Nutbourne

Cyber Security: the basics

Protecting your charity. Protecting your mission.

Who?

Patrick Burgess

Technical Director, Nutbourne

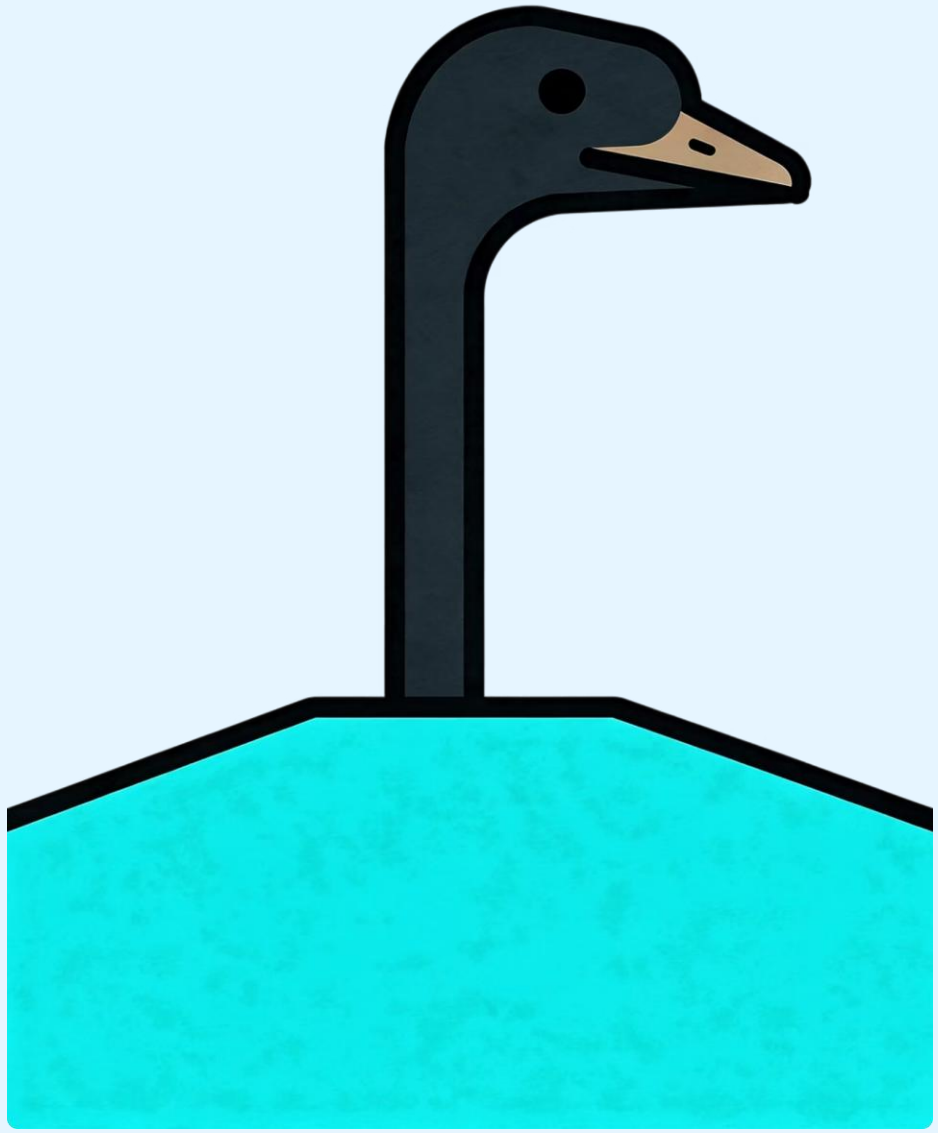
Patrick leads the technical team at Nutbourne, helping organisations of all sizes navigate cyber security with clarity and confidence.

Nutbourne

"It won't happen to us."

A dangerous assumption. Cyber criminals target any weak system — including charities, fundraisers and not-for-profits.

Every organisation is a target. The only question is whether you're ready.



"No one wants our data."

Think again. Donor details, bank records, beneficiary data, and grant information all have value. Attackers can sell it, steal it, or use your access to reach your supporters and partners.

Your data is worth something. Don't let criminals set the price.

"It just gets in the way."

