Microsoft

Strengthen your nonprofit's digital security: Protect your data and build trust

Introduction: Why security can’t wait at your nonprofit

As a busy nonprofit, your focus is your mission. Whether you’re supporting humanitarian efforts, promoting animal welfare, fighting climate change, or working to improve health equity, you are focused squarely on providing critical services and support to your community. Your organization is deeply engaged in delivering programs, coordinating and managing volunteers, processing donations, supporting fundraising efforts, and myriad other activities.

With all these priorities on your plate, security might seem like something that can wait. Unfortunately, it can’t. Security is more critical than ever for nonprofits.

In a recent survey, 21 percent of North American foundations reported a security breach in the preceding two years, with ransomware attacks as the largest single cause (38 percent).[i]

Based on analysis from the Microsoft Digital Security Unit, nonprofits (NGOs) are the most common targets of nation-state actors detected by Microsoft. NGOs received 23 percent of all notifications from 2018 to 2021. We define NGOs to include various nonprofit organizations including human rights organizations, charities, political parties, religious organizations, and think tanks—the leading targets in the sector. These organizations are attractive targets for nation-state actors because they often store information related to political views, and loyalty to parties or individual political candidates.

In 2021, Pegasus spyware was discovered carrying out surveillance on human rights activists, journalists, and public officials by accessing calls, messages, emails, contacts, media, microphones, and cameras.[ii]

[i] 2018 State of Philanthropy Tech | Technology Association of Grantmakers
[ii] Pegasus scandal: Are we all becoming unknowing spies? | BBC News

With more employees working remotely, the risk of a breach is increasing. Hybrid and remote work require access to organizational data, which creates new potential openings for attackers. In fact, in one survey, 56 percent of senior IT technicians said they believe their employees have picked up bad security habits while working from home, and 39 percent of employees admitted to using less-thorough security practices at home compared to in the office.[iii] It isn't just external attackers causing trouble—insider threats are also a concern, whether intentional or accidental.

Breaches are costly—and not just financially

It's easy to see why all this is happening. Nonprofits collect and store a vast array of data about their constituents. Much of this data includes sensitive information such as names, birthdates, social security numbers, credit card and billing details, and driver's license and state ID card data.

Securing this data is essential to keeping your organization healthy. For organizations that rely on donations, your reputation is critical to retaining the confidence of your stakeholders. Protecting that trust is—quite literally—currency.

Failing to secure your data can have other financial consequences. The average cost of a security incident in the nonprofit sector is $77,000.[iv] The current average cost of a data breach overall is $4.24 million, 10 percent higher than the average cost in 2019.[v] Ransomware attackers stole $350 million in 2020, a 311 percent increase from 2019.[vi] In addition to the cost of the actual breach, exposing sensitive data can have compliance repercussions that may include fines, depending on local governing laws.

$77K	$4.24M	$350M
Average cost of a security incident in the nonprofit sector	Average cost of a data breach overall	Ransomware attackers stole in 2020

[iii] Why remote working leaves us vulnerable to cyber-attacks | BBC News

[iv] Cyber Claims 2020 Report | Net Diligence

[v] Cost of a Data Breach Report 2021 | IBM

[vi] RTF Report: Combatting Ransomware | Institute for Security and Technology

Overcoming the challenges to prioritizing security

Despite these concerns, many nonprofits struggle to make security a priority. In its *2021 Security Guide for Nonprofit Organizations*, TCA SynerTech reports that, although cybercriminals attempt to access government and nonprofit databases every 39 seconds, up to 70 percent of charity networks lack a comprehensive vulnerability assessment to determine risk.[vii]

According to a report from NTEN,[viii] the reasons nonprofits aren't prioritizing security include:

- **Lack of funding**
- **Competing priorities**
- **Lack of executive buy-in**
- **Weak overall IT infrastructure**
- **Lack of knowledge**
- **Large volunteer and contingent staff dependencies**

However, with the right focus and commitment, these challenges can be overcome. Although a lack of security can have serious consequences, improving your security posture doesn't have to be expensive or complex. Microsoft seeks to simplify security for nonprofits while providing relevant, affordable, and innovative technology, so you can focus on your mission. Protecting your organization isn't something you'll do once then move on. Security is a journey, and every organization is at a different stage.

In this e-book, we introduce five key steps you can take to improve security at your nonprofit, with tips for organizations that are just starting on their security journey as well as for those further down the path.

