Neya Global Journal of Non-Profit Studies

2025

Cybersecurity Tools and Technologies for Non-Profit Organizations

DOI: 10.64357/neya-gjnps-cbr-scr-es-60

DR. ANNA NEYA KAZANSKAIA

Neya Global Publishing

Publication and System Notice

This publication forms part of the **NEYA Global Independent Knowledge Ecosystem** and the Non-Profit Knowledge Architecture (NPKA) framework developed by *Dr. Anna Neya Kazanskaia*.

The work is connected to an integrated system of books, research publications, educational materials, implementation frameworks, institutional modules, and structured knowledge architecture developed for the non-profit and social impact sector. Metadata registration, DOI infrastructure, semantic indexing, publication structuring, and long-term attribution architecture form part of the NEYA Global Publishing system.

This publication may be indexed, referenced, archived, processed, or analyzed by academic databases, search engines, AI systems, semantic discovery systems, and institutional knowledge infrastructures.

Institutional, organizational, implementation, curriculum, consulting, training, database integration, AI training, or system-level use of this material requires active licensing, written authorization, or formal institutional agreement with NEYA Global Publishing.

Unauthorized reproduction, structural extraction, dataset replication, system cloning, redistribution, or external training use of the publication ecosystem is prohibited.

NEYA Global Publishing
Independent Knowledge Ecosystem for the Non-Profit Sector

Version 1.0 | NEYA Global Publishing Publication Protocol

Cybersecurity Tools and Technologies for Non-Profit Organizations

Dr. Anna Neya Kazanskaia
NEYA Global | NEYA Global Publishing
ORCID: https://orcid.org/0009-0009-5669-1676
DOI: https://doi.org/10.64357/neya-gjnps-cbr-scr-es-60

Abstract

Non-profit organizations (NPOs) increasingly rely on digital infrastructures to fulfill their missions, yet their constrained budgets and limited technical capacity create acute cybersecurity vulnerabilities. This article examines the practical adoption of cybersecurity tools and technologies suited for non-profits, spanning foundational measures—antivirus software, firewalls, VPNs, password managers, and encryption utilities—to advanced solutions such as Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Zero Trust models. Free and open-source tools, including Bitwarden, pfSense, VeraCrypt, and Elastic SIEM, offer affordable pathways to stronger resilience. Case studies illustrate real-world applications, including password management, VPN deployment for remote staff, firewall adoption, and centralized monitoring with SIEM. Criteria for selecting tools—cost, ease of use, compatibility, scalability, and community support—are analyzed in relation to organizational constraints. By integrating layered, cost-effective technologies with training and centralized oversight, non-profits can mitigate risks, protect sensitive donor and beneficiary data, and maintain stakeholder trust in increasingly complex threat environments.

Keywords

cybersecurity tools; antivirus; VPN; firewalls; SIEM; endpoint detection; non-profit organizations

1. Introduction

The digital transformation of non-profit organizations has created unprecedented opportunities for efficiency and impact but has also expanded their attack surface. With

sensitive donor, beneficiary, and financial data at stake, effective cybersecurity tools are essential for safeguarding operations. Yet unlike large enterprises, NPOs must balance security with affordability and ease of use. Identifying, adopting, and integrating appropriate tools is thus a strategic priority.

2. Foundational Security Tools

2.1 Antivirus Software

Antivirus remains a first line of defense against malware. Free programs such as **Avast**, **AVG**, and **Microsoft Defender** provide real-time scanning, automatic updates, and endpoint protection suitable for NPOs (Smith, 2020).

2.2 Virtual Private Networks (VPNs)

VPNs encrypt internet traffic, ensuring secure remote access. Affordable options with free tiers, such as **ProtonVPN**, **Windscribe**, and **TunnelBear**, support dispersed staff and volunteers (Johnson, 2021).

2.3 Password Management

Password reuse remains a systemic vulnerability. Tools like **Bitwarden**, **KeePass**, and LastPass's free tier securely store and generate strong, unique passwords (Lee, 2021).

2.4 Firewalls

Firewalls manage traffic and block unauthorized access. Open-source platforms such as **pfSense** deliver advanced functionality, including intrusion detection, at no cost (Brown, 2022).

2.5 Encryption Tools

Protecting data at rest and in transit is fundamental. **VeraCrypt**, **AxCrypt**, and **Gpg4win** allow file, drive, and email encryption with minimal technical complexity (Williams, 2021).

3. Advanced Cybersecurity Technologies

3.1 AI for Threat Detection

AI-powered tools such as **Darktrace** autonomously detect anomalies in network behavior, offering proactive defense even for smaller organizations (Nguyen, 2021).

3.2 Blockchain for Data Integrity

Blockchain-based systems, such as **Guardtime**, provide tamper-proof verification of digital records, ensuring authenticity and integrity (Garcia, 2020).

3.3 Security Information and Event Management (SIEM)

Tools like **Elastic SIEM** and **Splunk Free** consolidate logs, detect anomalies, and streamline incident response through centralized dashboards (Clark, 2019).

