The Top 5 Cyber Threats Facing Charities in 2025

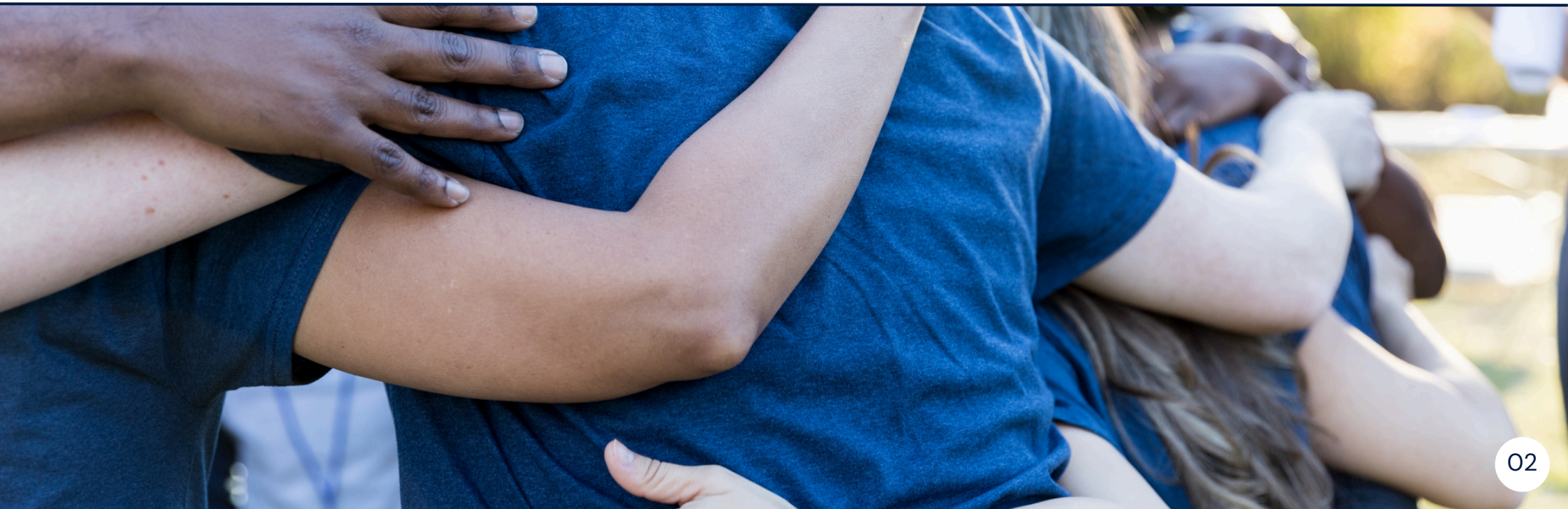
wanstor

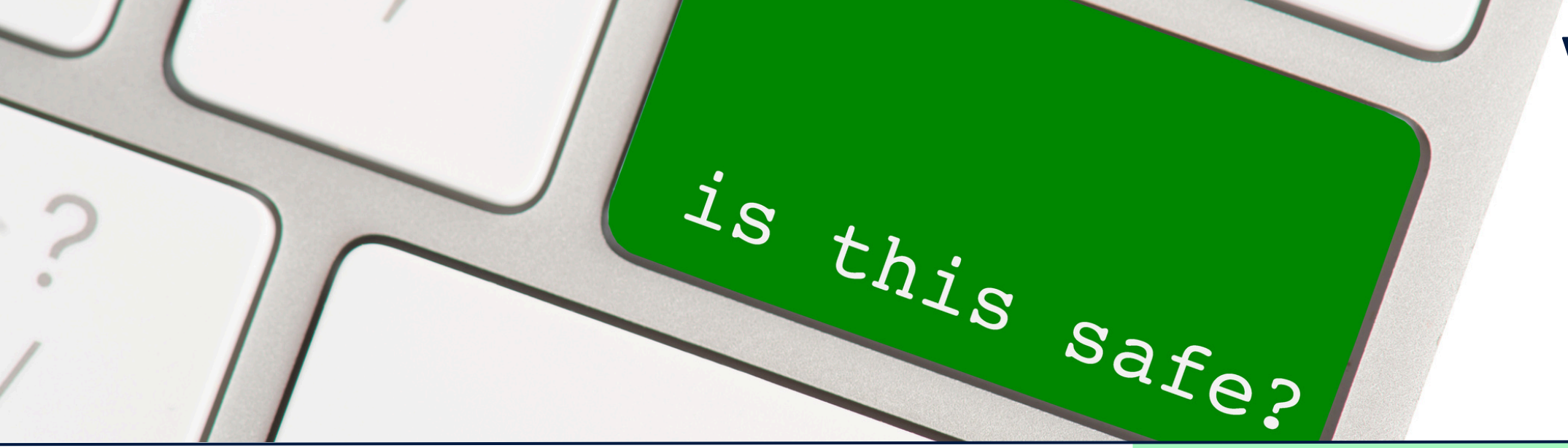
Contents

Charities are vital to communities across the UK, delivering essential services and making a real difference. However, their unique operating environments - including limited budgets, distributed teams, and high trust from the public - make them an increasingly attractive target for cyber criminals.

According to the National Cyber Security Centre, over 30% of UK charities experienced a cyber attack or data breach in 2024. Without strong protections in place, the risks can be significant: loss of sensitive data, disruption of services, financial penalties, and reputational damage.

Learn how to safeguard your charity from the five biggest cyber threats in 2025, with practical, budget-conscious defences you can implement today.





1

Phishing and Social Engineering

Key Insight: In 2024, 83% of phishing attacks against charities targeted financial or donor information.

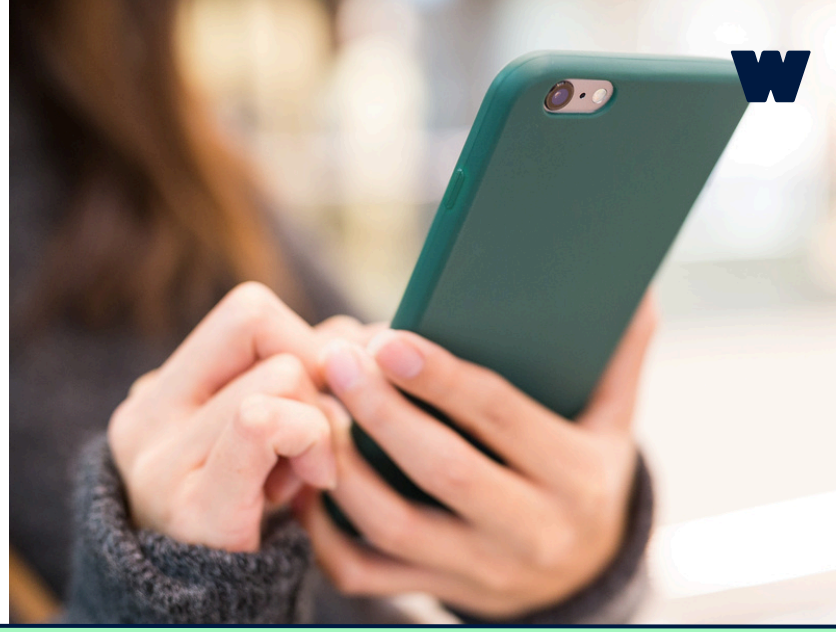
What is it?

Phishing is a form of cyber-attack where attackers impersonate legitimate organisations, often sending fraudulent emails or messages to trick individuals into revealing sensitive information such as login credentials, financial details, or personal data.

Social engineering is a broader term that encompasses manipulative tactics used to exploit human psychology, such as posing as a charity volunteer or donor to steal information.

Why it's a threat:

Phishing and social engineering attacks are highly effective because they exploit human trust and curiosity, which are often core elements of charity operations. Whether it's a fraudulent email asking for a donation or a link to a fake charity webpage, these attacks prey on goodwill, making charities especially vulnerable.



Actionable Steps:

MFA (multi-factor authentication):

Add an extra layer of protection to user accounts by requiring two or more verification methods. This significantly reduces the risk of unauthorised access, even if passwords are compromised.

Email Security Protections:

Invest in anti-phishing and email filtering solutions to detect and block malicious emails before they reach inboxes. Features like link scanning and attachment sandboxing can help stop threats before they cause harm.

Cyber Awareness Training:

Ensure staff and volunteers can recognise suspicious emails and requests. Regular training should cover common tactics used by cybercriminals and how to report phishing attempts.

