

FAAA CONGRESS 2026 | MORRIS'S FIELD NOTES

AI for Good, AI for Bad

Field Notes

The research behind the FAAA Congress 2026 session, by Morris Misel

Panel session: Thursday 26 November 2026, 8.45 to 10.00 am, Melbourne Convention and Exhibition Centre

The research that led up to the session, written before it. Facts checked on 8 and 12 November 2026.

Morris Misel

Business Futurist | Keynote Speaker | Author | Founder, Think-Along AI

A free download for FAAA Congress 2026 delegates

IMMEDIATE FUTURES™ *with* MORRIS MISEL

Illustration made for these notes: a practice room, with no people, faces or brands.

A note from me



Morris Misel
Business Futurist | Keynote Speaker | Author | Founder, Think-Along AI

Thank you for spending part of your Congress morning with us, and for the questions you brought into the room.

On stage at FAAA Congress 2026 I moderated a panel with James Ng from Insignia Financial and Rob Smith from NAB, two people who spend their working days keeping the bad guys out.

These are my field notes: what I was reading and gathering in the weeks before we went on, pulled together in one place, so you've got the research behind the session to keep and come back to.

Every figure about the threats has its source and its date beside it, so you can check anything I've said, and I suspect a few of you will.

If you run a small practice, you probably don't have a security team, and you certainly don't have time to read every alert that lands in your inbox, so I've tried to put the useful parts where you can find them quickly.

It starts with people, because that's where most of this trouble starts, and it finishes with a plate of eight plain habits and a checklist you can pin up beside the kettle.

Have a read when you've got a quiet few minutes, and if one thing on the checklist catches your eye, that's a fine place to start.

Choose forward,



Morris Misel
Business Futurist | Keynote Speaker | Author | Founder, Think-Along AI
morris@morrisfuturist.com

About these notes

Field	Detail
Prepared for	Delegates at FAAA Congress 2026, for the panel session "AI for Good, AI for Bad: cyber threats, deepfakes, regulation and the future of trusted advice"
Author	Morris Misel, Business Futurist | Keynote Speaker | Author | Founder, Think-Along AI. Moderator of the session.
Written	8 November 2026; updated 12 November 2026 to match the final slides
Facts checked	8 November 2026, and 12 November 2026 for everything added since. Every figure about the threats carries a numbered reference to a named source and date. Each reference says whether it was checked live that day or comes from a file I've kept.
Status	General information. Not financial, legal or compliance advice.

It's my view of the issues we put on the table, built on public research and the content the panel agreed for the day.

The panel was James Ng, Chief Information Security Officer (CISO), Insignia Financial, and Rob Smith, Acting Chief Security Officer, Group Security, NAB, with me in the moderator's chair.

The views are mine, not NAB's, Insignia Financial's or the FAAA's.

Anything I couldn't check is left out, and the back pages list what and why.

CONTENTS

A note from me 2
The short version 4
1. The way in was a person 5
2. What AI has changed, and what it hasn't 6
3. What's at the door: the eight threats 7
Can you tell who's knocking? (one-page sheet) 13
4. What's moving now, beyond the slides 14
5. Back at the practice: the eight basics 16
6. The floor: regulation and privacy 20
7. Immediate futures 21
8. Where to go next, and if it happens to you 22
Keep going with me 24
The bookshop 25
References 26
How I chose what went in 28
About Morris, and the fine print 29

The short version

IN SHORT AI has made criminals faster and more convincing, but they still come through the same old doors, and the same plain habits still keep them shut.

6 minutes

On average, how often a cybercrime report reached ReportCyber in 2025-26: over 82,000 reports in the year

ASD, 26 Oct 2026 [2]

$55,400

Average self-reported cost per cybercrime report for a small business, 2025-26

ASD, 26 Oct 2026 [2]

$2.18 billion

Reported lost to scams in Australia in 2025, combined data, up 7.8%

NASC, March 2026 [3]

Most small advice practices don't have a security team. They have a couple of advisers, someone on the front desk, a handful of software subscriptions and a lot of trust from their clients.

That trust is what the scammers are after, and AI lets them try more often, and with a far more convincing face.

The Australian Signals Directorate (ASD) calls AI "the defining force" in cyber threats over the past year, and says attackers can use it to launch attacks "at greater scale than ever before".[1] ASIC and APRA say much the same about the financial system.[6]

For a practice of five people, the good news is that the ways in are still mostly the old ones, like a message, a link, a call, a supplier or a payment request that looks right.

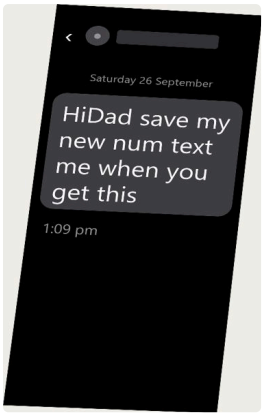
Which is why we started where the FAAA starts, with its own line: eat your cyber vegetables first.[17] It's the plain end of cyber, and I think it's the end that does most of the work.

My field notes follow the same themes we covered on stage:

- First, what's at the door, eight ways in from phishing to ransomware, each with its tell and a public example.
- Then back at the practice, eight basics in the order the panel agreed, with a checklist you can print.
- The floor, which comes down to two dates. On 27 August 2026 ASIC and APRA asked firms to move from awareness to action. From 10 December 2026, organisations covered by the Privacy Act must say in their privacy policy when they use personal information in automated decisions that could significantly affect people.
- And immediate futures, one thing to do before you're back at your desk, and the habit that keeps you safer after the next change.

The checklist in section 5 is a good place to land, and ticking what you've already done will show you quickly where the gaps are.

1. The way in was a person

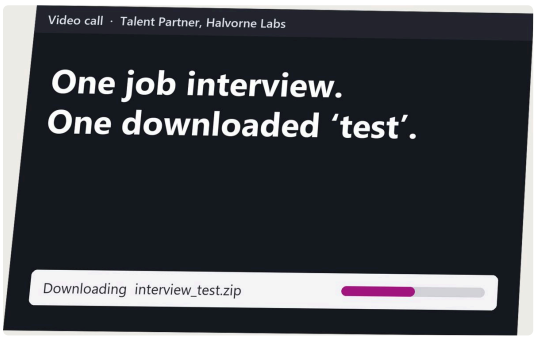


On Saturday 26 September a text arrived on my own phone. It read, word for word: "HiDad save my new num text me when you get this".

No name, no number I knew, and no reason to doubt it if you're a dad with kids who change phones, which is exactly what it's counting on.

A real message to Morris's phone, 26 September 2026. Number removed.

It's an old trick with a new coat of paint, where somebody you love has a new number and wants a small favour, and the first message asks for nothing but a reply, because a reply is all it needs to get started.[18]



The second story cost a great deal more. Binance, the world's largest crypto exchange, says attackers used fake job interviews and malicious code to take its funds.[5]

Illustration made for these notes.

Binance says an engineer was approached through a legitimate job-search site, about a role at a company that didn't exist. The "recruiters" built trust over time, then asked for a test exercise to be downloaded as part of the interview. The test carried the malware.[5]

The size of it: more than US$6 billion, about A$9 billion, as ABC News (AFP) reported it on 4 November.[5] Figures for the theft vary between outlets, so I use the figure all reports support. ABC also reported that Binance says 98 per cent of the affected assets have been recovered by drawing on its own funds.[5]

In Binance's account, the engineer downloaded a file that looked like part of the interview, and that gave the attackers their way in.

