

Cyber Security Checklist for Non-Profits



Protecting Your Impact: A Non-Profit's Guide to Cybersecurity

In today's digitally connected world, non-profit organizations must prioritize their IT infrastructure and cybersecurity. The following points highlight the critical reasons why taking cybersecurity seriously and partnering with a Managed Service Provider (MSP) is essential for the success and sustainability of non-profits.

Non-profit organizations are increasingly becoming targets of cyberattacks. According to a 2021 report by the Nonprofit Technology Enterprise Network (NTEN), 43% of surveyed non-profits reported experiencing a cybersecurity incident in the past year.

Data Protection

- ☐ Non-profits often handle sensitive donor information, beneficiary data, and financial records. A cybersecurity breach can lead to the exposure of this confidential information, eroding trust among donors and stakeholders.

Regulatory Compliance

- ☐ Many non-profits in Canada are subject to data protection laws & regulations, such as the Personal Information Protection & Electronic Documents Act (PIPEDA) and the Ontario Personal Health Information Protection Act (PHIPA). Non-compliance can result in significant penalties and legal consequences.

Financial Impact

- ☐ Cyberattacks can be expensive to remediate. Non-profits may struggle to recover financially from the costs associated with data breaches, including legal fees, notification expenses, and potential fines.

Loss of Donor Trust

- ☐ Donors expect their contributions to be used responsibly. A security breach can lead to a loss of trust, potentially resulting in decreased donations and support.

Reputation Damage

- ☐ A cybersecurity incident can tarnish the reputation of a non-profit organization, making it harder to attract donors, volunteers, and partners.

Limited IT Resources

- ☐ Many non-profits have limited IT staff and resources. Partnering with an MSP allows them to access expert cybersecurity services without the need for an in-house team.

Disruption of Operations

- ☐ Cyberattacks, such as ransomware or DDoS attacks, can disrupt the daily operations of a non-profit, affecting their ability to provide services or support their mission.

Scalability

- ☐ As non-profits grow or change, their IT needs evolve. A Managed Service Provider (MSP) can adapt security measures and infrastructure to meet these changing demands.

Proactive Security Measures

- ☐ A Managed Service Provider (MSP) can proactively monitor and defend against cyber threats, helping non-profits stay ahead of evolving security risks.

Disaster Recover & Business Continuity

- ☐ Non-profits need to ensure they can recover quickly from a cyber incident. MSPs often offer robust disaster recovery and business continuity planning to minimize downtime.

Investing in cybersecurity and collaborating with a trusted MSP is not just a strategic choice; it's a commitment to safeguarding your organization's mission, integrity, and the invaluable trust of your supporters and stakeholders.