Cyber culture checklist

A simple way to build safer habits at work

Cyber security isn't just about systems - it's about how people work together. This checklist helps you reflect on everyday behaviours, expectations and norms that reduce cyber risk and make it easier to catch problems early.

You don't need to tick every box.
Use it to start conversations and identify where small changes can make a big difference.

1. Speaking up feels safe

□ Staff know it's okay to question unusual requests
□ People aren't worried about "getting it wrong" or being blamed
□ Asking for verification is encouraged, not seen as inconvenient
□ Near-misses are discussed as learning moments

If this isn't happening yet: Start by openly thanking people who raise concerns - even when it turns out to be nothing.

2. Verification is normal

□ Changes to payment or bank details are always verified
□ Urgent requests are double-checked using known contact details
□ Staff understand that urgency is a common scam tactic
□ Verifying requests is built into everyday workflows

Tip: Verification isn't about mistrust - it's about protecting everyone involved.

3. Responsibility is shared

□ Cyber safety isn't seen as "just IT's job"
□ Finance, admin, reception and managers all know their role
□ New staff are told it's okay to slow things down if unsure
□ Leaders model the behaviours they expect from others

Remember: The first person to notice something feels off is often the one closest to the task.

4. Impersonation risks are understood

□ Staff know that scammers impersonate real people and businesses
□ Changes in tone, timing or process raise questions
□ Brand, supplier and identity trust isn't assumed automatically
□ People know that scams don't always look "obvious"

Reality check: Today's scams often look professional, familiar and convincing.

5. Escalation pathways are clear

□ Staff know who to talk to if something feels wrong
□ Escalation doesn't require certainty or proof
□ Concerns can be raised quickly and informally
□ There's no pressure to "just deal with it" alone

Good practice: If people hesitate because they don't know who to tell, risk increases.

6. Reporting beyond the business is understood

□ Staff know that suspicious patterns can be reported externally
□ Reporting isn't only for confirmed losses
□ Reporting is seen as helping others, not getting someone in trouble

If patterns or impersonation attempts could affect others, they can be reported anonymously to Crime Stoppers SA by calling 1800 333 000 or online at https://crimestopperssa.com.au

Use this checklist as a conversation starter. You don't need to score yourself. Instead, ask:

- Where are people unsure?
- Where might silence creep in?
- What would make it easier to speak up early?

Strong cyber cultures aren't built overnight - they're built through everyday behaviours, clear expectations and supportive leadership.

Protect your business. Empower your people. Speak up early.