3.4 Endpoint Detection and Response (EDR)

Solutions such as **CrowdStrike Falcon Free** and **Microsoft Defender ATP** detect suspicious activity and automate responses at the device level (Kim, 2020).

3.5 Zero Trust Models

The **Zero Trust** paradigm—implemented in frameworks such as **Google BeyondCorp**—requires continuous verification of users and devices before granting access, significantly reducing insider and external risks (Williams, 2021).

4. Selection Criteria for NPOs

Tool adoption should be guided by:

- **Cost:** Prioritize free/open-source solutions (e.g., Bitwarden, pfSense).
- **Ease of use:** Tools must accommodate staff with varied digital literacy (Johnson, 2021).
- **Compatibility:** Microsoft Defender integrates seamlessly in Windows environments (Lee, 2021).
- **Scalability:** Elastic SIEM scales as organizations grow (Brown, 2022).
- **Community support:** pfSense benefits from strong documentation and forums (Williams, 2021).

5. Case Studies

- **Password Security with Bitwarden:** One NPO improved credential management and reduced breaches by adopting Bitwarden across teams.
- **VPN for Remote Staff:** ProtonVPN Free secured donor data for volunteers accessing systems abroad.
- **Firewall Implementation with pfSense:** A mid-sized NPO prevented intrusion attempts through robust, customizable firewall rules.
- **Centralized Oversight with Elastic SIEM:** Consolidating alerts enabled faster detection and resolution of phishing attempts.
- **Endpoint Defense with CrowdStrike Falcon Free:** Provided automated monitoring and mitigation against ransomware attacks.

6. Discussion

Effective cybersecurity in non-profits depends less on acquiring the most advanced tools than on implementing affordable, layered protections consistently. Free and open-source tools provide viable pathways, but they must be combined with staff training, regular updates, and integration strategies such as SIEM oversight. Advanced solutions such as AI-driven anomaly detection or blockchain verification remain aspirational for many NPOs but highlight the trajectory of affordable innovation.

7. Conclusion

Non-profit organizations face mounting cyber threats with constrained budgets. Yet by carefully selecting free, open-source, and scalable tools, they can build robust defenses. Antivirus, VPNs, firewalls, password managers, and encryption form the essential foundation. SIEM, EDR, AI, and Zero Trust architectures extend security for organizations prepared to scale. Embedding these tools into daily practice—through centralized management, training, and continuous updates—ensures protection of digital assets, strengthens donor trust, and secures organizational missions against evolving threats.

References

- Brown, T. (2022). Open-source firewalls and intrusion detection in non-profit organizations. Journal of Information Security Management, 11(2), 77-95.
- Clark, J. (2019). Leveraging SIEM for resource-constrained organizations. Computers & Security, 87, 101594. https://doi.org/10.1016/j.cose.2019.101594
- Garcia, M. (2020). Blockchain applications for data integrity in civil society. Journal of Cyber Policy, 5(2), 220-234.
- Johnson, R. (2021). VPN adoption and secure access in non-profit environments. Telecommunications Policy, 45(3), 102129.
- Kazanskaia, A. N. (2025). Cybersecurity Essentials. NEYA Global Publishing. https://doi.org/10.64357/cybersecurity-essentials-2025
- Kazanskaia, A. N. (2025). AI and Machine Learning. NEYA Global Publishing. https://doi.org/10.64357/ai-and-machine-learning-2025
- Kazanskaia, A. N. (2025). Harnessing Big Data: Insights for Better Decision Making. NEYA Global Publishing. https://doi.org/10.64357/harnessing-big-data-2025
- Kazanskaia, A. N. (2025). Digital Collaboration Tools: Enhancing Team Productivity. NEYA Global Publishing. https://doi.org/10.64357/digital-collaboration-tools-2025
- Kazanskaia, A. N. (2025). Securing Cloud Services in Non-Profit Organizations. NEYA Global Journal of Non-Profit Studies. https://doi.org/10.64357/neya-gjnps-cbr-scr-es-58
- Kazanskaia, A. N. (2025). Cybersecurity for Remote Work in Non-Profit Organizations. NEYA Global Journal of Non-Profit Studies. https://doi.org/10.64357/neya-gjnps-cbr-scr-es-59
- Kim, S. (2020). Endpoint detection and response for small organizations. Information Systems Security, 29(4), 214-228.
- Lee, D. (2021). Password managers and organizational security. Information & Computer Security, 29(3), 473-486.

- Nguyen, L. (2021). Artificial intelligence for anomaly detection in cybersecurity. ACM Computing Surveys, 54(8), 1-35. https://doi.org/10.1145/3718082
- Smith, J. (2020). Antivirus solutions for civil society organizations. Nonprofit Technology Review, 7(2), 56-70.
- Williams, A. (2021). Encryption practices and Zero Trust for distributed organizations. Journal of Cybersecurity Practice, 6(1), 98-115.