Two stories, and in both somebody got a believable request through a channel they trusted, and said yes. When you're on the other end of a screen, you can't always tell who, or what, is asking.

I started with people because your clients trust you and your staff trust each other, and that trust is exactly what gets copied.

2. What AI has changed, and what it hasn't

CHANGED	NOT CHANGED
Scale	**The ways in**
Sophistication	**Your judgement**
Speed	**The basics**

The session's own summary (stage deck, agreed for the session, 7 November 2026).[17]

What has changed

The ASD's Annual Cyber Threat Report 2025-26 puts it plainly. It calls AI "the defining force in the cyber threat landscape over the past year", letting attackers find weak spots faster and use them at a scale, speed and sophistication it says have no precedent.[1]

The same report says defenders used to have months to patch a known hole, and now they have days, sometimes only hours.[1]

Scale just means a lot more messages going to a lot more people, and the ASD says attackers can now use AI to launch attacks "at greater scale than ever before".[1]

Sophistication means the clumsy giveaways are harder to find. The email can read like your client wrote it, the website can look like the real one, and a phone or video call can now be faked.

Speed means the gap between a weakness being found and being used against you is shorter than your next software update, unless that update is set to run by itself.

What hasn't changed

The ways in are mostly the old ones. A message that wants you to click, a caller who wants you to act, a supplier who holds your data, a payment that goes to the wrong account.

The National Anti-Scam Centre's figures show it. The biggest reported losses in 2025 came from investment scams, payment redirection, romance scams, phishing and remote access scams, and those five made up 60 per cent of all reported losses.[3]

Your judgement hasn't changed either, so the pause, the second look and the call back on a number you already have are all still yours, and I'd say AI has made that pause worth more than it was.

And the basics haven't changed. The Australian Cyber Security Centre (ACSC) still starts small businesses with three things: multi-factor authentication, software kept up to date, and regular backups.[11]

Eat your cyber vegetables first

That's the FAAA's own line for the session, and I think it's the right spine for all of it.[17]

Broccoli isn't exciting, but when I look at how most of these stories begin, a few plain habits would have stopped a good many of them.

So the questions we put on stage were plain ones: what's actually knocking, how would you know, and what would a practice of five people do about it tomorrow?

3. What's at the door: the eight threats

IN SHORT Plenty of people will knock, and not all of them are who they say they are. Eight ways in, starting with phishing, the most reported scam type, and ending with ransomware, each with its tell.



The session used a front door as its picture of the practice. Anyone can knock, so what we looked at was how you'd tell who's there before you open the door.

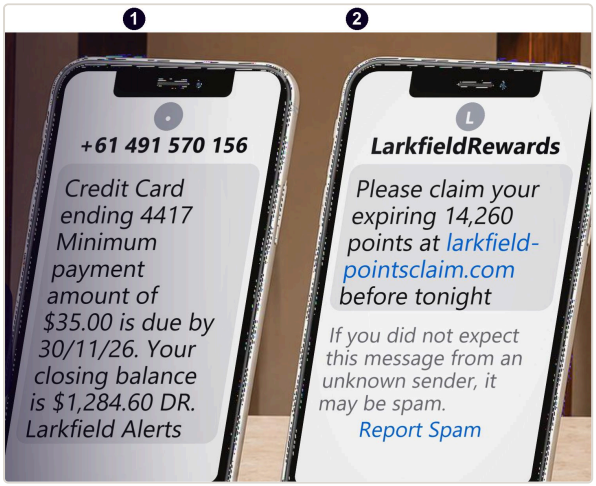
Below are the session's eight, in the wording and order the panel agreed,[17] each with a public example and its source wherever I could find one I could check.

At home we love watching Is It Cake?, where you guess which thing on the table is real, and the session played its own version, real or fake, twice: once with the two texts under phishing, and once with a voicemail. The other pairs didn't go up on stage, so they're here for you to try. All of them were recreated from real ones, with names and numbers changed, so you can look for the signs yourself. The answer under each one points to the warning signs; it isn't proof that the other one is safe.

Illustration made for these notes.

1 Phishing

The most reported scam type.



Recreated from a real example; names and numbers changed

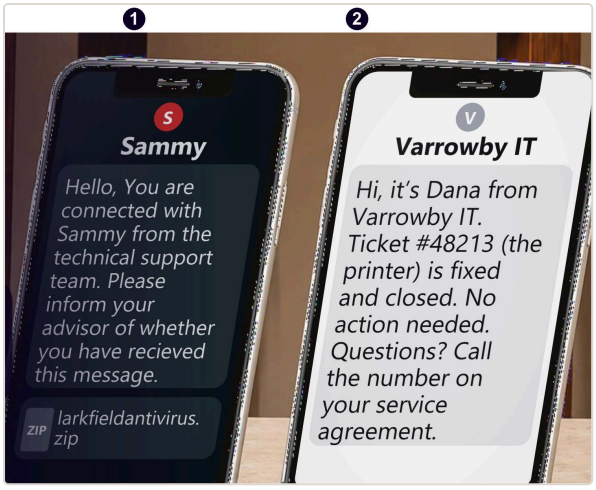
The answer: 2 is the fake. It has a sender name instead of a number, a deadline of tonight and a web address that's nearly right, while 1 asks you for nothing.

A message, by email or text, that wants you to click a link, open a file or log in somewhere. Usually it's the hurry that gives it away, or a reward or a threat, and a web address that's nearly right. I wouldn't act on the message; I'd check with the organisation using details I already have.

In 2025 phishing was the most reported scam to Scamwatch, with 65,361 reports.[19] It was also one of the five scam types with the biggest reported losses in 2025, at $97.6 million.[3] The ACSC's handbook asks small businesses to train staff to spot scams and phishing emails.[11]

2 Impersonation

Someone you trust, or someone you'd like to.



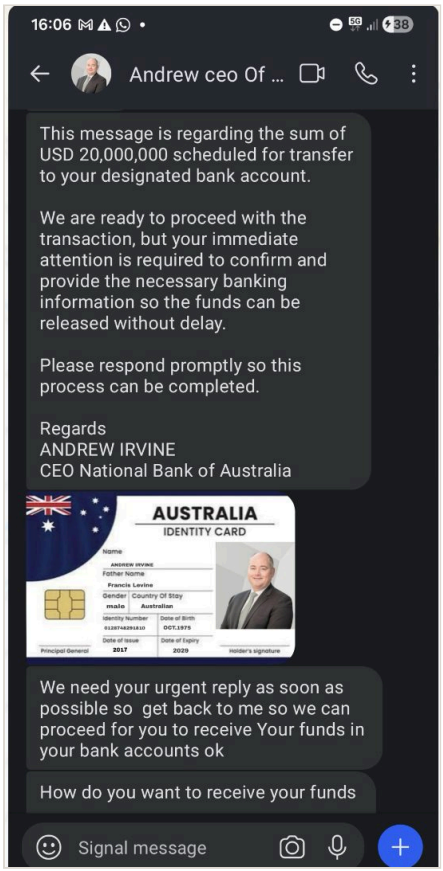
Recreated from a real example; names and numbers changed

The answer: 1 is the fake. It sends you a file over a chat app and asks you to tell your adviser, while 2 is about a ticket you raised and sends you to a number you already hold.