[vii] 2021 Security Guide for Nonprofit Organizations | tca SynerTech
[viii] State of Nonprofit Cybersecurity | NTEN Report

Gain buy-in from leadership and your board

Increasing your focus on security requires buy-in from all members of your organization, especially board members and executives. To do this, you should find security champions inside the organization who can help lead the conversation.

What if your organization doesn't have a CIO or other technology leader? Whatever your role, you can champion security and start driving the conversation around it. You might take the initiative by:

- Creating a summary of both general and nonprofit-specific security risks and challenges to share with leadership and the board
- Leading a Q&A session on security risks and concerns
- Coordinating and tracking security issues regularly while communicating with internal stakeholders
- Organizing a security special task force composed of technology leaders
- Ensure security is part of the board of directors' regular agenda

> We're just like any other company in need of protecting our assets and employees. Beyond our focus to secure business assets and employee data in the most cost-effective manner possible, our team considers protection of our residents' sensitive data and privacy to be core to our mission and beliefs.
>
> **– Tom Maynard,**
> **Vice President of Strategic Initiatives**
> **and Solution Delivery, Mercy Housing**

Build security awareness and skills throughout your team

Security is more than just a technology issue. A new report revealed that 85 percent of data breaches involved a human element, whether it was intentional or not.[ix]

A potentially devastating data breach can occur with a single mouse click. Because every organization is only as strong as its weakest link, staff and volunteers need the education and skills to learn how to identify and respond to threats. This training requires security awareness and skills across your entire team. Here are some suggestions on how to increase awareness:

Establish a security plan. By creating a formal plan, as well as embedding a workplace culture of best practices and safe business processes, you will help employees throughout your organization build and maintain trust with all constituents, including program participants, donors, and volunteers. Ensuring everyone is aware of this plan is especially important in today's workplace since employees are increasingly using their personal devices to work. The Microsoft free security assessment is a great place to start building your plan

Schedule ongoing, regular training. Consider scheduling regular security training for all employees, throughout the year, to ensure they have the knowledge and tools to identify threats, such as malware, phishing, and ransomware. Training should also show employees how to report suspected security incidents and update workers on specific, looming threats. Consider making this training an onboarding requirement for new staff members and volunteers as well as a refresher training for current employees.

Implement security testing. Many organizations send out regular phishing attacks to test employees' aptitude at identifying bogus emails. Whether employees pass or not, it can be used as an educational opportunity across the organization and serve as a consistent reminder to stay vigilant.

[ix] Security Essentials for Philanthropy | Technology Affinity Group

02

Security training initiatives

Microsoft is launching a proactive strategy to train 25 million people by 2025 to help meet the need for half a million security professionals in the United States. This strategy involves initiatives that will help existing technology professionals reskill or upskill into security roles, and partner with community colleges to help attract and financially support students pursuing security-related degrees.

Microsoft is also furthering this commitment with the Security Program for Nonprofits, as part of a suite of nonprofit offers. You can use the Security Program for Nonprofits to help protect your organization with a comprehensive set of security offerings that assess organizational risk, provide proactive monitoring and notifications, and give training.

> Security is everything in 2021 and beyond. The future is bright for [our organization], and that is partly because Microsoft is empowering us to save money while improving collaboration, strengthening our hosting options, and hardening our infrastructure against external threats.
>
> **– Stephen Pearl,**
> **Executive Director of**
> **Technology Operations, ECRI**

Free resources for building security awareness and skills

For non-IT employees

- Intro to cybersecurity
- Protect yourself from online scams and attacks
- Work from home more securely
- Be safer over wireless connections

For IT administrators

- Security collection on Microsoft Learn
- Security Skilling Hub
- Security Virtual Training Days
- Microsoft 365 Administrator’s Security Toolkit: The Fundamentals

Create and document security policies

Having clear policies in place, and making sure everybody understands and implements those policies, helps reduce the likelihood and severity of cyberattacks and breaches.