Security can feel like friction: extra steps, extra processes, slower workflows. But a breach costs far more — in lost donor trust, reputational damage, and operational disruption.

⚠ Today's inconvenience is cheaper than tomorrow's recovery.

WHEN, Not IF

The shift every charity leader must make: cyber threats are no longer a question of *whether*, but *when*. Even major organisations with dedicated security teams have been breached.

If it can happen to them, it can happen to you. Preparation is the difference.

Cyber Breaches in UK Charities & Not-for-Profits:

The Hard Numbers

Cyber attacks are no longer a distant risk for charities and not-for-profit organisations. They are real, rising, and the sector is increasingly in the crosshairs.

59%

Faced a Breach

Nearly 59% of UK SMEs were breached last year, charities face the same threat landscape, often with fewer defences.

Source: Hiscox Group

60%

Unable to Recover

60% of SMEs fail within 6 months of a major cyber attack. For charities, a breach can mean permanent closure or loss of funding.

Source: University of Salford – Cyber Foundry

1/3

Faced Fines

One-third of affected organisations faced major regulatory fine, charities are subject to GDPR and Charity Commission requirements.

Source: Hiscox Group

Common Cyber Attack Types in 2025

These four attack vectors drive most incidents affecting charities and not-for-profits today.

🎣 Social Engineering & Phishing

85% of SMEs affected in 2025. Cybercriminals use convincing emails to steal confidential information or gain access — charities are frequent targets due to high staff turnover and volunteer workforces.

🕵️ Insider Threats & Data Theft

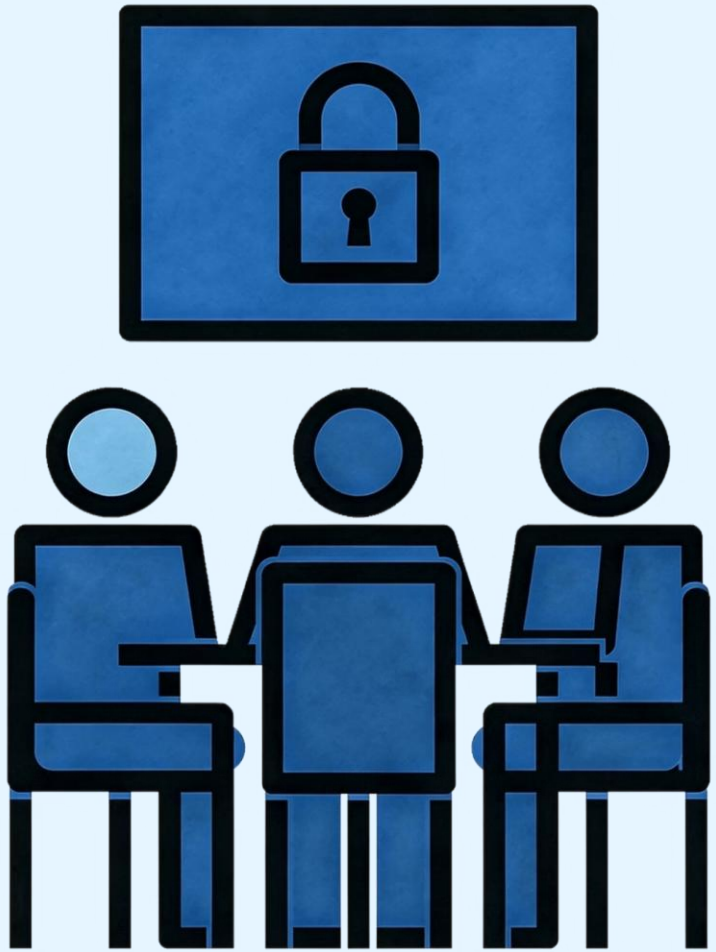
16 billion records exposed in June 2025 alone. Misused access from employees, contractors, volunteers, or partners can do major damage.

🔓 Exploiting System Vulnerabilities

23,600 vulnerabilities disclosed Jan–Jun 2025. Attackers exploit unpatched weaknesses to gain access fast — outdated systems common in the third sector are especially at risk.

💰 Ransomware & Data Exfiltration

27% of SMEs affected in 2025. Data is locked or stolen — often both at once. For charities, donor and beneficiary data is a prime target.



Cyber Security Is Everyone's Duty

How do we work out what to prioritise with limited resources?