A message that looks like it comes from a colleague, a client, a family member or a provider, often on a new account or a new number. My "Hi Dad" text is this one.

You'll usually notice a familiar name reaching you in an unfamiliar way, with a small, reasonable ask that grows. I'd reach the person through a channel you already had.

The example the session shows for this one is NAB's, below, and if time allows on the day it's followed by the Binance job interview from section 1, where the person being copied was a recruiter, somebody the engineer would have liked to trust.



NAB has also seen a Signal message from "Andrew, CEO of National Bank of Australia", with the bank's name wrong, US$20 million waiting and a request for banking details.

Supplied by NAB. An example NAB shared for this session.

3 Cloned voices and faces

A phone or video call can now be faked.

The voice sounds like your client, or the face on the video call looks like your principal. This is where AI's "sophistication" shows up at the front desk.[1]

Watch for the pressure, and for someone wanting money or access, or wanting you to keep quiet about it. I'd hang up and call back on a number I already have before anything moves.

On stage we played a voicemail made for the session, from a caller who doesn't exist, in a hurry and wanting his bank details changed. You can't tell by the voice any more, so I'd judge the request.

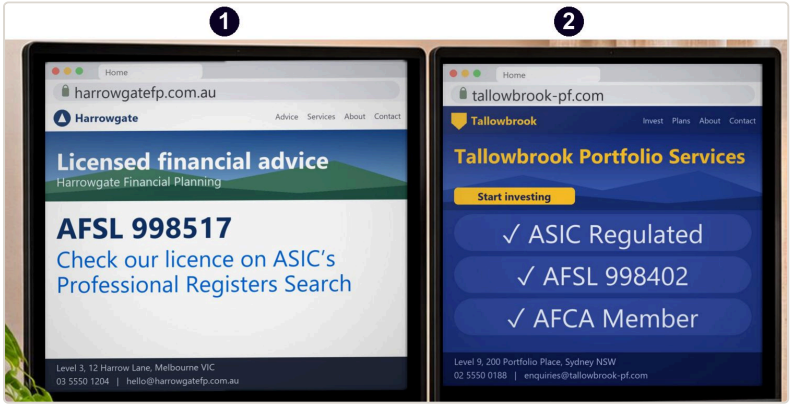


NAB has seen a Facebook ad that borrows the face of its former chief economist, Alan Oster, to draw people into a free "stock tips" WhatsApp group, where the grooming starts slowly and in a friendly way. One line from that chat says it all: "as you follow my investment strategies, trust will gradually build."

Supplied by NAB. An example NAB shared for this session.

4 Fake websites

Using a real licence number and address.



Recreated from a real example; names and numbers changed

The answer: 2 is the fake. Anyone can copy a licence number, and 2 dresses it up with badges ASIC doesn't issue, while 1 sends you to check it yourself on ASIC's register.

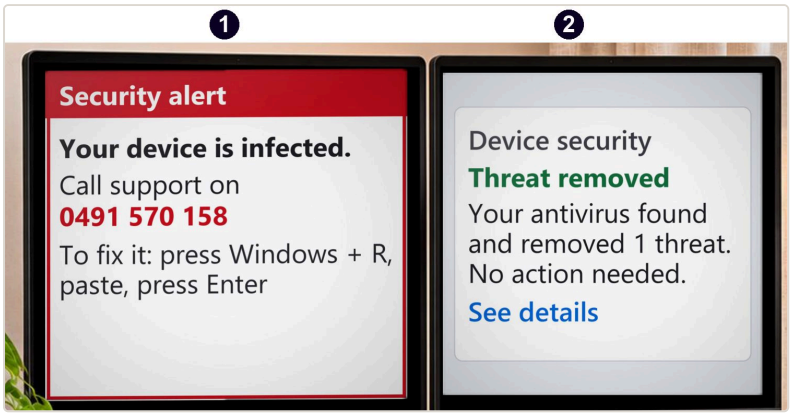
A polished site that borrows a real business's licence number and address, so a quick check seems to pass. Your clients may find it before you do.

The contact details give it away. I'd look the licence up myself on the regulator's own site, and use the phone number and address I found there, not the ones on the page.

---

5 Fake "fix this" pop-ups

Dressed up as a real company.



Recreated from a real example; names and numbers changed

The answer: 1 is the fake. It gives you a phone number and asks you to paste a command, while 2 asks for nothing and opens your own security app.

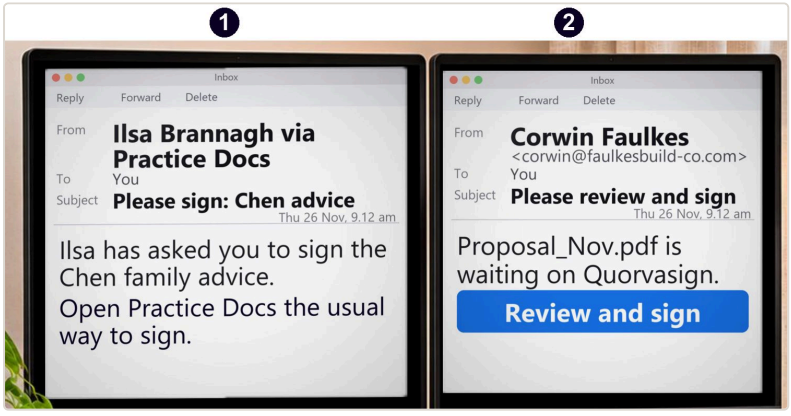
A pop-up says your computer is infected and gives a support number to call. Scamwatch has warned about these for years: they often borrow the look of Microsoft or Apple, then the "support" person asks for remote access.[12] It's the same trick, still running.

A newer version asks you to paste and run a command yourself. In May 2026 the ACSC warned of a campaign using fake "verify you are human" prompts on hacked websites of real Australian businesses, which installed malware that steals information. I wouldn't call or paste anything; I'd close it and open my own security app.[13]

---

6 Business email compromise (BEC)

An email from someone you deal with, asking you to sign or pay.



Recreated from a real example; names and numbers changed

The answer: 2 is the fake. It comes from an outside address and a signing service you don't use, while 1 is a colleague in your own system, sending you there the usual way. Even so, a familiar name or a message that looks internal isn't proof on its own, because accounts get taken over.

Someone takes over a real email account, or sets up one that looks like it, and uses it to redirect payments or requests. Often it starts with a request to sign something, and the link leads to a lookalike sign-in page.

