Read About My Real-World Scam Experience (So You Don't Have One)

Jane Richter, Communications Manager, Berries Australia

- **Stop.** *Does something seem off? If in doubt, stop and take a breath*
- **Check.** *Ask someone you trust or contact the organisation directly, using their official details*
- **Reject.** *Hang up on the caller, delete the message or email, and block (and report) the contact*
- **Secure:** *Change your password, enable MFA*

I'm embarrassed to admit that I have recently been the victim of a scam. To put it bluntly, I clicked a link I shouldn't have, and it cost me over $1,500 that I will never get back.

I consider myself reasonably tech-savvy. I run my own business almost entirely online and deal with a myriad of digital systems every day. I'm a multi-factor authentication fanatic, I'm far from careless online, and I'm usually sceptical of anything that feels even slightly off. And yet, on 21 December, I still got taken to the cleaners by a scammer from Uzbekistan!

The scam didn't arrive waving red flags. It looked routine. A familiar name (*an overseas hotel I have a genuine booking at in March 2026*), familiar language, and a request that didn't seem unreasonable in the moment (*we just need to reconfirm your booking*). There was urgency in the request but not panic. Authority, but not aggression. Everything sat just inside the bounds of 'normal enough' to keep me moving instead of stopping and reflecting on the origin and legitimacy of the request.

That's how many scams work. They don't rely on stupidity; they rely on momentum.

At the time, I didn't feel like I was taking a risk. I felt like I was being responsive and efficient. By the time I realised what had happened, the damage was already done.

What followed was worse than the financial loss. First came disbelief, then a deep sense of embarrassment. There's a strong instinct to stay quiet after something like this, especially when you think you should have known better. I've now been through the next phase: anger. I'm angry at the scammers, at the banking systems that didn't catch it, but most of all at myself for not slowing down and thinking twice before acting.

Why am I sharing this?

I need to channel my sense of shame into something useful. I'm telling my story so that you don't have to walk the same uncomfortable path I've been on since it happened. And I want to share what I've learned, including pointing people to the many free, practical resources available if you find yourself in the same position, either as a private individual or as a small business.

Scams thrive in silence. The idea that 'savvy people don't get scammed' is not only wrong, but it also actively helps scammers by keeping victims quiet.

What happened?

I fell for a classic 'impersonation' scam. I was contacted via WhatsApp by someone who claimed to be from a hotel where I have a genuine booking – made via Booking.com – for a stay in a foreign country in March 2026. The message I received included the correct dates of my stay, the full property name and address, and it came to my number with my name, so the scammer obviously had all of my personal information. It coincided with the expiry date of the credit card that I had used to make the booking, and I made the expensive(!) assumption that it was reasonable for the 'hotel' to ask me to reconfirm my card details, given my card was about to expire.

Add a sprinkle of 'urgency' – I was given 24 hours to respond, or my booking would be cancelled – and it was the perfect recipe to part this fool from her money. I'll save you the gritty details, but nonetheless, they caught me in a moment when I was emotionally distracted, multitasking, and failed to sniff a rat!

And because I thought I was responding to a legitimate request, even my multi-factor authentication addiction didn't save me; I authorised multiple payment attempts which have left me $1,500 out of pocket, with six lots of international transaction charges to add insult to injury!

Our digital devices are woven into everyday life. Phones, tablets and computers are how we work, communicate, shop, bank and stay connected. For most of us, they're the first thing we check in the morning and the last thing we look at before bed.

Scammers know this. They've learnt to exploit the way we use technology and to reach Australians through the channels we trust most: SMS, messaging apps, email, social media and online advertising.

The result is that almost any digital message now carries some level of risk. A simple text saying you missed a call can be the hook that leads to malware download. A convincing online advertisement can funnel you into an investment scam. Even messages that appear harmless or routine can be the starting point for fraud.

The uncomfortable reality is that spending time online means exposure. If you use digital devices, you will encounter scammers, fraudsters and people trying to access your personal or financial information. The challenge isn't avoiding the internet, it's learning when to slow down, question what you're seeing, and what to verify before you act. And it is being aware of the assistance that is right at hand here in Australia if you do happen to let your guard slip.

