

Safety on the tools and beyond

Small business cyber security guide for the Queensland construction industry



Why cyber security matters in construction



The construction industry is increasingly going digital, from online project management and supplier invoicing to drone footage and smart tools on site. But as technology becomes essential both on and off the tools, cyber attacks are becoming a real threat, especially for small construction businesses.

In the last financial year, **Queensland recorded the highest number of cyber incidents nationwide** – a serious concern given construction is the state's largest small and family business sector.

Nationally, the construction industry ranked among the top 10 reporting sectors for cyber incidents in 2022–23, according to the Australian Cyber Security Centre (ACSC)¹.

With 98 per cent of Australia's 445,081 construction businesses being small operators², often running on lean admin and IT support, basic cyber safety is no longer optional. It's essential.

A single cyber incident, such as a fake invoice, hacked email, or ransomware attack, can stall your job, lock you out of vital plans, **and cost an average of \$56,600 to recover from.**

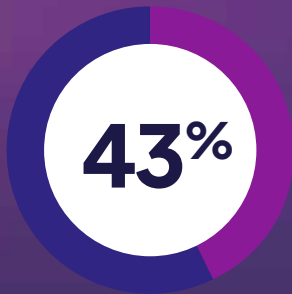
This cyber security guide tailored to Queensland construction small businesses will help you nail your cyber safety onsite and online.

It includes simple, practical steps to help you protect your clients, employee details, financial information, business data, project plans and reputation without needing to be a tech expert.

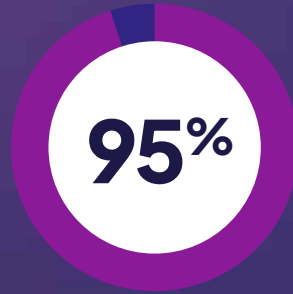
¹Australian Cyber Security Centre, 2023

²Master Builders Australia, 2022

Small business cyber security snapshot



**of cyber attacks
target small business**



**of cyber crime is
due to human error**



In the past year,
the average cost of a
cyber crime has risen to

\$56,600

**A cyber incident is
reported every**



PRO TIP!

Queensland's small and family businesses can access the Cyber Wardens program for free, giving your team the tools, knowledge, and confidence to protect your business from cyber threats, on and off the job site.

REGISTER TODAY



cyberwardens.com.au/qld-gov

Top cyber threats in construction



The construction sector increasingly relies on digital tools to boost efficiency and manage projects, but this also increases exposure to cyber attacks.

A reliance on third parties and contractors, as well as high-pressure project timelines, also put businesses in the crosshairs of online fraudsters.

These are the top threats affecting the construction industry:



Business email compromise (BEC)

BEC is when scammers send convincing fake emails posing as suppliers, clients, or authorities, tricking victims into sharing sensitive information or transferring money, believing the request is legitimate.



Fake invoices

Scammers send illegitimate supplier bills to staff or customers, claiming bank details have changed, so payments are redirected to the scammer's account.



Ransomware

Cyber criminals lock down your files and demand payment to release them, freezing access to critical files such as plans or project schedules.



Supply chain attacks

Construction projects involve many external partners, and each one adds a potential weak point. Supply chain attacks exploit weaker partners in a project to access the main target. If a supplier's system is compromised, hackers can reach valuable data like project files or financial information.



Data breaches

Unauthorised access to business and client information due to poor password security, misconfigured software, or lost devices. Project plans, financial information and workers' personal details are among the sensitive details that can be exposed.



IoT (Internet of Things) tool vulnerabilities

The rise of IoT devices such as smart tools and sensors are helping drive efficiencies. But many of these connected tools lack robust security protocols, leaving them vulnerable to hackers.

Recent cyber incidents in the construction industry

The construction sector has become a growing target for cyber criminals, with recent cases showing just how prevalent scams are becoming. From email impersonation to data breaches, even simple attacks can cause major financial losses and delays.

These incidents highlight the urgent need for small and family-run construction businesses to strengthen their cyber defences before they're caught off guard.

! Master Builders Queensland

MAY 2025

Master Builders Queensland issued a warning to its members about a sophisticated email scam. The fraudulent email appeared to come directly from the organisation's CEO and was distributed via Adobe. It asked recipients to update their membership details by clicking a link.

The email looked convincing, using branding and language designed to mimic legitimate communication. Upon discovery of the scam, Master Builders Queensland urged members not to click any links, and instead to report the message and delete it immediately.

This scam highlights how attackers often exploit trusted names within the industry to trick busy professionals into sharing sensitive information. Even when an email looks genuine, small clues, like unusual senders, unexpected requests, or unfamiliar platforms, can reveal a scam. Staying alert and verifying requests through official channels is critical to avoiding compromise.



! Total Tools data leak

SEPTEMBER 2024

A data leak hit major Australian hardware chain Total Tools, sparking a warning for small trade and construction businesses to be on alert for cyber attacks.

The leak compromised customer data, including names, credit card details, email addresses, Total Tools passwords, mobile numbers and shipping addresses.

At the time, more than 38,000 customers were reportedly at risk of further cyber incidents.

COSBOA and its member organisations, including Master Builders Australia and the National Timber and Hardware Association, acted quickly to warn customers of the potential for follow-up attacks.



01 001 0110 010
001 1010 10 111
1 1100 1011 011
1000 1110 010 1

Why construction businesses are in the sights of cyber criminals

The construction sector is becoming increasingly appealing to attackers. And it's not just big businesses at risk.

Small firms often store sensitive data such as blueprints, project budgets and supplier details, and regularly process large financial transactions and high-value payments among multiple subcontractors.

Many small construction businesses also use outdated systems or legacy software that lack basic security updates or protocols, making them easier to breach.

