



4 Practical Steps to Protect Your Hotel



Hotel Cybersecurity: A Practical Guide for Modern Hotels

Understanding how cybercriminals think – and how to
stay one step ahead

Discover the VISIT Platform → **visit.com**

Table of Content

02	INTRODUCTION
03	THE RISING THREAT LANDSCAPE
04	WHY THE HOSPITALITY INDUSTRY IS A PRIME TARGET
05	UNDERSTANDING THE AI BOOSTED HACKER'S PLAYBOOK
06	PROTECT YOURSELF: PERSONAL CYBER HYGIENE
07	PROTECT YOUR HOTEL: THE ULTIMATE 4 STEP GUIDE
08	TRENDS & EMERGING THREATS IN 2025
09	CYBER RESILIENCE SCORECARD
10	HOW TO CALCULATE YOUR CYBER RESILIENCE
11	INTERPRETING THE SCORECARD
12	KEY TAKEAWAYS & ACTIONS

Introduction

AI is not only helping us — it's also helping hackers. We need to adapt faster.

“

*“Cybersecurity is not a policy — it's a culture.
Awareness is the first line of defense.”*


Head of AI,
VISIT

Access simple, effective actions to reduce your cybersecurity risks.
Let's dive in!

The Rising Threat Landscape

Cybercrime has become one of the largest industries in the world – estimated at 10.5 trillion dollars in 2025, almost the size of the global tourism industry.

If hacking were a country, it would rank third in the world by GDP, just after the US and China. For hospitality businesses, this isn't just a distant concern. The industry is now a prime target for cyberattacks, with 31% of hospitality companies reporting a data breach in 2024.

Phishing remains the most common attack method, representing 84% of all cyber incidents. It's cheap, easy to automate, and increasingly sophisticated. Once an employee clicks a malicious link, attackers can install ransomware, steal data, or infiltrate your systems. Ransomware alone increased by 67% in the first half of 2025 – an 84% year-on-year jump.

Why the hospitality sector? Hotels store massive amounts of guest information – passports, credit card details, booking data – and operate around the clock, often with temporary or seasonal staff. Peak season brings a 21% increase in attacks, as hackers exploit busy operations and less-experienced employees.



AI-impact

83% use AI in cyber attacks

Why the Hospitality Industry Is a Prime Target

Hospitality businesses hold some of the most sensitive customer information in any sector – from ID and credit card numbers to booking history and preferences. This data is incredibly valuable on the dark web. Combine that with complex tech stacks (PMS, POS, IoT devices, Wi-Fi networks) and human factors like temporary staff, and you have a perfect storm for attackers.

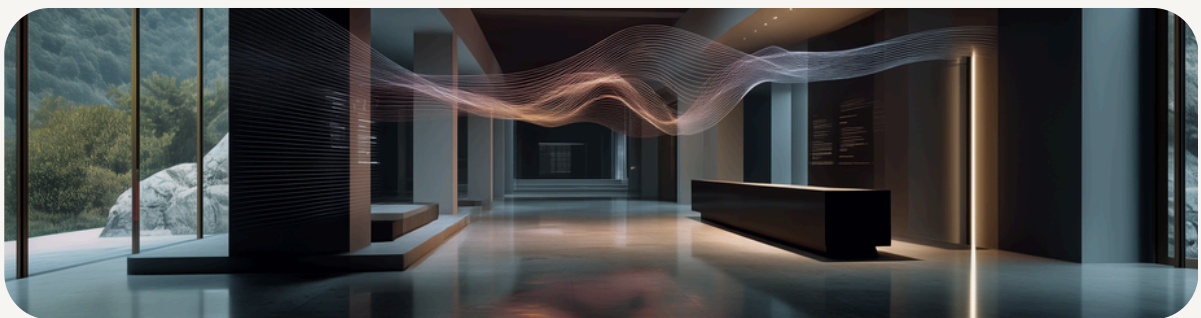
GUEST DATA

90%

*of attacks against hotels **aim to steal guest data***

58%

*of breaches **begin with phishing**. Seasonal peaks bring added risk – during busy months, security checks often take a back seat to operations.*



Understanding the AI Boosted Hacker's Playbook

To defend against attacks, it helps to think like a hacker. Cybercrime operates like a business — each attack follows a predictable return-on-investment logic. The goal: spend as little time and money as possible to get the biggest reward. Here's how it works.

Reconnaissance

Hackers start by gathering data. Social media and LinkedIn are goldmines for finding employee names, roles, and new hires. They also look at local events, hotel partnerships, and even guest information. With AI, this process is automated — AI tools can scrape the web, select targets, and identify the best moments to strike.

Initial Contact

Once a target is identified, hackers create a personalized phishing email, often followed by a fake voicemail or phone call. Using AI voice cloning, they can copy a manager's voice with just 20 seconds of recorded audio. Combining email and voice contact increases the click rate by 40%. The AI also translates the message, mimics writing tone, and sends it during the busiest shifts — boosting credibility and success rates.

Deployment

When an employee clicks the link or opens the attachment, malware is deployed. It spreads across the network, gaining access to PMS, CRS, or CRM systems. Attackers often use fake login pages to harvest credentials. Once inside, they extract valuable guest and payment data.