Scams don't target a 'type' of person. They hit people of all ages, backgrounds and income levels. There's no safe category you fall into just because you're experienced, educated or careful. At some point, everyone is vulnerable.

Scams work because they look legitimate and arrive when you're not expecting them. They're designed to blend into everyday life, not stand out from it. Scammers constantly adapt, using new technology, new products and major events to build believable stories that feel timely and real.

They don't need you to be careless. They just need you to be busy, distracted, or trying to get something done. That moment is often enough to convince you to hand over money, information, or access before you realise what's really happening.

Resources

Find out more about scams, cybercrime and identity theft

- www.accc.gov.au/consumers/consumer-protection/protecting-yourself-from-scams
- www.scamwatch.gov.au/types-of-scams
- moneysmart.gov.au/banking/banking-and-credit-scams
- www.idcare.org/learning-centre
- www.afp.gov.au/crimes/cybercrime
- www.cyber.gov.au/report-and-recover/so-you-think-you-have-been-hacked
- www.actnowstaysecure.gov.au/cyber-safe-actions

What I Wish I'd Known ...

Urgency is the biggest red flag of all

Anything that pressures immediate action is designed to short-circuit your judgement. Legitimate organisations will allow time for verification. If the message says you have a very limited time to respond, then listen to the warning siren that is going off in your head; don't ignore it!

Verification isn't rude — it's essential

A double-check in my Booking.com App, a quick phone call, or an email to the hotel directly to check would have stopped this instantly. Genuine requests will always stand up to scrutiny.

Familiarity can be faked

Names, logos, writing style, and tone are easy to copy. Familiar does not equal safe. My scammers had created a payment portal that used all the branding, logos, colours and fonts used by Booking.com even down to the little favicon in the browser tab, and that's the kind of attention to detail that I can't help having a begrudging admiration for!

Process matters more than politeness

Scammers rely on people not wanting to question authority or slow things down. If it doesn't feel right, dig your heels in and contact the 'business' through a separate, trustworthy channel to check its legitimacy.

Silence only helps the scammer

I can tell you that the shame feels very real, but talking about it is how awareness spreads, and damage is reduced. It strips the scammers of some of their power, and I'm all for that.

Help! I've been scammed! What to Do (Individuals)

If you suspect a scam, speed matters.
Don't wait to be sure.

1. Stop and contain it immediately

- Do not click any more links or reply to the message
- Disconnect the affected device from the internet if malware is suspected
- Take screenshots or save emails, texts, links and payment details

2. Contact your bank straight away

- Call your bank's fraud team immediately
- Ask them to freeze accounts, stop pending payments, replace bank cards and flag future transactions
- Change your online banking password from a clean device

NOTE: Your bank should always be your first call if the scam involves a financial transaction or the potential that your accounts can be accessed without your permission

3. Change passwords and secure accounts

- Change passwords for email, banking, social media and any linked services
- Enable multi-factor authentication (MFA) where available
- If a work email was involved, notify your employer immediately

4. Get expert support

- Contact IDCARE idcare.org or 1800 595 160
- They provide free, confidential support for Australians impacted by cybercrime, and step-by-step recovery plans tailored to your situation
- They also offer a free device cleaning service, which enabled me to be certain that my phone had not been compromised in any way

5. Report the scam

- Make a Cybercrime report at cyber.gov.au/report-and-recover/report
- Report the incident to Scamwatch.gov.au
- This helps authorities track scam trends and warn others
- Reporting is important even if money can't be recovered

6. Look after yourself

- Feeling embarrassed, angry or shaken is normal
- Talk to someone you trust
- Silence only benefits scammers - reporting and sharing helps reduce harm

Help! I've been scammed! What to Do (Small Businesses & Farms)

For farms and small businesses, scams often hit harder because they disrupt cash flow, relationships with suppliers, and trust. Always act fast and document everything.

