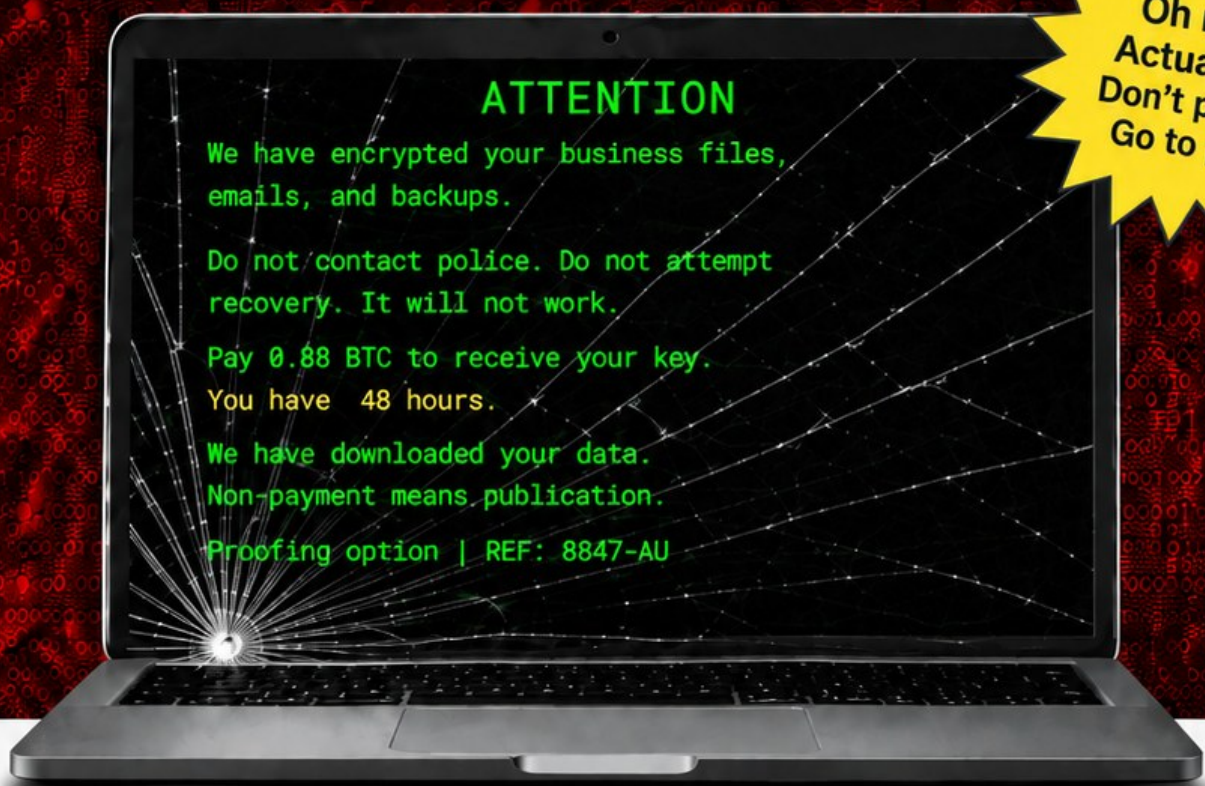


SHIT, I'VE BEEN HACKED!

Kevin Greely



Over 2.2 million Australian small businesses experienced a cyber incident in the past year.*

You weren't hacked by geniuses.
You were caught by gaps that could have been easily fixed.

This book shows busy business owners the simple, practical steps that stop the preventable stuff.

*Estimated using Cyber Wardens Small Business Cyber Security Pulse Check Report 2026 & ABS.



