Cybersecurity Essentials for Nonprofits

Second Edition
April 2024

Information Technology
Outreach and Education Program

Questions about this guide or TechOE program services contact:

Kai Dailey Program Manager
Information Technology Outreach and Education Program
501 Commons
kai@501commons.org

Cybersecurity Essentials for Nonprofits

The following security measures are suitable for all organization sizes that use cloud services. These essentials can be implemented for the cost of staff time only or in some cases for a low subscription fee from vendors who sell at nonprofit discounts.

By implementing these cybersecurity essentials and fostering a culture of security within your organization, you can significantly reduce the risk of cyber threats and protect your organization's valuable assets and reputation. Cybersecurity is a shared responsibility between all members of your organization and the software providers you use. It requires vigilance and proactive measures to stay ahead of emerging threats.

❑ *Multi-Factor Authentication (MFA)*

Implementing MFA adds an extra layer of security by requiring employees to verify their identity through multiple action steps, such as a password and a unique code sent to their mobile device or email account. This simple step can significantly reduce the risk of unauthorized access to your organization's accounts and systems. If you are prompted to set up this option, consider enabling it, particularly for data sensitive accounts. If you store sensitive data online with a vendor that does not offer this feature, reevaluate the vendor’s data safety capabilities and consider moving your data to a safer location.

❑ *Phishing Email Training*

This security measure is essential for combating the daily threat of phishing attacks. Regular training (monthly) improves employees’ ability to (1) identify suspicious emails, (2) avoid engaging with a phishing email, and (3) report potential threats promptly. With continued training most employees become adept at spotting sophisticated phishing attempts. This strengthens the organization's overall cybersecurity posture. Between 85% to 90% of cyber-attacks, particularly those involving stolen IDs and passwords, begin with a successful phishing email. Common methods used for phishing email training include interactive quizzes, videos, and exercises that simulate real-world phishing scenarios.

❑ *Separate Admin and User Accounts*

For account administrators, it is crucial to separate their use of administrative accounts from their regular user accounts. This helps prevent potential security breaches that could occur if an admin's user credentials are compromised. Executive leadership should always use separate accounts because they are prime targets of hackers. This requires having two accounts, one for general user activities, and one for administrative tasks. Administrators should not use their admin accounts for general use.

❑ *Formalize Cloud Account Administrative Role*

Describe and document security responsibilities for account administrators. Designate a primary account owner responsible for data privacy and account security. Ensure both account owners and admins are trained on the cloud software's security functions and options, and that they understand that security is a shared responsibility with the vendor. They should know where the vendor's responsibilities end and theirs begin. Create a schedule of security activities to be performed regularly.

Do not assume that large cloud software vendors are 100% secure. If they are breached, you are still responsible to the individuals whose data you stored there and to any applicable regulatory entities. Vendors generally take responsibility for the security of their own servers and software but do not have responsibility for incidents that occur because an account or web-facing form, used for example to collect newsletter signups, was compromised and as a result data loss or theft occurred.

❑ *Device Encryption*

Ensure that all devices, organization owned and personal, that are used by employees for business purposes, such as computers, laptops, and mobile devices, are encrypted to protect data in case of loss or theft. Windows and Mac operating systems include an encryption option that must be enabled. Apple devices and newer Android phones and tablets are encrypted by default if you set up a lock screen. For older Android devices, review and update settings, as needed. Encrypting data on computers will generate encryption keys that you can use if the device password is lost. Create and document procedures to protect keys from unauthorized access, modification, or loss. You can store them in a spreadsheet and encrypt them with another key or a passphrase and store in a separate location. Backup your keys regularly. Keep them offline or in a trusted cloud service.

❑ *Backups*

Regularly backing up important files and data is essential to prevent data loss and facilitate recovery in the event of a security incident. Determine what data and systems are critical to protect (including websites!). Document and schedule backup procedures. Test restoring from backup before a crisis. This is especially true for databases that may also need metadata restoration. Restoring a database can be time consuming. If you will rely on a vendor for assistance, you may be required to wait in a queue before your services are put back. Prepare a workaround for critical business processes that employees can use while data services are unavailable.

