CyberWardens.

Bon voyage to cyber threats

Help build a culture of cyber safety in the **tourism industry**

Small business cyber security guide for tourism operators, travel agents, and hospitality businesses

An initiative of COSBOA

cyberwardens.com.au

Tourism is a top target for cyber attacks

The tourism industry is a cyber criminal's dream holiday. With its global reach, reliance on technology, and constant flow of financial transactions, it's a target-rich environment for cyber crime.

From the moment a traveller starts planning their trip to the time they return home, they leave a digital footprint. Every booking, payment, and interaction generates valuable data that cyber criminals crave.

Tourism small businesses handle vast amounts of sensitive data, including financial information, personal details, passport numbers and customer bookings, which makes them particularly lucrative targets.

A cyber attack can be devastating for small businesses, leading to significant financial loss, reputational damage, and disruption to business operations.

Cyber criminals are becoming increasingly sophisticated, and small businesses are not immune to these threats. In fact, a cyber attack is reported every 6 minutes in Australia. What's more, the average cost of cyber crime per incident is nearly $56,600 for a small business—an amount many small businesses cannot afford to lose.

To help protect your tourism business, the Council of Small Business Organisations of Australia (COSBOA) has developed a dedicated Cyber Security Guide for the tourism industry. This guide provides essential information on common cyber threats, practical tips to safeguard your business, and steps to help protect your customers' data.

We also encourage you to enrol your staff in the free Cyber Wardens training program. This online course is designed to equip your team with the knowledge and skills to identify and respond to potential cyber threats.

By taking proactive steps to enhance your cyber security, you can protect your business, your customers, and your bottom line.

Cover photo: Tourism Australia

PRO TIP!

The Cyber Wardens Foundations module is a 10-minute introduction to the top cyber crimes, and the cyber security red flags that pose a threat to your business.

ENROL TODAY

cyberwardens.com.au/courses

Most common cyber attacks

With cyber attacks escalating in frequency and sophistication, the industry's reliance on digital systems presents both opportunities and vulnerabilities. From online bookings to guest services, the seamless integration of technology has enhanced customer experiences but also opened doors for cyber criminals.

Here are some of the most common cyber threats in the tourism industry:

1.

Data breach or data theft:

This involves the unauthorised access and theft of sensitive information, such as customer records, financial data, and intellectual property. Scammers then go on to launch secondary attacks using stolen data.

2.

Phishing attacks:

These involve deceptive emails designed to trick recipients into revealing sensitive information or clicking on malicious links.

3.

Ransomware:

In a ransomware attack, cyber criminals encrypt a victim's data and demand a ransom to restore access.

4.

Inbox break-ins

Email compromise attacks are like a break-in in your inbox. Once inside cyber criminals gain access to important information and can launch more damaging attacks.

5.

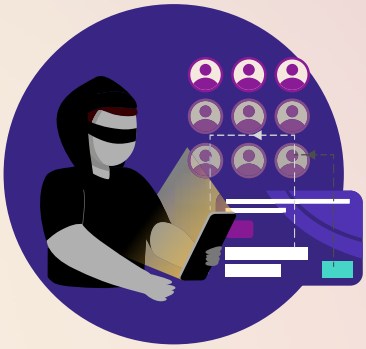
Fake invoices and payment redirection scams:

Business email compromise (BEC) fraud is a type of scam to trick recipients out of money or goods usually by sending fake invoices that redirect payments to hackers.

6.

Banking burglary:

Online banking fraud gives cyber criminals access to your bank accounts allowing them to transfer out your money.



Recent attacks in the tourism industry

The Australian tourism industry has been a frequent target for cyber criminals in recent years.

Inspiring Vacations data breach:

A Melbourne-based travel agency, Inspiring Vacations, inadvertently exposed over 112,000 customer records by leaving an Amazon AWS cloud storage bucket publicly accessible. The compromised data included personal information of customers from Australia, Ireland, New Zealand, and the UK.

Qantas Frequent Flyer data theft:

Approximately 1,000 Qantas customers had their frequent flyer points stolen due to unauthorised access by two overseas airport contractors. The perpetrators accessed and altered customer bookings, leading to the theft of points and potential exposure of personal information, including passport numbers.

Ticketek Australia cyber incident:

Ticketek acknowledged a cyber incident that may have exposed customer personal information, including names, dates of birth, and email addresses. The data was stored on a cloud platform managed by a third-party supplier. Ticketek assured that no payment details or customer accounts were compromised.