Most charities and not-for-profits operate with tight budgets and lean teams. You can't do everything — so focus on **critical assets, likely threats, and the highest-impact actions.**

Prioritisation is about making smart, informed decisions on where to act first.

You cannot protect your data if you don't know where it is.

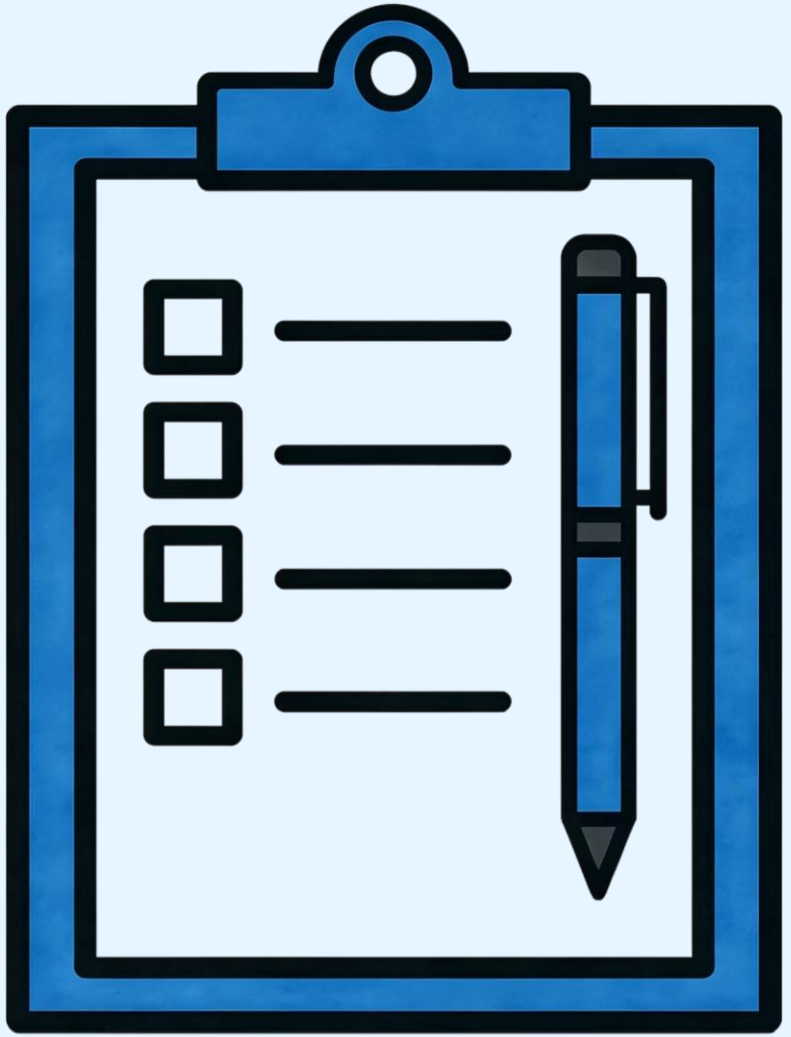
Where Are the Crown Jewels?

For charities and not-for-profits, your crown jewels might include:

- Donor and supporter personal information
- Beneficiary and client records
- Bank accounts and payment systems
- Grant and funding data
- Websites and applications
- Laptops, tablets and mobile phones
- HR and volunteer data
- Confidential correspondence

Information asset register = A List

Five Things You Should Have Today



NON-NEGOTIABLE #1

Multi-Factor Authentication

Stronger Account Security

MFA adds an extra layer beyond passwords.

Phishing Protection

MFA stops most phishing and credential-stuffing attacks.

No Exceptions — Ever!!

Enable MFA on every account. No exceptions.

What is this buzz about Passkeys?

NON-NEGOTIABLE #2

Secure Backups

Protecting Critical Data

Regular, tested backups let you recover from data loss.

Offsite & Cloud Storage

Store backups separately, ideally in the cloud, to avoid shared risk.

Encrypted & Immutable

Encrypted, immutable backups protect recovery data from tampering.

NON-NEGOTIABLE #3

Security Awareness Training

Ongoing Education

Short, regular training keeps security top of mind — especially important with volunteers and high staff turnover.

