

Your guide to cyber security for hospitality businesses



A guide for hospitality businesses.

From ransomware to data hacking or fraud, it is important to understand the potential issues, and what you can do about it!

In recent times we have see several high-profile businesses who have been disrupted due to hackers. Such as Marks and Spencer. Hospitality businesses are not immune with just this summer, several Italian hotels and Jeremy Clarkson’s pub losing £27k to hackers. Roslyns have tight security measures in place to protect our clients, and this guide will show you how you too can protect your business, and your customers.



CONTENTS

Select a topic to jump to that page

- [Point-of-sale \(EPOS\) & card payment](#)
- [Supplier fraud & invoice scams \(email/phone/WhatsApp\)](#)
- [Phishing and stolen logins](#)
- [Ransomware](#)
- [Social media & review sites](#)
- [Data protection \(GDPR\) & CCTV](#)
- [Starters/Leavers & shared devices](#)
- [Email and domain protection](#)
- [Chargebacks & card-not-present \(CNP\) fraud](#)
- [Training and security culture](#)
- [Physical risks](#)
- [Worse case scenario](#)
- [Your quick win action plan](#)



Point-of-sale (EPOS) & card payments

There is potential for card details to be stolen or intercepted.

Potential problems

- Card skimming/tampering with terminals.
- Malware or out-of-date tills.
- Staff writing card details on paper or saving images.
- POS equipment on the same Wi-Fi as guests.

What you can do

- Daily tamper check sheet: verify seals, cables, serials; lock terminals away overnight.
- Keep tills/PCs patched & antivirus-protected; remove unused apps/USB ports.
- Never store card data (paper or photos).
- Put POS on its own network/VLAN; different SSID/password from guest Wi-Fi. ([HOW?](#))



Supplier fraud & invoice scams (email/phone/WhatsApp)

You could be contacted by fraudsters pretending to be a supplier.

Potential problems

- Fake bank-detail changes, urgent “pay today” requests, look-alike domains.

What you can do

- Call-back rule: if supplier bank details change, phone your known contact before paying.
- Use shared AP inbox for invoices with rules to flag “urgent”, “overdue”, bank changes.
- Multi-factor authentication (MFA) on email for owners/managers/accounts.
You’ll be glad to know Roslyns already use MFA for our own client portal.

Phishing & stolen logins (staff emails or bookings)

Fraudsters could gain access to your systems by pretending to be someone you know at work.

Potential problems

- Password reuse; fake Microsoft/Google login pages; OAuth “app” access granted by mistake.

What you can do

- Password manager + auto-generated unique passwords.
- MFA everywhere: email, PMS, booking engine, payment portal, social media. You’ll be glad to know Roslyns already use MFA for our own client portal.
- Short phishing drill each quarter (3 examples; how to report).

Ransomware

Your data could be stolen and held to ransom with threats of important data deleted, or customer data sold on to other fraudsters.

Potential problems

- Encrypts bookings, EPOS data, accounts; threatens to leak HR/guest data.

What you can do

- Keep data backups with one offline copy; test restores monthly.
- Keep systems patched, disable macros by default, restrict admin rights.
- Segment networks (guest / POS / office / back-of-house).
- Incident card by the till: how to isolate cable/Wi-Fi, who to call, how to restore backups



Social media & review sites

Hackers could hold your online profile to ransom, or competitors damage your reputation.

Potential problems

- Hijacked Facebook/Instagram/Google Business leading to reputational damage & scams.

What you can do

- Business Manager/brand accounts (no personal owner logins).
- MFA enforced; remove leavers the same day or change passwords; keep a recovery admin.
- Store recovery codes in your password manager's shared vault.



Data protection (GDPR) & CCTV

You could accidentally breach your legal responsibilities to keep data safe.

Potential problems

- Excessive retention, staff/guest data leaks, unclear responsibilities.