When it comes to creating and documenting security policies, consider focusing on the following five areas:

1

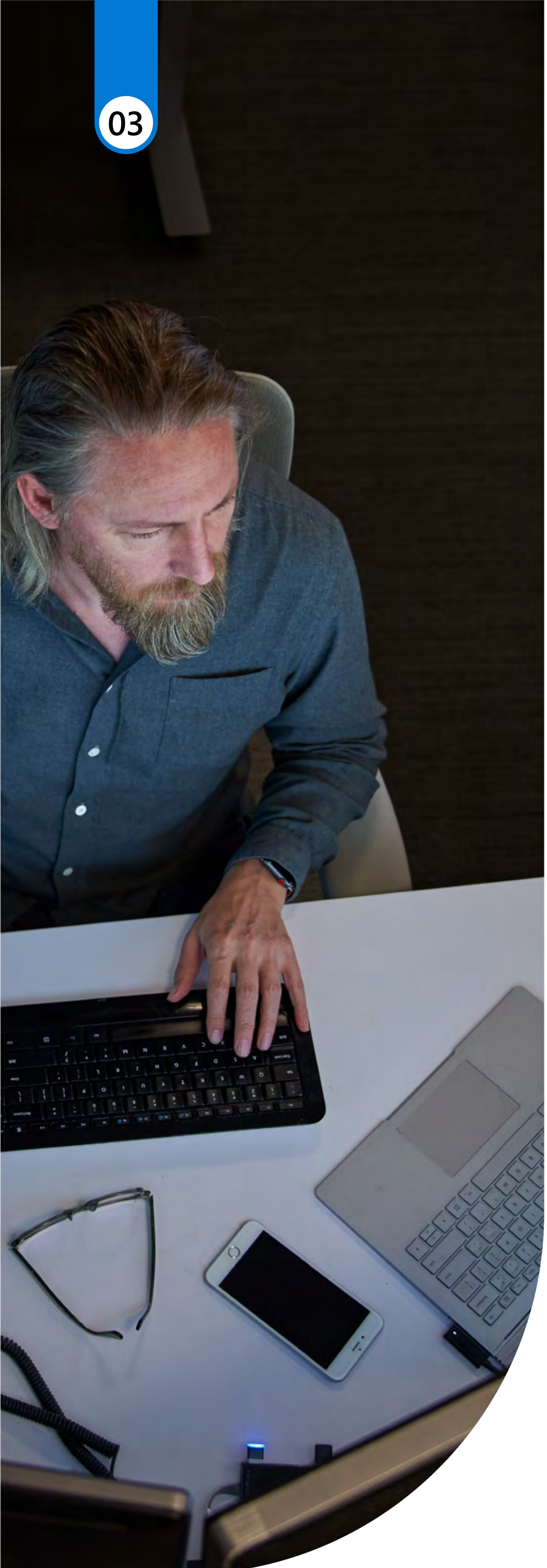
Credentials and passwords. Strong, unique, complex passwords are the easiest and first line of defense for the systems and data in your organization. Multi-factor authentication (MFA) ensures a secondary layer of protection by having users provide additional identity verification, like scanning a fingerprint or entering a code received by phone, to further reduce the risk of cyberattacks. Change passwords frequently, as volunteers and employees with access to your systems may join and leave the organization often. It’s also important to remove any inactive accounts, including those of former employees and volunteers. Additionally, consider using password managers, which provide secure, unique passwords for a variety of applications and log in users automatically.

2

Data backup. Backing up your critical data is an essential part of any security policy. By creating regular backups of all data, you can reduce the risk of data loss from a cyberattack or natural disaster. Ensure your employees also know how to use backup software during business disruption.

3

Data sharing. With more employees working and collaborating remotely, it is more challenging to control how and where data is shared. Using virtual private networks (VPNs) for remote network access enables stronger security for remote users. You could also consider restricting usage of personal mobile devices, allowing access only to specific applications that are required for work. Multi-factor authentication (MFA), rights management, and cloud-based storage are also effective tools to limit sharing.



4

Device configuration. You can be proactive about device security instead of worrying about the risk that comes with mobile devices throughout your organization. Configure devices by using endpoint protection, which monitors devices to identify and block threats to avoid network exposure. You should also regularly update your hardware and software to ensure all devices on your network are running with the most current security.

