When staff raise cyber concerns

When a staff member speaks up about something that doesn't feel right, the first response they receive matters. Handled well, it strengthens trust and prevents future risk. Handled poorly, it can silence people next time.

This guide outlines simple, practical ways leaders and managers can respond when staff raise cyber concerns or near-misses.

1. Thank them first
Start with appreciation, even if it turns out to be nothing.
Simple responses like:

- "Thanks for raising this."
- "I'm glad you said something."
- "You did the right thing by checking."

This reinforces that speaking up is valued.

2. Slow things down
Resist the urge to rush or minimise the concern. Even if the issue seems small:

- Pause any related action
- Avoid pressure to "just get it done"
- Create space to review calmly

Urgency is often what scammers rely on. Leaders should model the opposite.

3. Don't expect certainty
Staff don't need proof, answers or technical knowledge.
If someone says: "I'm not sure, but something feels off"
That's enough. Treat uncertainty as useful information, not a weakness.

4. Verify calmly and visibly
Take simple, sensible steps to check:

- Use known contact details
- Confirm requests through a second channel
- Ask clarifying questions

Where possible, involve the person who raised the concern so they can see that verification is normal and supported.

5. Avoid blame or embarrassment
Never respond with:

- "You should have known"
- "That was obvious"
- "Why didn't you...?"

Even casual comments can discourage future reporting. Focus on processes and patterns - not individual fault.

6. Share learnings, not mistakes
If appropriate, share the takeaway with the team:

- What was noticed
- What helped catch it early
- What to watch for next time

This turns a near-miss into collective learning, without naming or shaming.

7. Know when to report externally
If a concern involves:

- Impersonation
- Repeated suspicious behaviour
- Patterns that could affect others

It may be appropriate to report it anonymously to Crime Stoppers SA by calling 1800 333 000 or online at https://crimestopperssa.com.au

The takeaway for leaders
Strong cyber cultures aren't built through policies alone. They're built when leaders listen, take concerns seriously and make it safe to speak up - every time. Your response today shapes whether people speak up tomorrow.

Protect your business. Empower your people. Respond early.

Pause. Probe. Protect

Cyber security is a shared responsibility

CRIME STOPPERS .com.au 1800 333 000 South Australia