# Cybersecurity Conversation Starters

**How to Use:**

*These questions fit naturally into weekly team meetings, toolbox talks, or monthly check-ins. The goal is open, positive dialogue — building a security culture without blame. Each one includes a simple coaching tip to guide a quick, practical conversation.*

1

## When was the last time you changed your work password?

Remind staff that passwords should be changed regularly — not just when forced by IT.
Introduce password managers as an easy way to create and store strong, unique passwords.

2

## If your laptop or phone was stolen, what would you do first?

Emphasise the need for immediate reporting, using remote wipe tools if available, and making sure device encryption is turned on before it's needed.

3

## If you got an urgent email from the CEO asking for a money transfer, how would you verify it?

Teach staff to always verify high-risk requests out-of-band — like calling a known number directly — and to never trust urgent requests received only by email.

4

## Have you spotted any phishing emails or scam texts lately?

Encourage sharing real examples. Praise those who spotted scams — reinforce that vigilance is a positive team habit, not about fear.

5

## If we had a cyber incident today, what's the first thing you would do?

Connect this question back to your incident response plan. Focus on calm reporting, isolating the problem, and following a clear process — not trying to fix everything individually.

**Pro Tips for Using These Starters Effectively:**

- Stay positive. Focus on learning and improvement, not blaming mistakes.
- Keep it short. 5–10 minutes per discussion is enough — no lectures.
- Encourage stories. Let people share real examples they've seen — it makes the learning stick.
- Reward participation. A simple "great catch!" or casual praise keeps engagement high

mindsetcyber.com.au