On stage James walked us through how it usually plays out, and the slide had it in three steps:

1. They get a login.

2. They sit in the mailbox, quietly.
3. At the right moment: "new bank details".

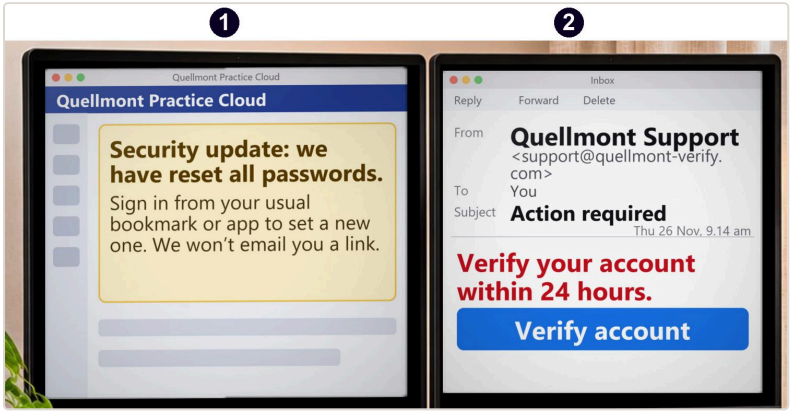
The ACSC's handbook describes it the same way: criminals "gain access to legitimate email accounts and use them to send fraudulent requests".[11,17]

I'd be wary of any request to change bank details, sign something you weren't expecting, or log in to see a shared file. Payment redirection scams were the second largest reported loss in 2025, at $166.8 million.[3]

---

7 Supplier and software risk

Where much of a small practice's data lives.



Recreated from a real example; names and numbers changed

The answer: 2 is the fake. It uses a lookalike address, a 24-hour deadline and a link to verify, while 1 sends you to your own bookmark.

Most small practices keep their client files with other people: the planning software, the cloud drive, the email provider, the paraplanner. If they're breached, your clients' details can go with them.

A public example from outside the advice sector: youX, a software platform used for vehicle finance. CarExpert reported in February 2026 that about 230,000 Australian driver licences were reportedly exposed when the firm was breached.[14]

---

8 Ransomware

A top threat to professional services.

Criminals lock or steal your data and demand payment. CyberCX says cyber extortion was the most common incident type in its own incident work in 2025, and that financial and insurance services was the most affected sector, at almost one in five incidents.[4]

How does it get in? The ACSC's handbook says ransomware "commonly spreads through: phishing emails, malicious links, unsafe websites, compromised accounts, infected downloads". It isn't only locked files any more, either: criminals "may also steal business information and threaten to publish or sell it".[11]

The case the advice world should know is FIIG Securities, an Australian fixed-income specialist and financial services licensee. ASIC says about 385 gigabytes of data was stolen in a 2023 attack, and about 18,000 clients were notified.[10]

ASIC's focus was the licensee's duty to be prepared, and what the Federal Court did about that is in section 5.

Where the money went: reported scam losses, 2025



Source: National Anti-Scam Centre, Targeting scams, report on scams data and activity 2025, March 2026. The top five made up 60% of total reported losses of $2.18 billion.[3]

Can you tell who's knocking?

The eight from section 3 on one page. Print it and keep it by the front desk.

	Who's knocking	What gives it away	What I'd do
1	**Phishing** *A message that wants you to click, open a file or log in.*	The hurry, a reward or a threat, and a web address that's nearly right.	Don't act on the message. Check with the organisation using details you already have.
2	**Impersonation** *Someone you trust, or someone you'd like to.*	A familiar name reaching you in an unfamiliar way, with a small ask that grows.	Reach the person through a channel you already had.
3	**Cloned voices and faces** *A phone or video call can now be faked.*	Pressure, and someone wanting money, access or secrecy.	Hang up and call back on a number you already have, before anything moves.
4	**Fake websites** *Using a real licence number and address.*	Badges and contact details that only appear on the page.	Look the licence up on the regulator's own site and use the details you find there.
5	**Fake "fix this" pop-ups** *Dressed up as a real company.*	A support number to call, a request for remote access, or a command to paste.	Don't call and don't paste. Close it and open your own security app.
6	**Business email compromise (BEC)** *An email from someone you deal with, asking you to sign or pay.*	New bank details, something to sign you weren't expecting, or a log-in to see a file.	Check through your own system, and never let one email move money.
7	**Supplier and software risk** *Where much of a small practice's data lives.*	A lookalike address, a deadline and a link to "verify".	Sign in from your usual bookmark or app, never from the email.
8	**Ransomware** *A top threat to professional services.*	Files locked or stolen, and a demand for payment.	Be ready before it happens: basics 3 and 8 in section 5.

Drawn from section 3 of these notes and its sources: the session's agreed list of threats,[17] Scamwatch[12] and the ACSC handbook.[11]

4. What's moving now, beyond the slides

IN SHORT Six things from the past few months that show which way this is heading. Each one is public, dated and checked.

21 AND 22 OCTOBER 2026

Reportedly, AI found the flaw. Then the race was on.

In October, two critical flaws were found in PHP, the programming language that quietly runs a large share of the world's websites. ABC News reports the issue was first discovered using AI, according to a Google-owned cyber security firm.[21]

Governments took websites offline as a precaution while a fix went out, and the ASD said cyber.gov.au and other Australian government sites had reported outages.[21] Reuters, via CNBC, noted reports that hackers were already exploiting the flaws, and quoted one researcher: "with AI exploitation may happen instantly".[22]

For a practice like yours, it's AI for good and AI for bad in the same week, and the question to ask whoever looks after your website and client portal is who applies the security updates, and how you'd know they had.

REPORTED 31 OCTOBER 2026

Once it's in, the software asks an AI what to take

WIRED reported research from Cisco Talos on a piece of information-stealing software, which Talos calls VOLTA-AUTODOXER, and which hands what it finds on a machine to a commercial AI model to work out what's most worth stealing.[28]

It's early days for this one, because Talos couldn't tell who built it, or whether it has been used on real targets yet.[28]

For a practice, it's the Binance story from section 1 with the next step added, and one more reason to treat a file from someone you've only met online with care.

JUNE TO AUGUST 2026

The regulators sat the industry down

In June and July 2026, APRA and ASIC ran nine roundtables on frontier AI with more than 380 entities and 600 attendees, and published what they heard on 27 August.[23]

One of the questions they suggest boards ask: "Have key escalation, shutdown, recovery and communications decisions been made before an incident occurs?"[23]

You may not have a board, but you can ask yourself the same question, and it's really basic 8, a plan for when it goes wrong, in one sentence.

26 OCTOBER 2026

The way in is trust, and the supply chain behind it

The ASD's latest report says cybercriminals keep adapting, exploiting trusted relationships and using social engineering. It adds that more interconnected systems, third-party suppliers and supply chains mean one compromise makes an incident far more complex.[1]

The same report flags something newer: "In recent weeks, new threats have emerged from the unintended actions of AI agents and model testing."[1]

My view for a practice is to give any AI tool that can act for you the same rule as a new staff member, only the access the role needs (basic 6), and to start it small.

30 MARCH 2026

Scam reports are shifting from text to online

The National Anti-Scam Centre says text message scam reports fell from 77,365 in 2024 to 29,058 in 2025, while reports of online-based scams with a loss rose 31.8 per cent, and their losses rose 21 per cent.[19]

For a practice, the knock is moving to the places your clients now spend their time online, and the tells in section 3 travel with it.