5

Cyberattack response. If a security incident is detected, a quick response can help mitigate the damage. Your response effort should include a formal plan that coordinates response activities between internal stakeholders (i.e., legal, IT, HR) and external stakeholders (i.e., donors, insurance companies, law enforcement). You’ll also need to analyze what went wrong, including any vulnerabilities that caused the incident, so you can reduce the risk of another occurrence in the future. By responding quickly and decisively, you can contain the impact

04

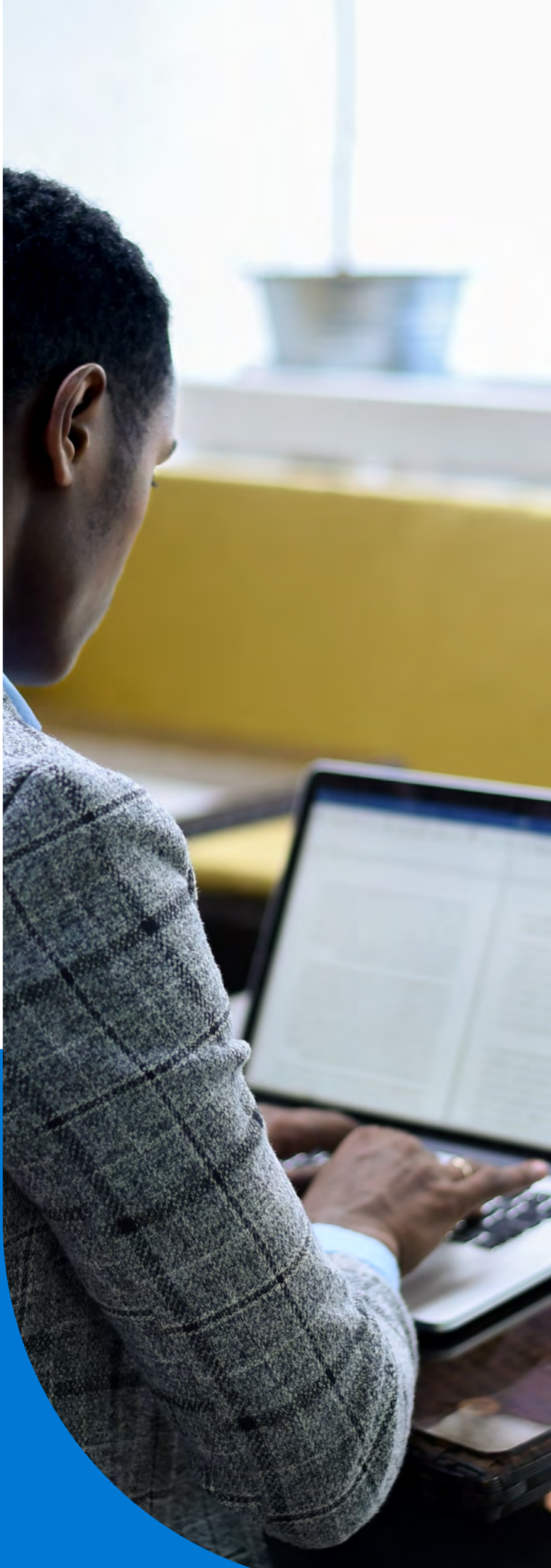
Choose and use technology designed for the way people work

Like most organizations today, nonprofits are going through a fundamental change in the way their staff members and volunteers work. Hybrid and remote-work environments are growing in popularity, and employees and donors alike are increasingly reliant on digital technologies. Because of the move to remote and hybrid work, there are changing security requirements, including:

- **Cloud and mobile apps.** People work using phones, tablets, and browsers as well as traditional PCs. Visibility and control over the apps people use at work requires security solutions built for this new environment.
- **Device proliferation.** IT personnel must spend more time managing and securing these connected network devices.

Technology designed for working in the office might not be as effective in securing hybrid or remote worksites. Security should not get in the way of employee productivity or privacy.

> ”
>
> Whether it’s a program participant or a donor, an employee or volunteer, PII [or personally identifiable information] abounds. How we handle that information is of paramount concern. Communicating through a single platform provides peace of mind when it comes to security. We no longer have to support all different message platforms or worry people are using unsupported platforms.
>
> **– Joff Williams, Director of Technology Projects, Mercy Ships**



To choose the right security technology for the way your people work, consider the following steps:

Evaluate the tools you are currently using. Take advantage of features you aren't using to improve security without an additional cost. Look for solutions where you can make strategic investments for your security where it's needed. You can also check your eligibility for a free security assessment from Microsoft.

Secure the hybrid environment. Protect users and their data wherever your teams work with coordinated defense capabilities across all cloud environments and platforms. These capabilities include:

- *Cloud and mobile app security.* By streamlining cloud-access security through natively integrated tools, you can gain better visibility into cloud apps and services using analytics.
- *Mobile device management.* You can protect and secure your organization's data from different devices by implementing device management technologies.
- *Multi-cloud and hybrid environments.* Using technology that centrally manages different operating systems and databases, you can create centralized visibility while delegating access and managing security policies through role-based access control.