❑ *Keep a List of All Cloud Accounts*

Know what cloud vendors are being used, who is using them, and what kind of data is being used and stored. For each cloud vendor, keep a log of accounts and permissions for each. This responsibility can be assigned to software account owners or administrators. A complete list of cloud accounts supports regular evaluation of cloud vendors to avoid paying for redundant subscriptions or placing sensitive data on risky platforms. An updated list and procedure for removing account access for separating employees, removes the likelihood that a hacker will gain access through a forgotten or unwatched account. Use a spreadsheet to inventory all cloud accounts, include information you may need to verify ownership with vendor support, in case the account is hacked, and you lose access.

❑ *Password Protection for Wi-Fi*

Secure your organization's Wi-Fi network with a strong password to prevent unauthorized access by implementing network encryption protocols such as WPA2. Remember to change the default Wi-Fi router password. If you are using a business internet service, create separate guest Wi-Fi access.

❑ *Malware Protection*

Install and regularly update antivirus and anti-malware software on all devices to detect and remove malicious software that could compromise your systems and data.

❑ *Software Updates and Patching*

Keep all software and operating systems up to date with the latest security patches. Vulnerabilities in outdated software can be exploited by cyber attackers to gain unauthorized access to systems. Because vender announcements that software updates are available also signals hackers about vulnerabilities in the older software versions, don’t wait to update!

❑ *Threat intelligence*

Know what software and cloud services are in use and be on the lookout for information about new security vulnerabilities. These surface regularly, so vigilance is important. This responsibility can be assigned to software account owners or administrators. Subscribe to vendor alerts, Common Vulnerabilities and Exposure (CVE) notices from Cybersecurity and Infrastructure Security Agency (CISA), and general newsletters on cybersecurity.

❑ *Cybersecurity Awareness Training*

Educate your staff and volunteers about cybersecurity best practices and the importance of maintaining strong security hygiene. Training sessions can help raise awareness of common threats and empower employees to recognize and respond to potential security risks.

501 Commons advocates for a whole organization approach to awareness. *Security awareness for a small organization works best when security activities, governance, and training are combined into a single program with shared responsibilities distributed among staff members.* All staff members should own a security activity.

❑ *Email Filtering*

Implement email filtering solutions to block spam, phishing attempts, and malicious attachments. Email is a primary method to launch cyber-attacks, so filtering incoming messages can help prevent your organization from falling victim to email-based threats. Educate employees on how to report suspicious emails that get through the filter, so settings can be updated by the administrator. If your email filtering/anti-phishing software offers labeling to alert employees to external or unsafe emails, enable this feature. Labels have been found to be more effective at preventing phishing email engagement than training.

❑ *Strong Passwords*

Encourage the use of long, complex passwords that are difficult for cyber attackers to guess or crack. Consider implementing password policies that require regular password changes and prohibit the reuse of old passwords. The minimum standard as of 2024 is 16-character passphrases. Avoid common passwords that hackers have likely already stolen and decoded.

❑ *Password Manager Software*

Use password management software to securely store and manage passwords for your organization's accounts. These strongly encrypted tools reduce the risk of password-related security incidents. Versions that include a browser extension make it convenient for employees to log into web accounts. Password management software also enables secure password sharing and centrally managed vaults that can be revoked when an employee separates from the organization. Use a password manager instead of storing passwords in a browser. While convenient, browser storage poses significant security risks because browsers are not as secure. If a web browser is compromised, all stored passwords can be exposed.

❑ *Log Out of Cloud Accounts*

Ask employees to log out of cloud accounts and online services after each work session to prevent unauthorized access if their browser is compromised. Disable "stay logged in" or set to the shortest duration, if possible. Use a password manager software with a browser extension to automatically fill in credentials to ease the burden created by frequently entering passwords. Proposed security improvements by major vendors are being developed. However, until more secure browser and cloud service authentication standards are implemented widely, staying logged into cloud accounts when they are not in use is not recommended.

❑ *Clearing Browser Cache*

Encourage employees to clear their browser cache and cookies regularly to remove traces of their online activity and minimize the risk of unauthorized access to sensitive information.

Recommended intervals are (1) upon closing the browser, (2) at the end of an online work session, or (3) daily. If you are logging out of cloud accounts and clearing cache daily, this reduces the risk of account access via session token theft.