Supply chain complexity can also amplify risk, and small contractors are often the weakest link, providing opportunities for attackers to strike larger clients or networks.

In other words, small construction businesses are low-hanging fruit for cyber criminals.



Cyber security is essential for Queensland's construction sector.



With small and family-run businesses at the forefront, safeguarding digital assets, from project plans to financial and business data, is critical.

From the admin desk to the job site, everyone in the business needs cyber security training to spot cyber red flags and know how to prevent a cyber incident.

Master Builders Queensland is committed to equipping our members with the knowledge and tools to protect their operations, ensuring they can focus on building Queensland's future with confidence."

Paul Bidwell

CEO, Master Builders Queensland





Quick wins to safeguard your business today



Use long, strong, unique passwords on all your accounts

☐

Turn on multi-factor authentication (MFA) across all platforms

☐

Use secure cloud storage to back up design files, invoices, and project data

☐

Keep computers, smartphones, tablets, and apps updated, especially field tools and portable devices

☐

Limit admin access to sensitive data only to those who need it

☐

Teach staff to spot fake emails, suspicious links, and unusual requests

☐

Include cyber security training in staff onboarding

☐

Secure your Wi-Fi and IoT tools

☐

Be extra cautious with emails, invoices and any changes to payment details

☐

Follow Cyber Wardens on social media on **@CyberWardens** for tips and real-life scam warnings

☐



REAL LIFE STORY

High-risk transactions

A Master Builders Queensland member, experienced a significant loss after two clients were tricked by fraudulent emails.

One client, David*, called the construction company to check whether his recent payment had come through.

When the company's bookkeeper checked the business bank account, the money was nowhere to be found.

David forwarded his payment receipt, and the bookkeeper immediately noticed the bank details didn't match their usual account. Further digging revealed that David had received an email claiming the business had changed its bank account.

Trusting the email, he had followed the instructions and sent \$15,000 to the "new" account.

Another long-term client, Lisa*, received a similar email and made a payment of \$70,000.

The emails were basic (no logos or contact details), yet appeared convincing enough during busy project deadlines. When the company's bookkeeper checked the accounts, both payments were missing as they were paid into fraudulent accounts.

Police traced David's \$15,000 to an inactive account in Central Queensland and recovered the funds.

However, Lisa's \$70,000 was transferred via Sydney into cryptocurrency, making it impossible to retrieve.

The builder was left out of pocket, while Lisa insisted her payment obligation had been met.



Never rely on email alone to confirm changes to bank details. Always double-check by phone or in person before making or accepting large payments.

**Names have been changed.*

Supply chain cyber security



Cyber security isn't just good business practice anymore; it's a legal requirement for many industries and businesses. Australia has introduced laws to protect the businesses and services our country relies on.

After all, one weak link in the supply chain can serve as a gateway for cyber attackers, putting all connected businesses at risk of data theft, system compromise, and costly disruptions.

Not every small business is directly covered by these laws. But if you work with bigger companies in critical industries (such as construction), they may pass some of these responsibilities down to you through contracts or supplier agreements.

Whether you're a supplier, contractor, or partner, your cyber security practices can help protect (or expose) the businesses you work with.

The Cyber Wardens program helps construction businesses like yours understand why supply chains are a growing focus in Australia's cyber security laws.

In the Cyber Wardens Course Level 3: Cyber Fit for the Supply Chain, you will learn:

-  What it means to be cyber fit, and why small businesses are key to supply chain security
-  The Essential Eight and SMB1001 cyber security standards, explained in plain language
-  How to check if your suppliers and service providers are managing cyber risks
-  Why every business needs an Incident Response Plan, and how to create one

PRO TIP!

The Cyber Wardens Cyber Fit for the Supply Chain course will help you understand your role in the supply chain and what's expected of you.



Free training for Queensland builders and construction businesses



All courses are also offered in webinar format.

START HERE →



Cyber Wardens Foundations ⌚ 10 mins



Learn to spot cyber security red flags and essential strategies to protect your business.

Format: Online course

Suitable for: Busy business owners and employees

Cyber Wardens Level One ⌚ 45 mins



Master four essential cyber security practices to protect your small business from common threats.

Format: Online course

Suitable for: Small businesses seeking improved cyber resilience

Cyber Wardens Level Two Safe AI for Small Business ⌚ 30 mins



Simple and effective ways to keep small businesses safe from complex AI scams.

Format: Online course

Suitable for: Small businesses seeking a deeper understanding of AI's cyber security threats

Cyber Wardens Level Three Cyber Fit for the Supply Chain ⌚ 30 mins

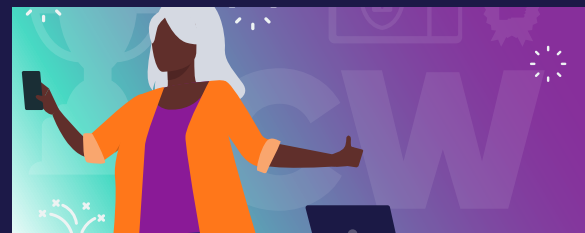


Strengthen your business's cyber security and meet the expectations of clients, partners and suppliers in your supply chain.

Format: Online course

Suitable for: Small businesses seeking to understand their critical role in the supply chain

Cyber Wardens Champions ⌚ 45 mins



Help others stay cyber aware, build safer habits, and protect their business.

Format: Online course

Suitable for: Individuals seeking to help others become more cyber aware

Give your site managers, subcontractors, bookkeepers, and team leads the tools to stay alert and take action.



Don't DIY your cyber security!

Just like donning a hard hat onsite to protect you from physical harm, Cyber Wardens is a simple way to help keep your business safe.

Register today cyberwardens.com.au

An initiative of