SteadyPoint
CYBER

www.steady-point.com

What's Inside the Full Book:

IF YOU ONLY DO 5 THINGS (THE 60-MINUTE CYBER UPGRADE)	4
HOW TO USE THIS BOOK	6
PREFACE – MEET THE HACKERS	8
INTRODUCTION – STOP THE BLEED	17
CHAPTER 1 – YOUR DIGITAL ID CARD	25
CHAPTER 2 – THE DIGITAL BACK DOOR	35
CHAPTER 3 – THE TECH REGO	44
CHAPTER 4 – CLOUD OR CHAOS	52
CHAPTER 5 — THE FIRE DRILL	62
CHAPTER 6 — THE HUMAN FACTOR	72
CHAPTER 7 — MONEY MOVES & RED FLAGS	83
CHAPTER 8 — WHO ELSE HAS A KEY?	91
CHAPTER 9 – GOVERNANCE WITHOUT THE CORPORATE STUFF	100
CHAPTER 10 – AI: THE NEW APPRENTICE	107
CHAPTER 11 — GETTING HELP WITHOUT GETTING FLEECE	117
CHAPTER 12 — THE LAST ~10%	122
CONCLUSION	127
APPENDIX A — GLOSSARY OF TERMS	133

If You Only Do **Five Things...**

You probably didn't sit down intending to read a cybersecurity book cover to cover. That's fine. Start here with a spoiler-alert: Take these five actions and you'll have already removed a large portion of the cyber risk that affects SMBs today. Come back and read the rest when you have time.

 **Most people finish in under 60 minutes**

THE 60-MINUTE CYBER UPGRADE

1 **Two-Step Login for Email**

Your email is the master key to your business. If someone takes control of it, they can reset passwords, impersonate you, and redirect payments.

Turning on two-step login (often called Two-Factor Authentication or Multi-Factor Authentication - 2FA/MFA) means a password alone cannot unlock your account even if it's stolen.

2 **A "Payment Change" Rule**

If a supplier emails new bank details, always confirm by phone using a number you already have on file. Confirm this rule with all staff who process payments.

Never rely solely on email for payment instructions. This single rule prevents one of the most common and expensive scams.

3 **Automatic Daily Backups**

Ransomware locks your files and demands payment. Businesses with reliable backups can restore and keep operating — without paying criminals.

Ensure important files are backed up automatically every day.

4 **Automatic Updates — Everywhere**

Software updates fix known security weaknesses that attackers actively abuse.

Enable automatic updates on computers, phones, and key business software so fixes are applied without relying on memory.

5 🐼 Make Reporting Mistakes Safe for your People

Most incidents start with a simple human mistake — clicking a suspicious link or opening the wrong attachment. The real damage often happens when people stay silent out of embarrassment.

If you have staff, make it clear that reporting something quickly will never get someone in trouble. Early reporting can stop an incident before it spreads.

Why These Five Things Matter

Take these steps as a reassurance. These five won't make your business perfectly secure — nothing does — but they remove the easiest opportunities that criminals rely on. Most cyber incidents affecting small businesses start with one of the five categories on the right.

The rest of this book explains how incidents unfold and how to strengthen your defences further, without turning cybersecurity into a full-time job.

MOST ATTACKS START WITH

- Stolen email access
- Fake invoices & payment fraud
- Phishing* emails
- Ransomware
- Unpatched software

You don't need to know everything about cybersecurity. You just need to know what matters to you, what reduces real risk, and what's worth your time and money.

How to Use This Book

Cybersecurity rarely makes anyone's weekend reading list. If you're holding this book, chances are something gave you a nudge. A story about a supplier or business just like yours getting hit, a client suddenly demanding proof of your security, or an insurance broker asking questions you weren't prepared for.

Here's how the book is built, and how to get what you need out of it without reading the whole thing tonight.

Three ways in

"I've got an hour." You've already met the five things at the front. If you did them, you removed a large slice of your risk in one pass. When you find another hour, read Chapters 1, 2 and 3 — to cover identity, invoice fraud, and backups respectively. Those three stop the attacks that close businesses. If you want one more after that, make it Chapter 5 on incident response. It's the one you'll wish you'd read at 6pm on a Friday.