What you can do

- Create a data map: bookings/HR/CCTV/marketing. Where it is stored, who has access, how long it is kept.
- CCTV signs, limit retention (e.g., 30 days), restrict access; log any exports to police/insurers.
- Ensure you are registered with the Information Commissioners Office.
- Keep card payments secure using **Payment Card Industry Data Security Standard** (PCI DSS). [FIND OUT MORE](#)

Starters/Leavers & shared devices

Employees could commit fraud using their access.

Potential problems

- Shared passwords on tills or reception PCs; ex-staff still have access; new staff could be untrustworthy.

What you can do

- One person, one login. Create a Starters/Movers/Leavers checklist.
- Auto-expire temporary accounts; disable leavers same day.
- Lock screens after 5–10 minutes; require PINs/biometrics on mobiles/tablets.
- Ensure thorough background check on new employees before issuing access.

Email and domain protection

Scammers could spoof your emails or website

Potential problems

- Spoofed emails sent to suppliers/staff; fake newsletters to guests, potentially issuing *new bank details* or requesting to click a link to pay a deposit for a great discount.

What you can do

- Set up SPF email security ([How?](#))
- Use a reputable bulk-email/CRM with unsubscribe and rate-limit controls.
- Monitor mailbox rules and forwarding (classic sign of compromise).



Chargebacks & card-not-present (CNP) fraud

(hotels/large bookings)

Fraudsters could use stolen cards to make payments over the phone/online

Potential problems

- Stolen cards used for deposits; disputes weeks later.

What you can do

- Use 3-D Secure where possible; verify billing address and contact.
- Keep evidence trail (booking logs, check-in ID policy, signed Ts&Cs).
- Set deposit/hold rules and limit manual card entry.



Training and security culture

Without employee engagement, you can never have a strong cyber security/fraud policy.

Potential problems

- High staff turnover; inconsistent practices between shifts/venues.

What you can do

- 15-minute induction covering: passwords, phishing, POS tamper check, incident reporting.
- Quarterly refresher with real screenshots; reward "spot & report".
- Keep one-page posters at the till/back office (who to call, do/don't).

Physical risks

Scammers could physically intercept your security

Potential problems

- Unlocked comms cupboard; exposed router; USB drops

What you can do

- Keep all tech access locked and ban employees from plugging in USB drives

Worse case scenario ...

- **Can't take cards:** instant lost sales
- **Tills down:** no tabs, no bookings, wrong orders, long queues
- **Ransomware:** days closed, pay to recover, big clean-up costs
- **PCI penalties:** higher processing fees, fines, forced audits
- **Supplier scam:** pay a fake bank account and stock doesn't arrive
- **Data breach:** ICO action and claims
- **Insurance:** claims refused if basics weren't in place
- **Bad reviews/press:** "couldn't pay / data stolen"

What's next?

How can you get started with protecting your business from cyber attacks of fraud?

Why not get started on your quick wins and then put in place a schedule to get where you need to be.

- **Turn on Multi Factor Authentication** for email, PMS/booking admin, payment portals, social accounts, and crucially make sure your accountant's portal uses MFA!
- **Separate Wi-Fi** (guest vs business vs POS), change all default passwords.
- **Backups & restore test** (prove you can restore a file).
- **Daily Point Of Sale tamper sheet;** remove shared logins.
- **Patch** Windows/macOS, routers, CCTV firmware. ([How?](#))
- **Speak to your insurers** about adding cyber security insurance or approach a [broker](#) for a new insurance package that includes this.

Further support ...

As specialists in business services to the hospitality sector, Roslyns can help every step of the way. Just click or tap your way to knowledge!

[What taxes will my hospitality business pay?](#)

[How can I pay less tax?](#)

[What about my own income and taxes?](#)

[What do I need to do when employing staff?](#)

[Is stocktaking important in a hospitality business?](#)

[CONTACT US](#)

Links to the official government advice

[Setting up as a sole trader](#)

[Setting up a limited company](#)

[Business taxes](#)

[Personal Taxes](#)

[Employer taxes](#)

Please note: These guides are based on the tax year during which they were written and are intended to outline the basic aspects of the topics addressed.

Please take advice based on your specific situation and business.

Contact us on support@roslyns.co.uk