Simulated Phishing

Safe phishing tests build real-world awareness across your whole team.

Create a Cyber Culture

Encourage curiosity, remove cyber shaming and build a safe environment to report concerns.

NON-NEGOTIABLE #4

Protecting Email Communications

Blocking Malicious Emails

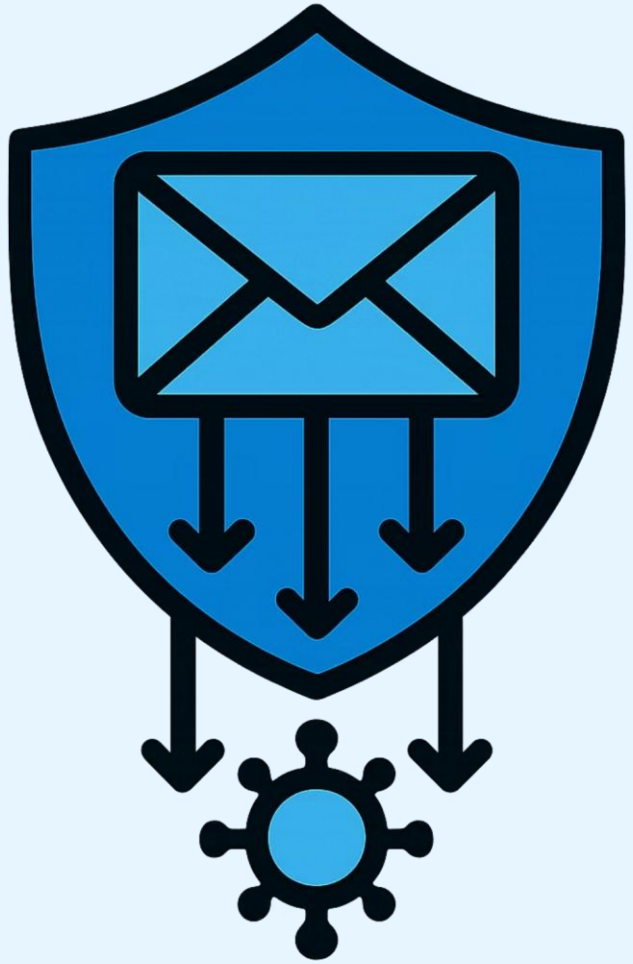
Quarantine phishing, spoofing, and attacks automatically.

Attachments & Links

Scan files and URLs in real time for malware and malicious sites.

Preventing Data Loss

Stop sensitive donor or beneficiary data from leaving the organisation.



NON-NEGOTIABLE #5

An Incident Response Plan Matters

Act Swiftly, Reduce Harm

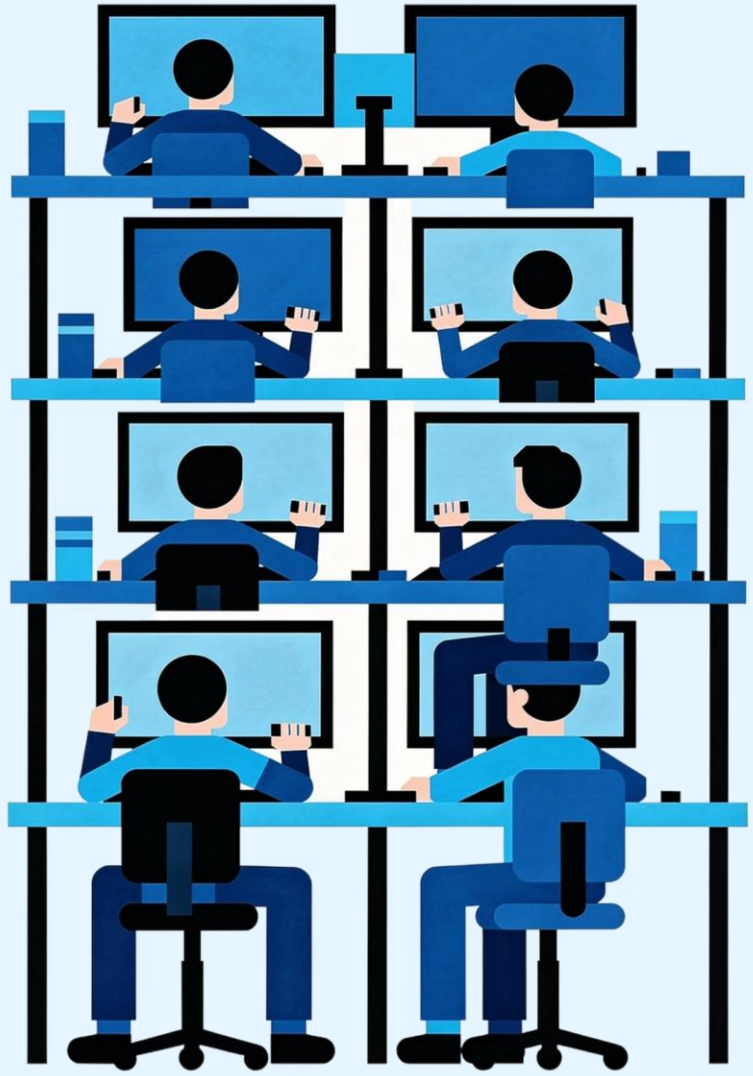
A plan helps your team respond fast and contain damage.