Extortion and Data Leak

After locking systems with ransomware, hackers demand payment to restore access. They may also threaten to leak guest data publicly. AI is used to calculate ransom amounts based on your hotel size, season, and estimated hourly losses — pricing the ransom just right to pressure you into paying.

Profit

For hackers, profit mainly comes from three streams: **ransom payments, selling guest data, or scamming guests directly through fake payment reminders.** For hotels, that means triple or even quadruple losses — financial, reputational, and regulatory. Even worse, most insurance providers no longer cover ransom payments.

Protect Yourself: Personal Cyber Hygiene

Cybersecurity starts with individuals.
Every click, password, and update counts.

Here are key steps you can take to
reduce personal risk:



Use unique passwords for every account. 81% of attacks start with password reuse.



Use a password manager (Apple, Bitwarden, 1Password, etc.).



Enable Multi-Factor Authentication (MFA) everywhere — it stops 99.9% of automated attacks.



Stay alert to red flags. AI-generated phishing emails look professional, correctly spelled, and personalized. Be cautious of messages urging you to act fast or click a link.



Keep your devices updated and protected with antivirus software.



Back up your data regularly — if ransomware hits, backups can save you.



Did you know? 81% of hacks start with password reuse

Protect Your Hotel: The Ultimate 4 Step Guide

1. Build a culture of security

Security is not a policy, it is business value. Encourage staff to prioritize security.

Actions:

- Identify the most likely scenario for your business
- Run your staff through the scenario and explain how to stop it.

68%

Human error
involved in
breaches

2. Employee Awareness & Training

Keep your employees up to date with the latest trends. Do phishing simulations and security workshops. Train employees on AI voice and video deepfakes and do not forget incident reporting.

Actions:

- Schedule a phishing test, start an employee training program
- Hire a third party to perform a security tests

- 60%

Success rate
after training

3. Safe Communication & Data Handling

Share sensitive information only through secure channels and limit access to guest data. Always back up your files. Trust but verify, which means; double-check identities or use a secret code before sharing details. Use multiple channels to confirm requests when something feels off.

Actions

- Review user permissions now and regularly
- Ensure there is more than 1 communication channel

4. Follow Compliance Standards

Work according to **GDPR** and **ISO27001** and apply industry best practices for data protection and information security. These standards guide how we collect, store, and share data responsibly. Following them helps us stay compliant, avoid costly fines, and protect our reputation by showing guests and partners that we handle their data with care.

Action

- Review your compliance status



At Visit Group, regular third-party security tests help identify vulnerabilities early and strengthen systems — a practice every business should consider.

Trends & Emerging Threats in 2026

Cyber threats continue to evolve rapidly, especially with the integration of AI and connected devices. Understanding emerging risks helps you stay ahead.



IoT attacks

By the end of 2025, 60% of hotel cyber incidents are projected to come through IoT devices like smart locks, thermostats, and TVs.



Deepfakes

AI-generated voice and video clones are used for fake invoices and wire-transfer scams.



CEO impersonation

Hackers can clone executives' voices or faces from conference recordings to request urgent payments.



AI-powered phishing

Attacks are localized and personalized in any language, making them harder to detect.

Cyber Resilience Scorecard

Use the scorecard to assess your organisation's cyber resilience across five key areas by rating each from 1 (Initial) to 5 (Optimizing). Calculate your overall score by averaging the five ratings.

A score above 4 indicates a strong level of cyber resilience, with opportunities for further optimization through continuous improvement.

Review and update the scores quarterly to track progress, identify gaps, and plan focused improvements.

Why this works well for hotels:

- ✓ Simple scoring, no certification required
- ✓ Focus on real-world risks and daily operations
- ✓ Clear path from "basic security" to "cyber resilience"

Cyber Resilience Maturity Levels (Inspired by CMMI)

This scorecard is inspired by the Capability Maturity Model Integration (CMMI) and evaluates not only whether security controls exist, but how well they are managed, measured, and continuously improved.

Level

Maturity Description

1. Initial	Activities are ad hoc or not implemented. Success depends on individuals rather than defined processes.
2. Managed	Basic practices are in place and responsibilities are assigned, but processes are not fully standardized.
3. Defined	Processes are documented, communicated, and consistently followed across the organisation.
4. Quantitatively Managed	Processes are measured using KPIs and managed based on data and regular reviews.
5. Optimizing	Continuous improvement is embedded, using metrics, testing, and lessons learned to improve resilience over time.

How to Calculate Your Cyber Resilience

Scoring Guidance: 1 = Initial 3 = Defined 5 = Optimizing

1. Identity Protection

Measure:

- % of accounts with Multi-Factor Authentication (MFA) enabled
- % of employees using a password manager
- Target: Use MFA everywhere — it stops 99.9% of automated attacks. Use a password manager — it prevents 81% of attacks.

2. Employee Awareness & Training

Measure:

- % of employees who completed phishing and security awareness training
- Phishing simulation click rate
- Target: Train staff on phishing — it stops 60% of attacks. 100% of employees trained, <10% phishing simulation click rate.

