KAREN STEPHENS

Karen Stephens is the co-founder and CEO of BCyber. After more than 25 years in financial services, Karen moved into SME cybersecurity risk management. She works with SMEs to protect and grow their businesses by demystifying the technical aspects of cybersecurity and helping them to identify and address cybersecurity and governance risk gaps. She was recently named inaugural Female Cyber Leader of the Year at the 2023 CyberSecurity Connect Awards in Canberra.

COLUMN

"Upon the conduct of each depends the fate of all" (Alexander the Great)

Welcome to 2025! Hasn't the year started with a bang?

We have been greeted with "Australia has become a 'honeypot' for bank scammers and the world is laughing." But wait, if you are scammed: "The chance of you getting your money back …[is] dire." I have seen the truth of this with my own eyes, and it isn't pretty. The whole cybersecurity "doom and gloom" theme appears to be centred around "you're on your own" rather than focussing on what we can do as a collective.

Cybersecurity risk management solidarity needs to become a thing. It needs to become our thing!

There has never been a 'silver bullet' for cybersecurity risk management. Nor is it possible to have one person or business fix everything for everyone. Alas, it is unlikely the people who are most vulnerable to a cyber breach are reading this (eg the 4.2 million retirees or the four percent of the population that does not work, or our 4.1m school children. Need I go on? This is where you and your personal network come into play.

By us all making and sharing a few basic changes, our cyber resilience as a community will improve. So, let your cybersecurity risk management solidarity journey start today with three free 'fixes' you can pass on to everybody.

1. **Go beyond the tech.** Accept that cybersecurity is not just a tech problem. While this sounds easy it (unfortunately) is not. It has been my experience that, when a breach occurs, the first thought is "it is a software security fail" when, usually, it is a person who has either been too trusting, too distracted and done something they should not have, or someone who decided to be nefarious. Security software cannot fix those issues. *The fix to share:* think beyond the security software. Don't accept unknown calls (that's what voicemail and number blocking are for) or unexpected emails (that is what the preview is for, quickly followed by blocking and deleting). Don't engage. EVER! **Your trust is valuable - don't just give it away.** In the 'good old days' you

2. basically trusted all and sundry from the get-go and if they did something wrong, you blacklisted them, in life

or in cyberspace. Unfortunately, if the rise in cybersecurity breaches has taught us anything, it's this: you should trust no one immediately. Let them prove themselves worthy of your trust.

The fix to share: when you get an email, text or call purporting to be from a trusted source (eg a bank, the ATO, etc) do your own due diligence e.g. Don't respond to the email/text or answer the call and call them back on a number you know to be correct. Remember, criminals hide in plain sight, and they sound like us.

3. **Good cyber hygiene - boring but necessary.**
Cyber hygiene should start from the very first time a device is put into anyone's hands, because practice makes perfect.

The fix to share: use passwords with 16+ complex characters that are never reused or shared and manually check that the patches of all your devices (phones, iPads, laptops, etc) are up to date. Sometimes 'auto patch' is not really automatic.

And now for your homework.

I have done my bit by providing you with some nice easy foundational steps for our cybersecurity risk management solidarity journey. It's now up to you. Your mission (and there is no refusing it I'm afraid) is to raise these first steps with three people you know. Then have them raise these steps with three people they know, and so on. Who knows, by this time next year cybersecurity risk management solidarity might not be only a thing; it might be a way of life.