Integrate security tools. Prevent, detect, and respond to attacks while simplifying security by using:

- *Security scoring and benchmarking.* With scoring and benchmarking, you can clearly measure your security posture to determine how to improve your security and better protect your organization.

- *Unified tools and administration across solutions.* Implementing a unified, infrastructure security management system can help you strengthen security while providing advanced threat protection across hybrid-cloud workloads and in physical data centers.

Deliver rapid, intelligent results. Find and resolve critical threats faster using the power of AI and analytics to enable:

- *Advanced threat protection.* You can rely on new technologies to prevent, detect, and respond to threats across identities, endpoints, applications, and cloud platforms.
- *Automated remediation.* Using a playbook that can run manually or automatically to specific alerts or incidents, you can automate and orchestrate your threat response.

> Many nonprofits think they will not get attacked because they're doing good work, which of course makes no difference to a bad person with a set of email addresses. Nonprofits need the same security as a large business!
>
> **– David Krumlauf, Chief Technologist,**
> **Pierce Family Foundation**

05

Collaborate with experienced experts

By working closely with a partner organization that specializes in security strategies and solutions, you can focus on your mission while getting ahead of today's complex threat landscape.

Microsoft is committed to helping nonprofits succeed by providing training, resources, and discounts. Our end-to-end security approach is built for today's world of hybrid and remote work, helping protect data and privacy across clouds, apps, data, and devices. Microsoft offers a partner ecosystem with industry-specific solutions to address your most urgent business and technology challenges. For more information, visit [Microsoft 365 Nonprofit Solutions.]

[Find a partner.]

> Microsoft Enterprise Mobility + Security helps us address one of our highest priorities in IT at Save the Children: data protection. This tool means we can ensure all personal devices used for work meet our security policy standards and, most importantly, safeguard children.
>
> – Cristian Alfaro,
> Enterprise Technology Manager,
> Save the Children

Microsoft security solutions for nonprofits

Microsoft provides the following comprehensive security technologies to help protect your nonprofit's critical data:

Microsoft 365.
Through the subscription-based Microsoft 365 suite of apps, your employees, volunteers, and donors can stay connected through popular applications such as Microsoft Word, Outlook, and Excel.

Microsoft Azure Sentinel.
This solution is a scalable, cloud-based security information event management (SIEM) and security-orchestration, automated-response solution. It enables you to collect data at scale—across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds—and detect and respond faster to multi-stage attacks.

Microsoft Defender for Office 365 Plan 2.
This updated version includes best-in-class threat investigation and response tools that help you anticipate, understand, and prevent malicious attacks.

Microsoft Defender for Endpoint.
Microsoft Defender for Endpoint is an endpoint security platform that helps you prevent, detect, investigate, and respond to threats. You can focus on your mission while experiencing preventative protection, post-breach detection, and automated investigation.

Microsoft 365 Defender.
This solution relies on the Microsoft 365 security portfolio to automatically analyze threat data across domains to build a complete picture of a cyberattack in a single dashboard.

Microsoft Azure Security Center.
This solution is a unified infrastructure security management system designed to strengthen the security posture of your Azure environment, enabling you to visualize your security state through Secure Score recommendations.

Next steps

Register as a nonprofit to get Microsoft grants and discounts. Nonprofit grants include a $3,500 annual credit for Azure and a Microsoft 365 Business Premium grant for up to 10 users. We also provide discounts of 75 percent on most Microsoft 365 products.

Take advantage of the Security Program for Nonprofits. This offer for eligible nonprofits provides end-to-end security through several solutions:

- Microsoft AccountGuard for Nonprofits proactively monitors for nation-state attacks and notifies organizations if their organizational or associated personal accounts have been compromised. Sign up through your Nonprofit Hub.
- A concierge service to proactively engage your organization on the security journey.
- Security assessments to help organizations understand their risk profile and prioritize an action plan aligned to their architecture and risk vectors.
- Funding and deployment assistance to support security deployments and augment the cost.
- Nonprofit security thought leadership and recommendations to help organizations mitigate risk considering nonprofit threat trends.

Get access to security training. Visit the Microsoft digital skills training site for information on current training options available to nonprofits.

Learn more about Microsoft Cloud for Nonprofits