Verify Requests

Always verify any donation request or communication from donors through a secondary method, such as a phone call, before taking action.

2

Ransomware

What is it?

Ransomware is a type of malicious software that locks or encrypts an organisation's data and demands a ransom for its release.

It often spreads through phishing emails or unsecured networks, locking vital files or systems, and can bring an entire charity's operations to a halt.

Why it's a threat:

For charities, ransomware attacks can be devastating. They not only disrupt essential services but can also damage relationships with donors and other stakeholders. Charities are especially attractive targets because they often lack the resources to recover from such attacks.

Key Insight: The average ransom demand against UK charities in 2024 was calculated at £24,000.

Actionable Steps:

Regular Backups:

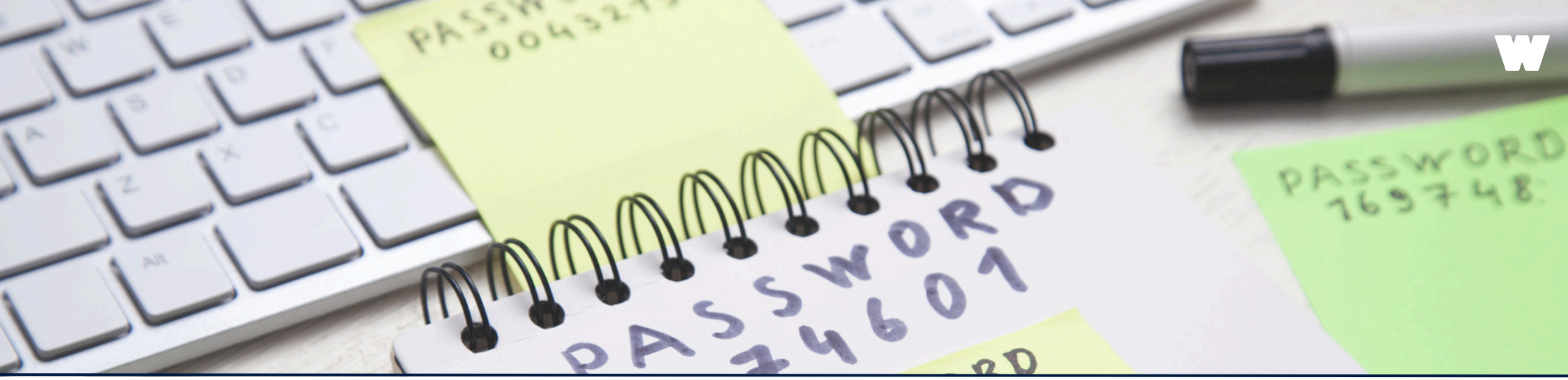
Regularly back up your data and store copies in secure, encrypted environments, offline or in the cloud. Use immutable backups, which cannot be altered or deleted for a set period of time.

Incident Response Plan:

Develop a clear, tested incident response plan to manage a ransomware attack, including steps for communicating with donors, stakeholders, and the authorities.

Endpoint Protection:

Use endpoint protection solutions across all devices and servers to detect and prevent malware from infecting and spreading across the systems.



3

Weak Passwords and Technical Vulnerabilities

What is it?

Weak passwords and technical vulnerabilities refer to gaps in your organisation's IT infrastructure that cybercriminals can exploit, such as outdated software, poorly secured networks, and reused or simple passwords. Cybercriminals often use automated tools to exploit these common, "commodity-based threats" and gain access to systems.

Key Insight: In 2024, 62% of charity-related breaches were linked to poor password management or unpatched vulnerabilities.

Why it's a threat:

Many charities rely on legacy systems, which are more vulnerable to attack. Staff and volunteers may also use weak or reused passwords, making it easier for attackers to gain access. Without regular security updates, these systems remain open targets for those looking to steal data or infiltrate networks.

Actionable Steps:

Regular Software Updates:

Implement a patch management strategy to ensure that all software, like operating systems and applications, is kept up to date with the latest security patches.

Strong Password Policies:

Enforce complex password rules and require staff to update passwords regularly. Consider using a password manager to store and generate passwords.

Multi-Factor Authentication (MFA):

Enforce MFA across all accounts to add an additional layer of protection against password-based attacks.