❑ *Integrity - Culture of Security*

Foster a culture of security within your organization by emphasizing the importance of permissions management, file labeling, and organization with confidentiality in mind. Regularly review access permissions and file sharing practices to minimize the risk of unauthorized access to sensitive data.

❑ *Governance*

Develop clear written policies and procedures for handling sensitive data, including guidelines for using USB drives, encrypting email communications, and securely managing cloud services. Regularly review and update these policies to ensure they remain effective in addressing evolving cybersecurity threats.

Classify your data (suggested categories: restricted, confidential, internal, public) and provide instructions on how documents and data in each category should be handled. For example, restricted data should not be attached to an unencrypted email and sent outside of the organization. If you have access to file labeling features in the document storage software that you use, you can tag restricted or confidential files to be more easily recognized by employees. If your document storage does not offer this feature, investigate optional plug ins to provide this effective method of data loss prevention.

❑ *Least Privilege*

Use the principle of least privilege for programs, data, or processes to ensure access is granted to only those employees who need it to complete their work. This reduces the risk of unauthorized access, limits the impact of cyberattacks, and enhances system security. Review permissions regularly and remove unnecessary access. Train your employees to voluntarily relinquish access when it is no longer needed, for example after the completion of a project or a change in position. Privileges should be viewed like communal keys that are checked out and returned when the work is done. Keeping unnecessary access permissions is like leaving the file room door open and unlocked after business hours.

❑ *Privacy Compliance Regulations*

Develop a list of compliance responsibilities and keep it updated. Subscribe to Google Alerts to get information on news stories on a regulation or court rulings that may impact how a regulation is interpreted or implemented. There is no central location for all compliance information. Federal, state, and professional organization websites and newsletters tend to provide the most reliable information. Make your compliance list accessible to everyone in your organization, include breach notification requirements and consequences of failing to meet compliance requirements.

❑ *Virtual Private Networks (VPNs)*

VPNs are used to create a secure, encrypted connection between a device and a remote network. VPNs allow employees to access restricted websites and resources securely, even over public internet connections. They hide the employee's true IP address and encrypt all traffic, providing privacy and security. VPNs are commonly used by remote workers, travelers, and anyone who needs to access sensitive data over the internet.

❑ *Firewalls*

Firewalls are essential security tools that can be implemented as both hardware devices and software applications. Their primary function is to protect networks by inspecting incoming and outgoing traffic, and then blocking any traffic that fails to meet predefined security rules. Firewalls are essential for protecting business and home devices and networks from cyber threats like malware, hacking attempts, and unauthorized access. Firewalls also protect the internet of things (IoT) connected to your network, such as doorbell cams, Wi-Fi enabled kitchen appliances, smart speakers, intelligent lighting, and door locks.

Home Wi-Fi Security for Remote Work. The internet router supplied by your cable company has a built-in firewall that blocks incoming traffic not initiated by devices on the network. However, it does not safeguard against traffic designed to disrupt, damage, or illegally access a computer system or network. Windows, Mac, and iOS devices come preloaded with a basic software firewall to filter out or block malicious traffic to protect an individual computer from being compromised or infected. Android devices do not come with firewalls or antivirus software and must be installed separately.

When you regularly allow operating system updates for Windows, Mac, and iOS to be installed, it keeps your firewall up to date, so it knows what traffic to block based on the latest threats. Check operating system settings to confirm this feature has been enabled. It is recommended that you also purchase third-party software firewalls, if you have a lot of devices sharing your Wi-Fi network, and you use it for both remote work and personal use. Third-party firewalls provide more advanced security capabilities, such as intrusion detection, application-level filtering, and real-time threat monitoring for each device that can detect and block more sophisticated attacks.

Firewall software cannot protect against malware that has already infected a computer or system, while antivirus software cannot prevent unauthorized network access attempts. Consider vendors that combine both services for a single subscription price.

Note: If your organization maintains on-premises servers, switches, hardware firewalls, or a complex network of Wi-Fi access points, this essentials list does not address technical security oversight required of hardware and sophisticated networked environments. It focuses primarily on employee behaviors. Measures such as hardware firewalls and VPNs for business office, may require substantial investment to install and maintain.