"I want to do this properly." Front to back, a chapter a week. Do the action list at the end of each chapter before you start the next one. The reading isn't the point. It's the action lists.

"Someone has asked me a question I can't answer." A client, an insurer, a tender document. Go straight to the self-assessment checklist in the Conclusion and tick what's genuinely in place. The unticked boxes tell you which chapters you need, and in what order.

How each chapter works

Some chapters open with something that happened to a business about your size. Then the explanation of why it worked. Then a one-page action list: what to do, roughly how long it takes, what it costs, and whether it's your job or your IT person/provider's.

If you read nothing else in a chapter, read the action list.

The symbols

	How long it takes
	What it costs
	You can do this one yourself
	Shared with your IT provider
	Your IT provider handles this one

	Where you've got to so far
	Oi, there's a printout, poster or template for this

About the templates

Everything marked with the printout symbol is in this book in full. Photocopy it, laminate it, stick it on the wall near the payments desk. Yours to use.

The versions at www.steady-point.com/resources are the same documents for when you'd rather type than write: All docx, .xlsx and PDFs, a risk register you can sort, policies you can drop your own business name and logo into.

About Bronze, Silver and Gold

You'll see Bronze, Silver, Gold, Platinum and Diamond used throughout. That's SMB1001, a cybersecurity standard built for businesses your size rather than for banks. Why I chose it, and my connection to the not-for-profit that publishes it, is on page 19. If someone asks you about a different framework, such as the Essential Eight, Appendix B shows how your work carries across. You don't need to understand the tiers to use this book. Work through the chapters and the book will tell you where you've progressed to. Most people finish further up than they expected.

If you want to use your favourite AI assistant alongside this book

AI is so useful for adapting the templates in here to your business. Try something like:

I run a [type of business] in [town], Australia, with [number] staff. Rewrite the policy below so it fits how my business actually works; in plain English my team will read. Keep it to one page.
[paste the template]

Two rules though: Start a fresh conversation, and don't paste real customer names, bank details or staff records into a free AI tool. Chapter 10 explains why, and what to use instead.

One last thing

Nothing in this book is a test, and none of it is a judgement on how you've run your business so far. Each gap you find is just a job you hadn't got to yet.

Start with the ones that protect your money.

Chapter 2 – The Digital Back Door

Email, Invoice Fraud, and Phishing Defence

You can have the best locks in the world — but if someone sweet-talks an employee into letting them in, you're cooked. *That's phishing in a nutshell.* Cyber-attacks rarely start with a technical exploit anymore. They start with a conversation, an email or a small believable request. These attackers don't break in. They get invited.

AI has now turned phishing into a factory operation.

Mostly gone are the misspellings and strange grammar. Today's scam emails are increasingly clean, well-written, and often perfectly match your industry.

AI is to a scammer what Canva is to a small business marketer. It makes professional-looking communication cheap and fast.

The biggest financial threat to Australian small businesses today isn't ransomware.

It's **invoice fraud** — also known as Business Email Compromise (BEC).

This is where someone impersonates a supplier, business owner, or staff member and convinces your business to transfer money to the wrong bank account. The payment looks legitimate. The invoice looks correct. The email conversation appears genuine.

And by the time anyone realises, the money is gone.

What This Actually Looks Like

These are not rare edge cases. Variations of these happen across Australia every week.

SCENARIO 1

The Tradie Supplier Change

You run a construction or trade business. You regularly pay a supplier you've used for years with the same contact person and the same email chain. An email arrives:

"Hi mate, just letting you know we've changed banks. Please use the attached invoice with updated payment details for this month's order. See you at the awards next week."

The email is polite and the writing style matches. The signature block looks correct. The ABN on the invoice is valid.

What you don't see: the attacker accessed the supplier's mailbox weeks earlier seeing every email since. They watched and waited. They learned your billing cycle. They drafted the new invoice, read it three times to make sure the tone matched, and went for a coffee.