Adopt Cyber Essentials:

A government-backed scheme offering practical steps (like passwords, patching, and firewalls) to protect against common threats.

4

Website and Email Spoofing

What is it?

Website and email spoofing occurs when cybercriminals create fake versions of legitimate websites or impersonate charity email addresses to deceive donors, clients, or stakeholders. This can lead to significant financial loss and damage to the charity's reputation if donors make contributions to fraudulent sites.

Key Insight: Over 400 fake charity websites were taken down in 2024 as part of anti-fraud efforts.

Why it's a threat:

Charities, with their strong public trust, reputations for doing good, and regular donation activity, are highly attractive targets for scammers. Cybercriminals exploit this trust by creating fraudulent websites that closely mimic official charity pages - complete with logos, branding, and donation forms - to trick individuals into handing over money. Email spoofing tactics are used to impersonate staff or leadership, deceiving stakeholders, donors, or suppliers into sharing sensitive information or transferring funds. These attacks can cause significant financial loss, damage reputations, and erode public confidence.

Actionable Steps:

Protect Your Domain:

Implement SPF, DKIM, and DMARC—3 simple but powerful email authentication protocols that work to prevent criminals from sending fake emails using your charity's domain.

Secure Your Website:

Use HTTPS on your charity's website and secure online donation portals to ensure the integrity of financial transactions.

Regular Monitoring:

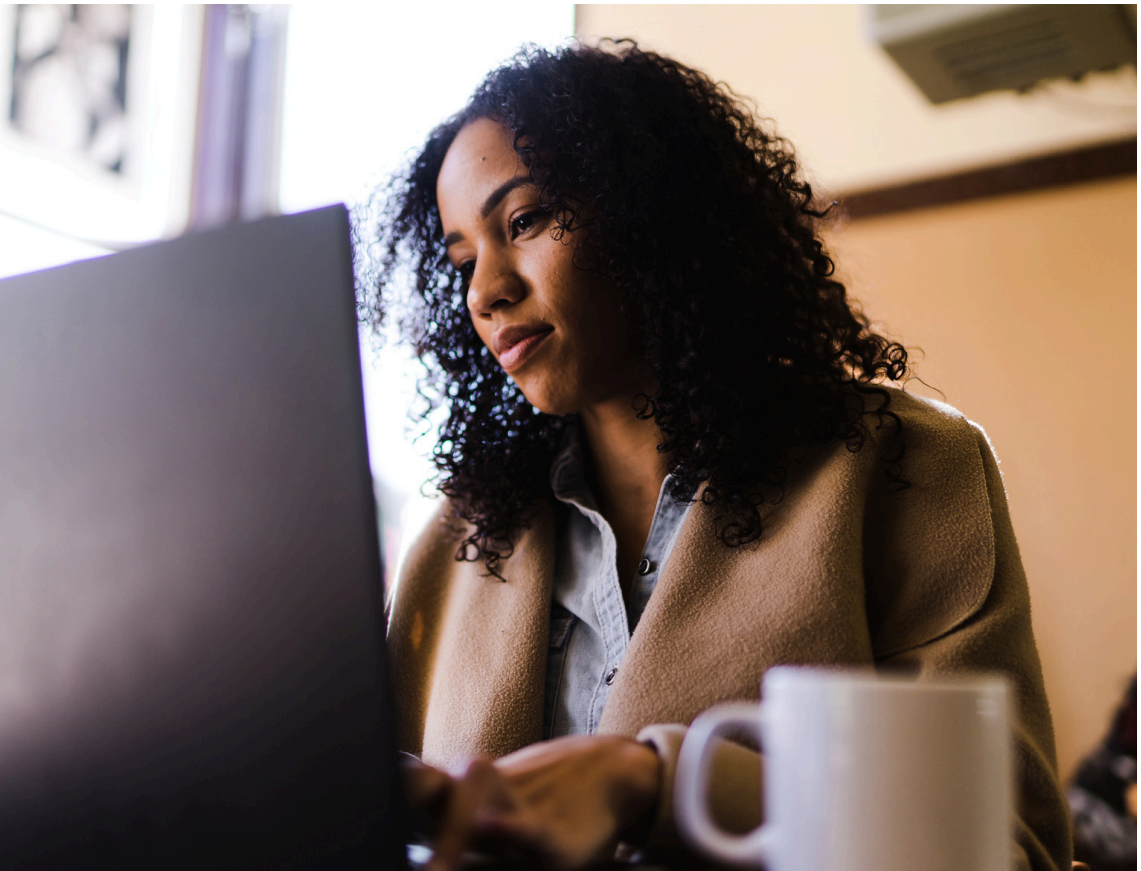
Regularly monitor the web for fraudulent sites or social media profiles impersonating your charity. Use Google Alerts or a third-party monitoring tool to spot potential spoofing.