REPORTED 27 AUGUST 2026

When the supplier goes down, the shelves go empty

Cyber Daily reported on 27 August that bookstores faced stocking delays after a cyber attack on the publisher Hachette, which said a timeline for a return to full operations was impossible to judge.[24]

The attack was on the supplier and the empty shelves turned up in someone else's shop, which is a ripple, so I'd ask what you'd tell your clients if your planning software or file storage went down for a week.

5. Back at the practice: the eight basics



Illustration made for these notes: the plate, the session's picture for the basics.

The eight basics come from the lists NAB and Insignia Financial each shared for this session, and from the Australian Cyber Security Centre's Small business cyber security handbook (October 2026). Where both gave the same advice, I've credited both.[11,17]

The ACSC itself starts with three: multi-factor authentication, keeping software up to date, and regular backups.[11] Basics 5, 6 and 8 also sit in the ACSC handbook.

Under each basic there's a line that says why it helps. They're the lines that came up on the slides, so you've got them here to keep.

WHAT IT COST WHEN THE BASICS WEREN'T THERE: FIIG SECURITIES

In February 2026 the Federal Court ordered FIIG Securities to pay a $2.5 million penalty, and $500,000 towards ASIC's costs. ASIC says it's the first time the Federal Court has imposed civil penalties for cyber security failures.[10]

The penalty wasn't for being attacked. It was for what FIIG didn't have in place between 13 March 2019 and 8 June 2023. Here's ASIC's own list of what it failed to do, beside the basic each one matches.

ASIC's words	The basic on the plate
"implement adequate cyber security measures, including multi-factor authentication for remote access users"	1. Turn on MFA
"have a structured plan to ensure key software systems were being updated to address security vulnerabilities"	2. Automatic updates on
"strong passwords and access controls for privileged accounts"	4. A password manager; 6. Only the access each role needs
"have an appropriate cyber incident response plan that was tested at least annually"	8. A plan for when it goes wrong, practised
"provide mandatory cyber security awareness training to staff"	Under all of them: your people
"regular penetration testing and vulnerability scanning"	Testing that your basics work

> Backups and the payment process aren't on ASIC's list, so I haven't put them beside it. ASIC's Deputy Chair, Sarah Court, said "the consequences far exceeded what it would have cost FIIG to implement adequate controls in the first place."[10]
>
> Source: ASIC, media release 26-021MR; ASIC v FIIG Securities Limited [2026] FCA 92.[10]

1 Turn on MFA (multi-factor authentication)

Why it helps: A stolen password on its own won't get them in.

A password on its own can be guessed, bought or tricked out of someone. Add a second step, a code or an approval on your phone, and a stolen password isn't enough any more. I'd start with email, then anything that holds client data or moves money.[11] Stronger still are phishing-resistant options, such as passkeys or security keys.[20] *From NAB and Insignia Financial, and the ACSC handbook.*

2 Automatic updates on

Why it helps: Closes the known holes that old software leaves open.

The Australian Signals Directorate (ASD), the government's cyber agency, says the gap between a flaw going public and criminals using it "has never been narrower".[1] It says defenders now have days, sometimes only hours, to patch.[1] Nobody in a small practice can keep up with that by hand, so I'd let the machines do it, on your phones, laptops, browsers and the software you rely on. *From NAB and Insignia Financial, and the ACSC handbook.*

3 Back up, and test the backups

Why it helps: Get your files back without paying. Keep a copy offline, and test it.

If you've never tried restoring a backup, you don't really know yet whether it works. The ACSC asks you to back up important business and customer information regularly, and "test that you can restore it if needed".[11] *From NAB and Insignia Financial (testing the backups: NAB), and the ACSC handbook.*

4 A password manager: a different password everywhere

Why it helps: One stolen password doesn't open everything.

When one site is breached, the same password on another is the next door to go. A password manager remembers a different one for every site so you don't have to. The ACSC asks for strong, unique passwords or passkeys.[11] *From NAB and Insignia Financial.*

5 A set process to approve every payment

Why it helps: Two people on every payment, and ring back on a number you already have.

This is the one that most directly protects your clients' money. I'd decide how a payment, or a change of bank details, gets approved, and never let one email or one call be enough. NAB's advice is to split the duties, so no one person both makes and approves a payment, and the ACSC says to always verify payment requests through a trusted channel.[11] *From NAB, and the ACSC handbook.*

6 Only the access each role needs. No shared logins.

Why it helps: Limits how far one taken-over account can reach.

The front desk doesn't need the keys to everything, and neither does a departed contractor, and a login everyone shares is one nobody can account for. Fewer people with access to a system means fewer ways in, and the ACSC handbook has a chapter on restricting and monitoring access.[11] *From NAB and Insignia Financial, and the ACSC handbook.*

7 Devices lock themselves; wipe before you sell

> **Why it helps:** A lost or sold device doesn't hand over client files.

Laptops and phones get left in taxis and cafés. A screen that locks itself after a short time, and a full wipe before an old device is sold or given away, keeps client files from walking out the door. *From Insignia Financial.*

8 A plan for when it goes wrong, practised

> **Why it helps:** Everyone knows the first steps, so a bad day stays smaller.

Who do you call, who tells clients, who rings the insurer, and where's that list kept if the computers are down? I'd write it on one page and run through it regularly with the team. The ACSC handbook asks small businesses to put incident response plans in place and to test them.[11] *From NAB and Insignia Financial (practising it: NAB), and the ACSC handbook.*

> **Under all of them: your people**
>
> Most of the examples in these notes got in through a person, so I'd teach your team to stop, check and ask: stop before they click, pay or reply, check through a channel they already trust, and ask if anything feels off. *From Insignia Financial (Tips & Resources: "Educate employees about cyber security").*[16]

AI in the practice: a good use, and one check first

AI works for the people defending a practice too. The simplest way to try it this week is to ask it questions about your own set-up, with no client details in it.

I'd give it a role before I ask, something like "You're a security chief with 30 years' experience. Give me ten tips to secure the way my practice uses its accounting software", because you'll get a sharper answer than a general question gets, and you can check what it says against the ACSC handbook.

> **Before any client information goes into an AI tool**
>
> Check two things: where the information goes, and whether the tool keeps it or learns from it. The ASD's guide for small business says some AI providers "may use customer-submitted data to train or refine their models", and that this "can depend on the configuration settings or the type of subscription". Its checklist asks you to verify "what data the AI tool collects and where it is stored", and to confirm whether your data "will be used to train AI models".[29]

The plate: a checklist for your practice

Sources: NAB and Insignia Financial, advice for this session, as credited under each basic above, and the ACSC's Small business cyber security handbook (October 2026), which covers 1 to 3, 5, 6 and 8.[11,17]

	Basic	Done	Who	By when
1	Turn on MFA (multi-factor authentication) Why it helps: A stolen password on its own won't get them in.	☐		
2	Automatic updates on Why it helps: Closes the known holes that old software leaves open.	☐		
3	Back up, and test the backups Why it helps: Get your files back without paying. Keep a copy offline, and test it.	☐		
4	A password manager: a different password everywhere Why it helps: One stolen password doesn't open everything.	☐		
5	A set process to approve every payment Why it helps: Two people on every payment, and ring back on a number you already have.	☐		
6	Only the access each role needs. No shared logins. Why it helps: Limits how far one taken-over account can reach.	☐		
7	Devices lock themselves; wipe before you sell Why it helps: A lost or sold device doesn't hand over client files.	☐		
8	A plan for when it goes wrong, practised Why it helps: Everyone knows the first steps, so a bad day stays smaller.	☐		

The question the session put is a fair one: if a practice did just the first three, how far would that get it? My view is that it gets you a long way, and that the other five are where a practice with client money and client files earns its clients' trust.