1. Stop transactions and secure systems

- Contact your bank's business fraud team immediately
- Freeze affected accounts, cancel bank cards and halt pending payments
- Disable compromised user access (email, accounting, payroll)

2. Preserve evidence

- Save emails, invoices, payment instructions, SMS messages and links
- Keep logs of times, amounts, account numbers and contacts
- Don't delete anything until advised

3. Contact IDCARE for business guidance

- IDCARE also supports small businesses with a range of free services
- Contact IDCARE at idcare.org or 1800 595 160
- They help assess business impact, reputational risk and recovery steps
- Particularly valuable if payroll, supplier payments or invoices were affected

4. Report the scam formally

- Report the incident to Scamwatch.gov.au
- Make a Cybercrime report at cyber.gov.au/report-and-recover/report
- ReportCyber is run by the Australian Cyber Security Centre and is the official channel for cybercrime affecting businesses

5. Notify internal and external stakeholders

- Alert staff so the same scam doesn't spread internally
- Contact suppliers or customers if invoices or payment details were compromised
- Transparency early is far better than cleanup later

6. Review and strengthen processes

- Introduce or reinforce payment verification procedures (e.g. call-back checks, MFA)
- Separate payment approval and processing roles where possible
- Train staff and family members involved in the business to pause and verify

Remember, scammers don't target the careless. They target the busy, the helpful, and the responsible. The best defence isn't just better technology, it's giving yourself permission to pause, verify, and ask questions without apology.

Scams don't just take money, they shake confidence and erode trust. Acting quickly, using the right support services, and talking about what happened are the best ways to limit damage and protect others.

If sharing my experience can help just one person take a pause before clicking or paying, I've already made a difference.

Multi-Factor Authentication (MFA) *for Dummies*

What is MFA?

Multi-factor authentication (MFA) is a second layer of security for your accounts.

Instead of relying on just a password, MFA requires two or more factors to verify that you are really you. Even if a scammer gets your password, MFA can stop them from getting into your account.

Think of it like this:

Password = the key and **MFA** = the deadbolt

Both are needed to get through the door.

How MFA Works

When you log in:

1. You enter your password
2. You're then asked to confirm your identity using something else
3. Only after both are verified do you get access

That second step is what blocks most account takeovers.

MFA Methods from Strongest to Weakest

1. Hardware Security Keys (Gold Standard)

- Physical devices you plug in or tap to approve logins, like a Yubico (YubiKey) or a Secure Key from a bank

Why are they excellent?

- They are immune to phishing, there are no codes to steal, and they are extremely reliable.

2. Authenticator Apps (Strongly Recommended)

- These apps generate time-limited codes on your phone. They do not rely on SMS, which makes them much harder to intercept.
- Common options used in Australia include Google Authenticator, Microsoft Authenticator and Authy

Why are they good?

- They work offline, are not tied to your phone number and are resistant to SIM-swap scams

3. App Push Notifications (Very Secure)

- Instead of entering a code, you approve a login attempt via an app notification. These are often used by Microsoft accounts, Google accounts and many banks and business platforms

Why are they good?

- They are fast and user-friendly, harder to fake and alert you immediately to suspicious login attempts

Remember: If you get a push you didn't request, **deny it** - someone has your password, so you need to change it immediately to a secure option.

4. SMS One-Time Codes (Better Than Nothing)

- A code is sent to your phone number via text message.

Why is it weaker?

- It is vulnerable to SIM-swap scams, messages can be intercepted or redirected, and it is often targeted by impersonation scams
- Use only if App-based MFA isn't available.

5. Email Codes (Low Security)

- A code is emailed to you.

Why is it risky?

- If your email is compromised, MFA is useless and this is often exploited in phishing attacks
- It's better than nothing, but not ideal.

What a MFA does not do

✗ Won't stop you clicking a scam link

✗ Won't protect you if you approve a fake login

✗ Isn't a replacement for common sense

It does dramatically reduce the damage if credentials are stolen.

Top tips

- Use **authenticator apps** wherever possible
- Protect your **email account first** as it's the gateway to everything else, especially if you use a Password Manager embedded in your Google or Microsoft account
- Never share MFA codes with anyone, ever, no matter who asks
- Treat unexpected login prompts as a warning sign to change passwords and contact the account provider to check you are employing the best security they currently offer
- Back up MFA recovery codes and store them securely (offline)

Passwords alone are no longer enough. MFA is one of the simplest, cheapest, and most effective ways to protect yourself and it stops a large percentage of scams dead in their tracks.

If you use email, online banking, cloud services or accounting software and you don't have MFA turned on, it's the one change you can make right now after hearing my sorry tale that will make you significantly safer in today's online world.