You pay the \$18,420 invoice. Three weeks later the real supplier calls asking why they haven't been paid.

The money is unrecoverable within hours once transferred overseas.

SCENARIO 2

The "Boss Is Busy" Transfer

You're the office manager or bookkeeper. At 4:52pm on a Friday, you receive:

"Hi, I'm tied up in meetings with a client and need an urgent transfer processed before close of business. I can't take calls. I'll send details in the next email."

The name matches the business owner. The tone sounds like them. The email address looks correct at a glance (kevin@greelygroup.co instead of .com.au).

You don't want to hold things up and upset the boss. You process the \$9,800 payment.

You just transferred money directly to a criminal.

This attack works because it relies on authority and urgency, not technical skill. I can almost guarantee you know people that have been scammed by this one. I know many!

SCENARIO 3

The Accountant Intercept

Your accountant emails requesting end-of-year payment for BAS or tax instalments. Except the attacker has already compromised either your email account or the accountant's. They

silently create forwarding rules and monitor conversations. At exactly the right moment they insert a message:

“ATO payment details have changed. Please see updated remittance.”

The email thread looks genuine because it is. They are replying inside a real conversation. You transfer \$42,000 to what you believe is the ATO payment account.

It is not.

Why This Works So Well

Invoice fraud succeeds because it targets processes, not computers.

1

Access to a mailbox

*Bought, breached, or
compromised through phishing*

2

A convincing domain

*One character off is easy to
miss at a glance*

3

A distracted staff member

*Friday afternoon, end of month,
or just a busy day*

“Everything looked normal.” And that is the point.

Why Email Is the First Thing We Secure

Email is the central nervous system of your business. Compromise it and an attacker can convincingly become anyone in your organisation.

- invoices and payment conversations
- payroll communications
- supplier relationships
- password resets for every other system

CHAPTER 2 ACTION

Stop Fraud Before It Starts

TIME
1–2 hours

COST
Free

LED BY
● Owner

PRIORITY
Do first

- ☐ 1 **Write a “verify by phone” rule** ● Owner
Bank details never change on the strength of an email. A written rule removes the guesswork. Chapter 7 and [steady-point.com/resources](https://www.steady-point.com/resources) have a ready-to-use version.
- ☐ 2 **Brief your finance people** ● Owner
Fifteen minutes with whoever handles invoices or payroll. Walk them through the three scenarios in this chapter.
- ☐ 3 **Add the fraud alert footer** ● Owner
Put the fraud-alert wording from this chapter into every staff email signature. Done when the next email anyone sends carries it.
- ☐ 4 **Build a verified supplier phone list** ● Owner
Your top 10 suppliers, with numbers confirmed from your own records, not from an email or invoice. Do it now, before you need it in a hurry.
- ☐ 5 **Check your DMARC setting** ● Shared
Free at mxttoolbox.com. Done when your policy shows quarantine or reject. If it shows none, or nothing at all, raise it with your IT provider.

● Owner: you do it ● Shared: you and your IT provider ○ IT provider: they do it

This single process change protects more businesses than most expensive security products.



ADD THIS TO YOUR EMAIL FOOTER

IMPORTANT FRAUD ALERT

Please be aware that there is a significant risk posed by cyber fraud, specifically affecting email accounts and bank account details. Always confirm bank account details and transfer instructions with us in person or via a telephone call to a trusted and verified phone number.

This is a selection preview of ***Shit, I've Been Hacked!*** by Kevin Greely

In the remainder of the book, you'll gain the confidence to understand what enough looks like for your business. The protections you put in place through this layered approach will help your business bounce back quickly from an incident or simply bounce through it.

Reserve your copy today. Get publication and preorder details at:

www.steady-point.com/landing-book

© 2026 Kevin Greely. All rights reserved. Not for resale or redistribution.