6. The floor: regulation and privacy

27 August 2026
ASIC and APRA ask financial entities to move "from gaining awareness" of frontier AI risks "to taking decisive action".[6]

10 December 2026
New privacy policy rules on automated decisions take effect for entities covered by the Privacy Act.[7]

27 August 2026: from awareness to action

In a joint release, ASIC and APRA urged financial market entities to move from gaining awareness of risks linked to frontier AI to taking decisive action.[6]

They noted they had both warned publicly that frontier AI is increasing the speed, scale and sophistication of cyber threats to the financial system.[6] The regulators are saying the briefings are over and it's time to get the basics in, and I agree with them.

10 December 2026: saying when a computer decides

The Privacy and Other Legislation Amendment Act 2024 added new transparency rules to Australian Privacy Principle 1, at APP 1.7 to 1.9. The Office of the Australian Information Commissioner (OAIC) says they take effect on 10 December 2026.[7]

WHEN THE RULE APPLIES, IN THE OAIC'S THREE PARTS

1. A computer program makes a decision, or does something substantially and directly related to making one;
2. the decision could reasonably be expected to significantly affect a person's rights or interests; and
3. personal information about that person is used in the program's work.

Source: OAIC, APP 1.7 to 1.9 Transparency Obligation Fact Sheet, September 2026.[7]

Where all three apply, the privacy policy must set out the kinds of personal information used, the kinds of decisions made by the program alone, and the kinds where the program does something substantially and directly related to the decision.[7]

The OAIC says outputs from machine learning or generative AI used for these decisions would generally be in scope, "unless subject to extensive human oversight and control".[7] If you're trying out AI tools in your practice, it's worth a careful read.

As for who's covered, the OAIC says most small businesses, those with an annual turnover of $3 million or less, aren't covered by the Privacy Act. Some must follow the privacy rules regardless of turnover for certain activities, for example a reporting entity under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006, for those activities.[9]

Whether your practice is covered, and what your policy should say, depends on your business, your licensee and your tools.

Check what this means for your practice with your own legal or compliance adviser.

7. Immediate futures

I call the near distance immediate futures: what's likely to change for you in the next few weeks and months, and what you can do about it today, while there's still time to choose.

The session closed by asking each of the three of us two things. What's the one thing to do before you're back at your desk? And what's the habit that keeps you safer after the next change?

For me, it's this.

ONE THING NOW

On stage I ask everyone to count on their fingers how many of the eight basics they've already got, and my one thing is whichever basic comes next on your count, started before you're back at your desk. If you weren't counting, tick the checklist in section 5 and take the first gap you find.

THE HABIT

I'd pause before acting on any request that moves money or data, and check it through a channel I already trust. Then every few months I'd look up at what's changed, so I spot the next one myself.

Morris's view. Sources for the steps: ACSC, Small business cyber security handbook (7 October 2026).[11]

The ripples

When I work with organisations on the future, I talk about ripples: the effect, and then the effect of that effect.

Say an adviser's email is taken over and a client's withdrawal goes to the wrong account. The first effect is the lost money. The ripples come after that.

- The client stops trusting email from the practice, and maybe stops trusting the practice.
- Their family hears about it, and so does the next person they'd have referred to you.
- The licensee, the insurer and possibly the regulator now have questions for you.
- Your staff start doubting every message, which slows the whole practice down.

With advice it's your clients' data on the line, and that's also why they chose you.

When a worried client rings you about a strange text or call, what do you say to them? That was one of the questions the session put, and I'd love to hear how you'd put it.

If you've already got an answer written down and shared with your team, that client will probably trust you more after the call than before it.

8. Where to go next, and if it happens to you

Resource	What it's for
ACSC, Small business cyber security handbook (7 October 2026)	The government's plain-English starting point for small businesses. cyber.gov.au/publication/small-business-cyber-security-handbook
ReportCyber	Report a cybercrime to the ASD. cyber.gov.au/report-and-recover/report
The ASD's hotline: 1300 CYBER1 (1300 292 371)	The ASD's hotline, for when you're unsure what to do next or how to make a report.[30]
ASD, Questions to ask managed service providers	Five questions to put to whoever looks after your IT, starting with "Are you implementing better practice cyber security?"[31] cyber.gov.au, questions to ask managed service providers
ASD, Artificial intelligence for small business	The risks of AI tools in a small business, with a checklist.[29] cyber.gov.au, artificial intelligence for small business
ASD, the Essential Eight	The ASD's own framework: eight strategies that work together.[32] cyber.gov.au, Essential Eight
Scamwatch (ACCC and the National Anti-Scam Centre)	Current scams and how to report one. scamwatch.gov.au
OAIC, automated decision transparency	The fact sheet and guidance on APP 1.7 to 1.9.[8] oaic.gov.au, new resources on transparency
ASIC and APRA, 27 August 2026	The joint release on frontier AI. asic.gov.au, media release 26-201MR
NAB Security Hub	NAB's public security pages.[15] nab.com.au/security
Insignia Financial, Tips and Resources	A PDF of tips from the ACSC's small business checklist, in the Congress app.[16]

The session page: welcome.morrismisel.com/faaa-congress

The slides, these notes and the links from the day are here.

If it happens to you

- **Money has moved:** ring your bank straight away, on the number on its own website or your card.
- **Report it:** to ReportCyber at cyber.gov.au, and to Scamwatch for a scam. If you're not sure where to start, ring the ASD's hotline on 1300 CYBER1 (1300 292 371).[30]
- **Free support for a small business:** the Australian Government's Small Business Cyber Resilience Service, run by IDCARE, gives free, person-to-person support to small businesses with up to 19 employees, to improve their security and recover from an incident. Call 1800 595 170 (Monday to Friday, 8 am to 6 pm AEST) or see idcare.org/smallbusiness.[25]

- **Client information was involved:** if the Privacy Act covers your practice, the OAIC says you must tell affected people and the OAIC when a data breach is likely to result in serious harm.[26] Check the detail with your licensee or compliance adviser.
- **Tell the people who need to know:** your licensee and your insurer, as your agreements with them require.

Keep going with me

IN SHORT There's plenty more where this came from: a free month of Mo, my books, and a few easy ways to keep hearing from me.



Meet Mo

Choose Forward is where I've put more than thirty years of my work, and at its heart is Mo, my AI double, who thinks along with you about what tomorrow might look like for you. With him are six specialist teammates, each a distinct way of looking at a problem: seven views in all, Mo included.[27]

What you get in Choose Forward

- Talk any decision through with Mo, day or night, out loud or typed.
- Six digital teammates, each looking at your question from their own side.
- You leave with your immediate futures, straight into your calendar.
- Mo picks up where you left off, and you see what he keeps.
- Once a month, a question straight to me. I read it myself.