Clarity Prevents Panic

Clear roles, escalation paths, and templates keep everyone aligned — including trustees and senior leadership.

Know Where to Get Help

Pre-agreed contacts — IT, legal, insurance, Charity Commission — mean you're not alone.



Key Takeaways

1

Change the Mindset

It's when, not if, charities are not exempt.

2

Know What Matters

Build an information asset register.

3

Five Non-Negotiables

MFA, backups, training, email protection, response plan.

4

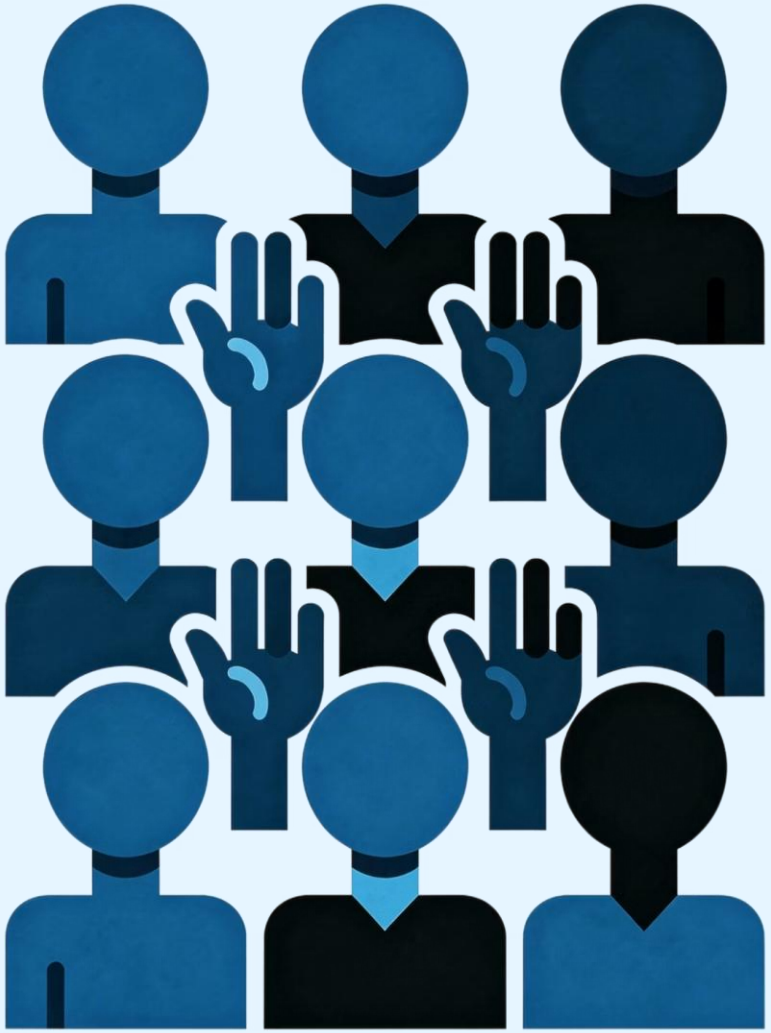
Use Available Resources

NCSC tools and your IT partner can help.

5

Understand the Gaps

Complete a benchmark and create a roadmap to move forward.



Questions?