3. Safe Communication & Data Handling

Measure:

- % of employees using secure channels for sensitive information
- Frequency of access permission reviews
- Target: Share sensitive information only through secure channels, limit access to guest data, and review permissions quarterly.

4. Device & System Security

Measure:

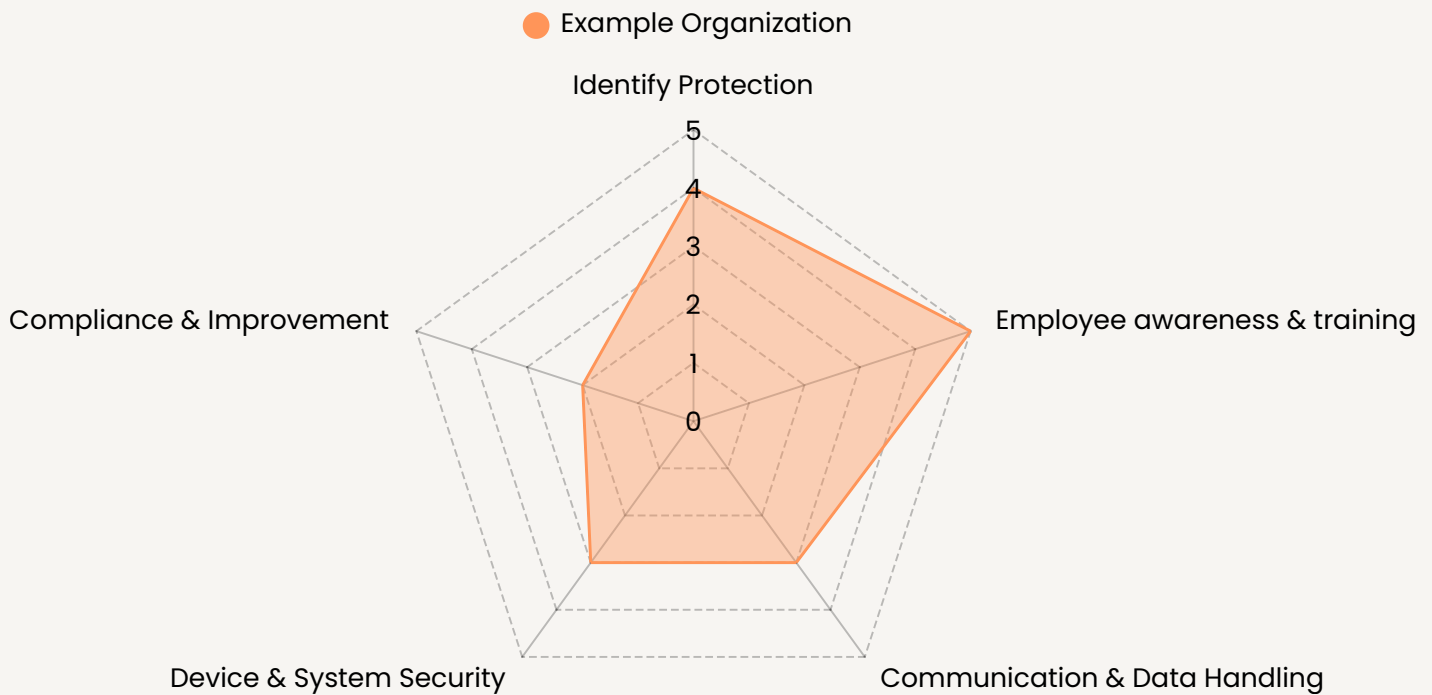
- % of devices and systems updated and protected
- Frequency of backup testing
- Target: Keep devices updated with antivirus protection and test data backups at least twice per year.

5. Compliance & Continuous Improvement

Measure:

- Completion of annual GDPR and ISO27001 compliance review
- Frequency of third-party security tests or audits
- Target: Conduct an annual compliance review and hire a third party to perform security tests.

Interpreting the Scorecard



How this scorecard supports continuous improvement

By combining technical controls, process maturity, and regular measurement, this scorecard helps organisations move from reactive security efforts toward a structured and continuously improving cyber resilience program.

Regular reviews and data-driven improvements align the organisation with higher maturity levels, supporting long-term resilience rather than one-time compliance.

Takeaways & Key Actions

Top three actions

If you only remember three things from this guide, make it these:

99.9 %

Use MFA –
stops 99.9% of attacks

81 %

Use a Password Manager
– stops 81% of attacks

60 %

Train your staff on
phishing – reduces
success rate by 60%

MAKE IT DIFFICULT

Together, these simple actions make attacks far more expensive for hackers – and much less likely to succeed. In other words, you've just saved your business potential losses.

ABOUT VISIT

Visit empowers the experience industry with technology that drives efficiency, innovation, and safety. Our mission is to help tourism and hospitality businesses thrive in a connected world – securely.

[Learn more at visit.com](https://visit.com)





Sources

Cobalt. Top Cybersecurity Statistics 2025
SentinelOne. Cybersecurity Statistics
VikingCloud. Cybersecurity Statistics & Industry Trends