XEROCON SYDNEY 2023

Cybersecurity trends you need to know about

Top takeaways from this session

1. **As accountants and bookkeepers, you're working day-to-day with sensitive data** — both financial and personal information. That's the data cyber criminals want to get their hands on. So it's vital that you get a plan together to protect yours and your clients' data .
2. We're seeing **evolving access to cybercrime tools and a rise in ransomware as a service.** With a reduced barrier to entry, cyber criminals don't need to concentrate their efforts on bigger businesses with large amounts of data — small businesses are more attractive.
3. **AI might help cyber criminals — as they have the potential to do more, with less.** But this doesn't mean we have to throw out existing cybersecurity advice on best practice. If anything, it's more important than ever to get the basics right.

Key things to do back at the office

- Undertake a risk assessment for your practice, to know where to focus your efforts. The Australian government's risk assessment quiz is a great resource.
- Check your passwords: they should be long, complex and unique to every account. Use password managers — they'll do the hard work of making up and providing strong passwords for you.
- Turn on multi-factor authentication (MFA) wherever possible.
- Develop privacy policies in your practice to include what data you collect, why you collect it, how you intend to use it and how long you intend to hold it for.
- Invest in secure data storage, with access and sharing set up only for those who really need it. Make sure it's backed up regularly — this is what you'll revert to if you lose your access.

Resources, books, blogs

- If you operate a business in Australia, make sure you're familiar with your obligations under the Notifiable Data Breaches scheme.
- For more guidance or to report cyber security problems, visit: CERT NZ, Australian Cyber Security Centre, or the Cyber Security Agency of Singapore.