Airport Wi-Fi network attacks:

Hackers targeted Australian airport and hotel Wi-Fi networks using inexpensive devices to create fake networks that mimic legitimate ones. These “evil twin” networks trick users into connecting, enabling attackers to intercept personal data. Such attacks pose significant risks to travellers and the hospitality sector.

CASE STUDY

The CrowdStrike crash: a cyber criminal's windfall

The global systems meltdown triggered by the CrowdStrike outage in July 2024 created a perfect storm for cyber criminals. With businesses crippled and panic spreading, scammers saw an unprecedented opportunity to prey on vulnerable individuals—particularly those frustrated and affected by grounded flights.

Almost immediately, suspicious and unverified social media accounts popped up posing as airline customer service representatives, offering to help stranded customers. Reported scams included a range of phishing attacks, like selling people bogus plane tickets, or gaining personal information or financial details from people under the guise of rebooking assistance.

How to avoid tourism cyber scams

Don’t lose your way

- **Verify your visitors:** Ensure every customer is who they claim to be, especially for high-value bookings or unusual requests.
- **Avoid phishing pitfalls:** Be wary of suspicious links or attachments, and double-check email addresses before clicking.
- **Don’t be rushed:** Scammers often create a sense of urgency. Take your time and verify information before making decisions.

Protect your belongings

- **Lock down your devices:** Strong, unique passwords and multi-factor authentication are your first line of defence.
- **Keep your guard up:** Regularly update software and antivirus programs to protect against the latest threats.
- **Beware of unexpected guests:** Don’t grant remote access to your computer unless you’re absolutely certain of the person’s identity.

Unpack your luggage carefully

- **Scrutinise any refunds:** Verify refund requests thoroughly, especially if they seem unusual or urgent.
- **Invoice inspection:** Double-check every invoice for discrepancies or red flags.
- **Resist the rush:** Don't feel pressured to make hasty decisions when dealing with unexpected requests or offers.

Train your team

- **Knowledge is power:** Educate your team about common scams and how to identify them.
- **Verify, verify, verify:** Encourage staff to confirm information with trusted sources before taking action.
- **Report suspicious activity:** Create a process for reporting potential scams.

Stay alert, not alarmed

- **Trust your gut:** If something feels off, it probably is. Don't hesitate to end a conversation or ignore a request.
- **Verify independently:** Always verify information through official channels before taking action.
- **Be prepared:** Have a plan in place for responding to a cyber attack, including contacting relevant authorities.

Photo : Tourism Australia

Cyber security checklist

- [ ] **Read this guide** and start recognising where you can improve your cyber safety habits
- [ ] Complete the free Cyber Wardens training and encourage your staff to enrol. Sign up at cyberwardens.com.au
- [ ] Regularly **discuss** cyber security with your team including what data you collect and how you protect it
- [ ] Investigate ways to **share personal and financial information** in a secure way and know your client data and privacy obligations
- [ ] **Look twice** at invoices, emails and social posts before engaging
- [ ] **Follow** Cyber Wardens on social media for simple small business safety advice
- [ ] **Regularly review** the simple steps in your Cyber Security Action Plan

Photo : Tourism Australia

All aboard small business cyber security with **Cyber Wardens**

Cyber security doesn't stop with just one person—it's a team effort!

Make sure your entire team has the knowledge and tools they need to keep your business safe online.

There are many ways for you and your team to complete the Cyber Wardens training.

Choose from our expanding course offering:

CYBER WARDENS FOUNDATIONS

A 10-minute module helping you identify the cyber security red flags that pose a threat to your business

CYBER WARDENS LEVEL ONE

A short course introducing you to basic cyber security measures and actions to improve your cyber awareness

CYBER WARDENS FOUNDATIONS WEBINAR

An interactive session delivered live or on demand where participants can learn through live engagement with a Cyber Wardens educator

CYBER WARDENS REFRESH

A module where Level One graduates can refresh their skills and knowledge while being introduced to new and emerging threats.

Visit **cyberwardens.com.au/courses** to enrol in **FREE** training and access resources to share with your team.

Join the Cyber Wardens community

CyberWardens.

Don't lose your way: keep your tourism business cyber-safe!

Complete the Cyber Wardens training in as little as 10 minutes and start your journey to cyber security.

CyberWardens.

An initiative of COSBOA

Enrol today at **cyberwardens.com.au**