a number you already have** before changing any bank details. A real mailbox can be taken over, so a real sender does not prove a real request.

For the Owner

- [ ] Accounts **Turn on two-step login** for company email, banking, domain and social media accounts.
- [ ] Browser **Stop saving passwords in the browser** for those same accounts.
- [ ] Laptop + Phone **Remove browser extensions and free apps** nobody in the team recognises.
- [ ] Email **Check forwarding rules** on the owner and finance mailboxes. Delete any rule nobody remembers adding.
- [ ] Accounts **Remove access** for staff and vendors who have left: email, banking, website, domain and social media.
- [ ] Domain **Check who holds your domain** and when it expires, with the free WHOIS tool.
- [ ] Email **Check your email protection** with the Email Protection Check. Enter your domain and it tells you, in plain words, what to ask your email provider.

If Someone Already Clicked

- [ ] Laptop + Phone **Disconnect that device from the internet.** Keep it switched on for checking.
- [ ] Accounts **Change passwords from another device,** starting with email and banking.
- [ ] Accounts **Log out of all sessions.** A stolen login session can keep working after a password change.
- [ ] Email **Check that mailbox** for new forwarding rules.
- [ ] Payments **If money moved, call your bank's scam hotline or NSRC at 997 at once,** then lodge a police report.
- [ ] Report **Report the incident to Cyber999:** 1-300-88-2999 (office hours) or cyber999@cybersecurity.my

General guidance only: the steps differ by email provider and device.