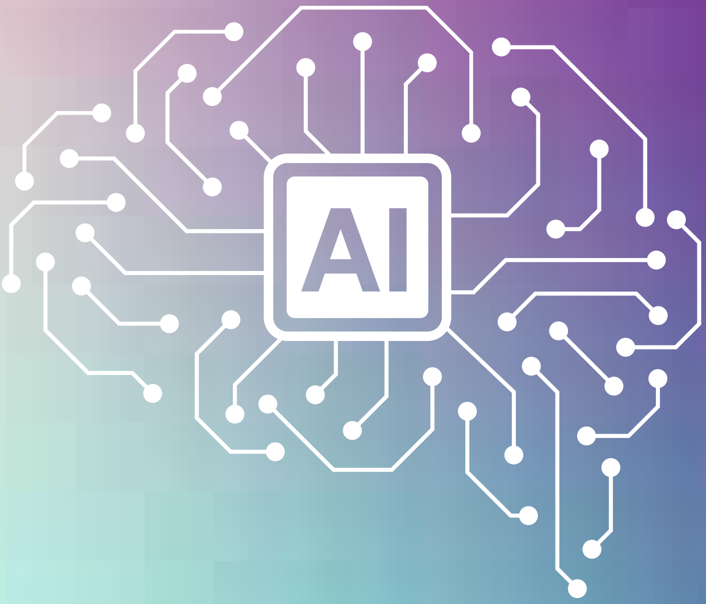
CyberWardens.

Identity theft



FACTSHEET

Identity theft unmasked: What every small business needs to know

Our identities are among the most valuable things we own—they define who we are, both personally and professionally.

But they've also become a prime target for cyber criminals. With just a few pieces of stolen information, criminals can wreak havoc on individuals and businesses alike, from draining bank accounts to damaging hard-earned reputations.

For small businesses, the stakes are even higher. Protecting your identity is more than a name game—it's the key to safeguarding your business and reputation. A single case of identity theft can lead to financial losses, regulatory penalties, and a loss of customer trust that can take years to rebuild.

What is identity theft?

Identity theft occurs when a criminal steals someone's personal or business information to commit fraud or other illegal activities. This can include using stolen data to open accounts, access financial resources, or impersonate an individual or company for malicious purposes.

Think of identity theft as a backstage pass that gives cyber criminals access to all your personal and business details—without your permission.

For businesses, identity theft can lead to unauthorised transactions, compromised customer data, and reputational harm.

How do cyber criminals steal identities?

Identity theft often starts with cyber criminals exploiting vulnerabilities to obtain sensitive information. Common methods include:

- Phishing: Criminals send deceptive emails or messages to trick recipients into sharing login credentials, financial details, or personal information. These scams often appear to come from trusted sources, such as a bank or colleague.
- Data breaches: Large-scale breaches can expose sensitive data, such as employee records, customer details, or business credentials. Cyber criminals use this information to impersonate individuals or businesses.
- Social engineering: By manipulating individuals into sharing confidential information, criminals exploit trust to access sensitive data. This can occur through fake phone calls, emails, or in-person interactions.
- Malware: Malicious software installed on devices can capture keystrokes, passwords, and other sensitive data, giving criminals unauthorised access to accounts or systems.
- Public data mining: Cyber criminals can gather information from publicly available sources, such as social media, business directories, or unsecured online profiles, to build a profile for fraudulent activities. Cyber criminals mine public data like prospectors panning for gold, turning your online information into their treasure.

Consequences of identity theft for businesses

The repercussions of identity theft can be severe for small businesses, including:

- Financial losses: Unauthorised transactions and fraudulent activities can drain resources, disrupt cash flow, and incur recovery costs. A single breach can take a big bite out of your bottom line, leaving your business scrambling to recover.
- Reputational harm: Customers may lose trust if their data is compromised or misused, leading to long-term damage to your brand. Once trust is stolen, it's a hard sell to win it back.
- Regulatory penalties: Failure to protect sensitive information can result in fines or legal action under data protection laws, such as the Australian Privacy Act.
- Operational disruption: Time and resources spent addressing identity theft can take focus away from running the business.

What does identity theft look like?

Identity theft is a widespread problem in Australia, impacting both individuals and businesses.

- In September 2022, telecommunications giant Optus suffered a significant data breach, compromising the personal information of up to 9.7 million customers, including names, birth dates, phone numbers, addresses, and in some cases, driver's licence, Medicare, and passport numbers. The fallout was immense, including significant remediation costs, a $1.5 billion loss in brand value, and the replacement of over 178,000 driver's licences in Queensland alone. A hacker claimed to have deleted the stolen data, but uncertainty remains, leaving customers at ongoing risk of identity theft.
- In early 2023, a Melbourne couple fell victim to identity theft, losing $370,000 to cyber criminals. The hackers gained control of their phones by porting the numbers to another device, which allowed them to access the couple's bank accounts, lock them out, and sell their shares. The criminals also created 20 credit and debit accounts in their names, and accessed their email accounts to try and ensnare friends and family. While the couple was affected by data breaches at Medicare and Latitude, they were uncertain how hackers obtained their licence and passport details.
- In 2024, it was revealed that an Australian gambling syndicate had purchased personal identification documents from individuals for $1,000 each. The syndicate used these identities to create multiple betting and bank accounts, conducting extensive transactions without the knowledge of the individuals involved, and leaving them at risk of identity theft.

How to protect your business and personal information

There are proactive measures you can take to secure sensitive information and prevent identity theft:

- **Use strong passwords:** Create long, strong and unique passwords for all accounts and change them regularly. Avoid reusing passwords across platforms. A strong password is your digital doorman—don't let just anyone in.
- **Enable multi-factor authentication (MFA):** Add an extra layer of security by requiring multiple forms of verification for sensitive accounts and systems. Think of MFA as your cyber bouncer—it checks IDs twice before letting anyone in.
- **Secure data storage:** Encrypt sensitive files and use secure cloud storage services to protect data from unauthorised access. Regularly back up data to prevent loss.
- **Train employees:** Educate your team about the risks of phishing, social engineering, and other cyber threats. Provide training on recognising and reporting suspicious activities.
- **Limit public exposure:** Reduce the amount of personal or business information shared publicly, such as on social media or company websites.
- **Monitor accounts regularly:** Keep an eye on financial transactions, email logs, and other account activity for any signs of unauthorised access.

What to do if identity theft occurs

When in doubt, shout it out—letting everyone know about the breach helps stop the spread of damage. If you suspect identity theft has affected your business or personal accounts, act quickly:

- **Report the incident:** Contact relevant authorities, such as ASD's Report Cyber, Scamwatch, or IDCARE for support and advice.
- **Secure your accounts:** Change passwords immediately, enable MFA, and log out of all active sessions to regain control of compromised accounts.
- **Notify stakeholders:** Inform your bank, suppliers, customers, and employees about the breach to prevent further exploitation.
- **Review financial activity:** Check for unauthorised transactions and notify your bank or payment processor of any irregularities.
- **Update security measures:** Enhance your cyber security defences to prevent future incidents. This could include updating software, investing in detection tools, or revising company policies.

How to stay vigilant against identity theft

As cyber criminals become more sophisticated, protecting your business and personal information has never been more critical.

Take the first step today by enrolling in the free Cyber Wardens training program at **cyberwardens.com.au.**