5

Insider Threats and Human Error

What is it?

Insider threats occur when employees, volunteers, or contractors either accidentally or intentionally cause harm to the organisation's security. This can include mishandling sensitive data, clicking on malicious links, or sharing credentials.



Why it's a threat:

Human error remains one of the biggest causes of security breaches in charities. With staff working across various roles and locations, it's essential that everyone understands the importance of cybersecurity and follows best practices.

Key Insight: In 2024, 24% of charity breaches were due to insider actions, either accidental or malicious.

Cybersecurity Policies :

Develop and implement clear policies around data handling, secure communications, and acceptable device usage. Ensure all staff are trained to follow these policies.

Access Control:

Limit access to sensitive data to only those who need it. Ensure that former employees or volunteers do not have ongoing access to systems after they leave the organisation.

Regular Security Audits:

Conduct internal security audits and encourage staff to report any suspicious activities or security weaknesses they may encounter.

Foster a Security-First Culture:

Encourage a culture where cybersecurity is everyone's responsibility. Regularly remind staff of common threats, promote safe digital habits, and make it easy to report mistakes.

Building Cyber Resilience

How Charities Can Stay Protected

At Wanstor, we believe that technology should empower charities, not burden them. Protecting your organisation doesn't have to be expensive or complex, but it does require planning and proactive management.

We recommend charities take the following actions:

- Secure basic protections through frameworks like Cyber Essentials.
- Implement layered cybersecurity: strong email filters, endpoint protection, regular patching, and secure cloud services.
- Educate and empower everyone in your organisation with accessible cyber training.
- Partner with an IT provider who understands the not-for-profit landscape.

Why choose Wanstor?

At Wanstor, we have over 20 years of experience supporting charities, NGOs, and social enterprises with affordable, secure, and future-ready IT solutions.

We understand your world — limited budgets, compliance pressures, and the need for seamless collaboration — and we design IT strategies that let you focus on your mission while we take care of your technology.

With Wanstor, your charity gains:

- Future-Ready Foundations: Scalable, cloud-first solutions that grow with your mission.
- Stronger Donor Trust: Secure and transparent digital operations to protect your reputation.
- Maximised Efficiency: Less time managing IT, more time driving impact.

Our services include:

- Cloud and Remote Working Solutions: Empower teams with secure access anywhere.
- Cybersecurity and Data Protection: Meet GDPR requirements and protect sensitive information.
- Managed IT and Support: Reduce IT overheads with proactive, affordable service.

We believe in enabling charities through technology, not overwhelming them with it. Our approach combines expert advice, tailored solutions, and ongoing support designed specifically for NFPs.

How Wanstor Supports Charities Like Yours

At Wanstor, we specialise in helping charitable organisations transform their IT. We supported The Fostering Network by resolving a failed Microsoft 365 and server migration, enabling smooth operations for 100+ staff. By streamlining their infrastructure and migrating their CRM to Microsoft Dynamics, we helped them save £80,000 annually on licensing, infrastructure, and support, while future-proofing their IT to support their mission to support fostered children.

Similarly, our work with Jobs 22 showcases our capability in helping not-for-profits scale quickly and efficiently. We deployed 200+ new devices within a tight timeframe, streamlining the onboarding process and eliminating the need for software imaging. This was achieved through Zero Touch deployment services, which reduced time, cost, and logistical challenges, while ensuring a simplified end-user experience. These results reflect Wanstor's ability to deliver robust, scalable, and secure IT solutions, essential for charities looking to enhance operational efficiency and secure their digital environments against evolving cyber threats.

Ready to Protect Your Cause?

Ready to secure your mission from cyber threats?

Visit wanstor.com to speak to our not-for-profit experts today and discover how Wanstor can help your charity stay protected, compliant, and confident in 2025.