Say you're weighing up moving your practice's files to a new cloud platform. You tell Mo what you're thinking, and he looks at what's happened, what's happening and what might happen, then follows the ripples, the effect and then the effect of that effect. George gives you the case against, kindly, before anyone else does, and Dave checks whether the sums hold up, from what you choose to share.

Mo gives guidance, not advice: general information, never legal, tax, financial, medical or HR advice.[27]

Talk about the decision, not your clients, and keep client details out of it. Your chats with Mo and the team are private, and never used to train AI.[27] Meet him at chooseforward.today.

Two offers for FAAA Congress delegates

FAAA26

A free month of Choose Forward membership, with Mo.

Use it at members.morrismisel.com/gift.

Type FAAA26 with your first name and email. No card, nothing to pay, and nothing renews: the month simply ends.

FAAA20

20% off five PDFs, marked in my bookshop, bought direct from me.

morrismisel.com/books

Both codes work until 31 January 2027, and you'll find them on the session page, welcome.morrismisel.com/faaa-congress. The codes close on 31 January, so don't leave it to the last week.

The Tuesday email
A short, free newsletter from me, every Tuesday. welcome.morrismisel.com/join

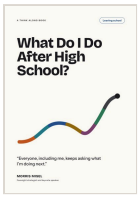
Then and Now, the podcast
What a futurist said on the radio, with the date on it, and how it turned out. Listen here, or in Apple Podcasts or Spotify.

YouTube
Keynotes, interviews and radio, on shelves by subject. youtube.com/@morrismisel

Talk to Morris
Keynotes, workshops and advisory work for your own people. Write to me at morris@morrisfuturist.com, or see morrismisel.com/speaking.

The bookshop

THE THINK ALONG BOOKS: ONE FOR EACH OF LIFE'S BIG TURNS



What Do I Do After High School?

FAAA20

Not sure what comes after school? That's exactly where this book starts.

Buy the PDF



Am I on the Right Path?

Find out if it's the road, or just a bump in it.

See the book



What's My Next Move?

Your skills are always yours. So is your next move.

See the book



Should I Keep Working or Retire?

Your age won't answer this one. You will.

See the book



What Do I Do Now I've Retired?

Work's finished. You're not.

See the book

FOR YOUR BUSINESS



Before the Year Turns FAAA20

For small business owners and their teams, getting ready for 2027.

Buy the PDF

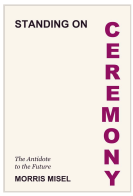
THE BOOKS



Choose Forward

For anyone who makes or moves decisions: a way to keep deciding when nothing holds still.

Reserve your copy

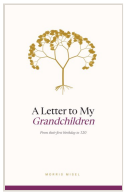


Standing on Ceremony

For anyone who spends their day in front of other people: on a building site, on a ward, behind a counter or in a classroom.

Reserve your copy

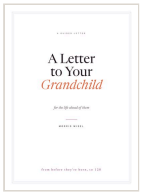
FOR GRANDPARENTS



A Letter to My Grandchildren FAAA20

For grandparents, and anyone who wonders what world the children in their life will grow into.

Buy the PDF



A Letter to Your Grandchild FAAA20

For grandparents and great-grandparents who want to leave their grandchild something in their own words.

Buy the PDF



The grandparent pair FAAA20

A Letter to My Grandchildren + A Letter to Your Grandchild. Three PDFs, only here, A$4.95 less than buying them separately.

Buy the pair

FAAA20 takes 20 per cent off five PDFs, marked, bought direct from me, until 31 January 2027. It doesn't cover paperbacks, Kindle, Etsy or Gumroad.

Visit the bookshop

References

"Checked 8 November 2026" (or 9 or 12 November) means the page or PDF was opened live that day and the wording or figure was found. "From a file I've kept" means the fact comes from a file named in the reference and was not re-opened that day.

[1] Australian Signals Directorate (ASD), Annual Cyber Threat Report 2025-26, 26 October 2026. "The defining force" and the scale, speed and sophistication wording: the report's opening summary. "At greater scale than ever before" and the patching lines ("has never been narrower"; months, now days, sometimes hours): the report's threat sections, including "Vulnerability discovery" (opened 11 November 2026). cyber.gov.au, Annual Cyber Threat Report 2025-26 (PDF); landing page cyber.gov.au/publication/annual-cyber-threat-report-2025-26. *Checked 8 November 2026.*

[2] ASD, Annual Cyber Threat Report 2025-26, Year in review, 26 October 2026. cyber.gov.au, year in review. Over 82,000 reports, one every 6 minutes on average; average self-reported cost per report, small business, $55,400. *Checked 8 November 2026.*

[3] National Anti-Scam Centre (NASC), Targeting scams: report of the National Anti-Scam Centre on scams data and activity 2025, March 2026. nasc.gov.au/reports-and-publications/targeting-scams. $2.18 billion (up 7.8%), 481,523 reports, top five losses. The page's own five-year list rounds 2025 to $2.2 billion. *Checked 8 November 2026, on the NASC page; the full report PDF was not opened.*

[4] CyberCX, 2026 Threat Report, media release, 3 March 2026. cybercx.com.au/news/2026-threat-report. Almost one in five incidents, in CyberCX's own incident work, not all of Australia. *Checked 8 November 2026 (wording); release date from a file I've kept (session brief, 7 November 2026).*

[5] ABC News (AFP), "Binance investigation uncovers fake job plot involved in $9 billion crypto-heist", 4 November 2026. abc.net.au/news, 4 November 2026. US$6.6 billion (A$9 billion); the job-site approach and the test exercise. Figures for the theft vary between outlets, so these notes use "more than US$6 billion", about A$9 billion. *Checked 8 November 2026.*

[6] ASIC and APRA, media release 26-201MR, "ASIC and APRA warn frontier AI awareness must turn to action", 27 August 2026. asic.gov.au, 26-201MR. *Checked 8 November 2026 (wording); date as shown on the APRA copy, from a file I've kept (session brief, 7 November 2026).*

[7] Office of the Australian Information Commissioner (OAIC), APP 1.7-1.9 Transparency Obligation Fact Sheet, September 2026. oaic.gov.au, fact sheet (PDF). *Checked 8 November 2026.*

[8] OAIC, "New resources on transparency for use of AI and automated decision making". oaic.gov.au, media centre. *Checked 8 November 2026 (page opens).*

[9] OAIC, Small business. oaic.gov.au, small business. $3 million turnover; reporting entities under the AML/CTF Act covered for those activities. *Checked 8 November 2026.*

[10] ASIC, media release 26-021MR, "ASIC action sees FIIG Securities ordered to pay $2.5 million over cyber security failures", February 2026. asic.gov.au, 26-021MR. The penalty and costs, the 385 gigabytes, the 18,000 clients, ASIC's list of failures (13 March 2019 to 8 June 2023), "the first time the Federal Court has imposed civil penalties for cyber security failures", and Sarah Court's words. Judgment: ASIC v FIIG Securities Limited [2026] FCA 92, 13 February 2026. *Checked 8 November 2026, and again on 12 November 2026.*

[11] Australian Cyber Security Centre (ACSC, part of ASD), Small business cyber security handbook, published 7 October 2026. cyber.gov.au, small business handbook. The three starting measures; the chapter "Common cyber threats to small businesses" (how business email compromise and ransomware work). *Checked 8, 11 and 12 November 2026. It does not mention a password manager, screen lock or device wipe.*

[12] Scamwatch (ACCC), "Don't get scammed by dodgy internet pop-ups", 10 April 2017. scamwatch.gov.au, pop-ups. *Checked 8 November 2026.*

[13] iTnews, Juha Saarinen, "'ClickFix' attack tricks users into hacking themselves, ACSC warns", 8 May 2026. itnews.com.au, ClickFix. *Checked 8 November 2026. The ACSC alert itself was not opened.*

[14] CarExpert, Damion Smy, "230,000 Australian driver licences exposed in ransomware attack on vehicle finance firm", 24 February 2026. carexpert.com.au, youX. *Checked 8 November 2026.*

[15] NAB, Security Hub. nab.com.au/security. *Checked 8 November 2026 (page opens). Named as a resource only.*

[16] Insignia Financial, Tips & Resources (PDF), in the FAAA Congress app, including "Educate employees about cyber security" and "Limit the use of shared accounts". *From a file I've kept (shared 29 October 2026); opened 9 November 2026.*

[17] The session's agreed content: the eight threats, the eight basics and their order, the FAAA's line "Eat your cyber vegetables first", and the "Changed / Not changed" summary. The basics come from NAB's list and Insignia Financial's tips, both shared on 29 October 2026 for the session, as set out item by item in the focus areas document (v4.1, 30 October 2026); no private material is quoted. The three steps of business email compromise and the eight "why it helps" lines are from the final slides. *From files I've kept (stage deck and design notes, 6 and 7 November 2026; the final deck, 12 November 2026); not a public source.*

[18] Morris Misel's own story: the "Hi Dad" text on his phone, 26 September 2026 (screenshot in the session briefing deck, 28 October 2026). *From files I've kept.*

[19] National Anti-Scam Centre, "Continued action critical to combat fraud as annual scam losses exceed $2 billion", media release, 30 March 2026. nasc.gov.au, media release. Phishing the most reported scam to Scamwatch in 2025, 65,361 reports. *Checked 8 November 2026.*

[20] ASD, "Implementing multi-factor authentication". cyber.gov.au, implementing multi-factor authentication. Phishing-resistant MFA; passkeys; security keys over SMS. *Checked 8 November 2026.*

[21] ABC News (Thomas Morgan, with wires), "Australian government sites among those exposed to 'critical' PHP software flaw", 22 October 2026. abc.net.au/news, 22 October 2026. *Checked 8 November 2026.*

[22] CNBC (Reuters), "Government websites go dark as software flaw sparks security scramble", 21 October 2026. cnbc.com, 21 October 2026. *Checked 8 November 2026.*

[23] APRA and ASIC, "Insights from the APRA-ASIC Industry Roundtables" (Resilience at Frontier AI Speed), information paper, 27 August 2026. apra.gov.au, roundtables. *Checked 8 November 2026.*

[24] Cyber Daily, David Hollingworth, "Aussie publisher Hachette restoring systems following 'detection of unauthorised activity' on network", 27 August 2026. cyberdaily.au, Hachette. *Checked 8 November 2026.*

[25] business.gov.au, "Small Business Cyber Resilience Service"; IDCARE, "Services for sole traders and small businesses". business.gov.au; idcare.org/smallbusiness. *Checked 8 November 2026.*

[26] OAIC, "Notifiable data breaches". oaic.gov.au, notifiable data breaches. *Checked 8 November 2026.*

[27] Choose Forward, with Morris Misel. members.morrismisel.com/gift ("Mo is my AI double"; "It's like having your own futurist on call"; chats "private, and never used to train AI"). *Checked 8 November 2026. Morris's own product.*

[28] WIRED, 31 October 2026, reporting Cisco Talos research on the VOLTA-AUTODOXER infostealer. Other reports of the same research: Help Net Security, "AI-powered infostealer picks out the most profitable parts of your stolen data", helpnetsecurity.com; iTnews, itnews.com.au, Talos. The caveat (who built it, and whether it has been used) is from TechSpot's report of Talos. *Checked 12 November 2026, by web search across these reports; the WIRED article was read on 10 November 2026.*

[29] ASD's ACSC, "Artificial intelligence for small business" (PDF dated December 2025). cyber.gov.au, artificial intelligence for small business. *Checked 12 November 2026.*

[30] ASD, "Submit a report": the hotline, 1300 CYBER1 (1300 292 371). cyber.gov.au/submit-a-report. *Checked 12 November 2026.*

[31] ASD's ACSC, "Questions to ask managed service providers" (PDF dated October 2021). cyber.gov.au, questions to ask managed service providers. *Checked 12 November 2026.*

[32] ASD, "Essential Eight": "a framework developed by the Australian Signals Directorate to help organisations protect themselves against cyber threats. It consists of 8 strategies". cyber.gov.au, Essential Eight. *Checked 12 November 2026.*

How I chose what went in

Nearly everything in here is public and dated: government reports, regulators' releases, and cases that were widely reported about organisations, such as Binance, youX and FIIG Securities. The rest is the content the panel agreed for the session and my own "Hi Dad" story, which come from files I've kept, and the references say which. Nothing private from NAB or Insignia Financial is quoted.

Every figure has a source I opened, or a file I've kept, and the references say which. Where I couldn't open a source again on the day of checking, the figure stayed out.

One thing stays out on purpose: what James, Rob and the room said on the day is theirs.

About Morris, and the fine print



Morris Misel is a Business Futurist, Keynote Speaker, Author and the Founder of Think-Along AI. For more than 30 years he has worked with leaders, boards, associations and businesses on what's coming next and what to do about it, across 2,800+ keynotes and workshops in 25 countries. He is heard by more than a million people each year.

He moderated "AI for Good, AI for Bad" at FAAA Congress 2026.

Stay in touch

The Tuesday email, free, every Tuesday: welcome.morrismisel.com/join

LinkedIn: connect with me

YouTube: youtube.com/@morrismisel

Instagram: @morrisfuturist

Facebook: MorrisFuturist

X: @MorrisMisel

Substack: morrismisel.substack.com

Want me in your room? morrismisel.com

The slides, these notes and everything from the session

Disclaimer

These notes are general information only, current to 12 November 2026, and figures and rules move. It is not financial, legal, compliance or taxation advice. It does not take account of any person's or practice's objectives, financial situation or needs, and it is not a substitute for advice from a qualified professional. Sources are named so you can check them yourself. The views are Morris Misel's own and do not represent the FAAA, NAB, Insignia Financial or the other panellists. No liability is accepted for decisions made in reliance on this document.

The pictures in these notes were made for the session and the notes, and show no real people, faces or brands, apart from Morris's own photograph, Mo's portrait, the covers of his books, and the two examples NAB supplied in section 3, which show the faces and brand the scammers used. The example messages in section 3 are recreated from real ones, with names, brands and numbers changed. The "Hi Dad" message is a real message to Morris's phone, with the number removed.

The FAAA26 and FAAA20 offers are Morris's own; the FAAA, NAB and Insignia Financial aren't party to them.

© Morris Misel 2026. These notes may be shared in full and unaltered, with attribution.