nten

Website Security for Nonprofits

2023 GUIDE

AN NTEN GUIDE
by Jason Shim

What's Inside

Introduction

WHY NONPROFIT WEBSITE SECURITY IS IMPORTANT

A website is an essential part of a nonprofit's online presence. It's where people can learn more about your mission and how to engage, including accessing services, volunteering, donating, and contacting your organization. However, it can be one of the most vulnerable systems for an organization if it is not secured correctly, creating vulnerabilities and harming those engaging with you, your staff, and the organization.

An analysis of public data from NTEN's Tech Accelerate, a free online assessment tool that evaluates and benchmarks nonprofit technology use and policies, indicates that "security continues to need investment."[1] This analysis is based on nonprofits who have taken a comprehensive assessment of technology use, and the results indicate that the lowest overall average scores across all budgets and staff sizes are around the topic of security.

While nearly all organizations, including businesses, may face similar technical issues regarding website security, nonprofits often need help with specific challenges regarding the audiences they serve, the resourcing available, and the constraints that may present. Many nonprofits work with donation systems that may be integrated with their website and process donor information, as well as online systems for program and service delivery that may handle volunteer and constituent data. Administrative access to these systems within organizations may include access by staff, volunteers, and consultants. Nonprofits also often need help with resourcing and securing funding for ongoing operations. Data security, privacy, and cyber risk awareness may be limited from technical and compliance perspectives. For many organizations, "[i]n the absence of sustained, sufficient funding for cybersecurity, organizations leverage free software, donated hardware, volunteer IT support, and, when needed, consultant security services to fill the gap."[2]

Much of the work nonprofits do is based on trust, whether in community services or the relationships built with donors. For a nonprofit to function effectively, the risks associated with website security must be addressed to maintain trust and credibility with your online audiences and ensure the continuity of your organization's operations, services, and, ultimately, your mission.

1 https://www.nten.org/accelerate/data

2 https://ccndr.ca/wp-content/uploads/2023/02/Building-the-Cybersecurity-and-Resilience-of-Canada.pdf

CONSEQUENCES OF LAX SECURITY

When website security is not adequately addressed, the results can be costly. First, if your website gets compromised, it immediately impacts your organization because people visiting it may be unable to access or find the information they need. In addition, the time and resources spent remediating and recovering your website will be significant in direct and indirect costs. The direct costs include: investigating the root cause and remediating your website, securing professional services to assist with remediation, and the inability to process payments and donations while your site is down. The indirect costs may come in the form of loss of trust among beneficiaries, partners, and donors, damage to your organization's reputation, the potential for higher cyber insurance premiums or loss of coverage, and a negative impact on operations and lost productivity. Generally speaking, dealing with a website cybersecurity incident can also be stressful for staff. When it comes to website security, preventative measures can have a significant impact on the future well-being of your organization and staff. The adage, "An ounce of prevention is worth a pound of cure," was initially used about fire hazards. However, it may readily apply to website cybersecurity.

THE THREAT LANDSCAPE

When someone visits a website, their activity typically involves navigating numerous pages and accessing information. However, website administrators with access to server traffic logs and analytics will see a different layer of activity: the significant amount of traffic generated by malicious bots that are constantly crawling websites looking for vulnerabilities.[3]

This threat landscape is a reality of the internet, and it is vital to remember that nonprofits are not immune to website cyberattacks. Automated bots are indiscriminate in the websites they crawl, as they are scripted to seek out weaknesses and entry points that may exist on any organization's website. These malicious bots access sites, attempt to brute-force logins and passwords, and seek to exploit different vulnerabilities on various web applications. These threats are on the rise each year[4] in part due to the increasing availability of automated tools, which make it easier for malicious actors to scale attacks and utilize credentials from other breaches.[5]

However, there is hope for those defending against these attacks. Many common causes of breaches share common characteristics, meaning specific mitigations can have a significant impact. According to IBM Security, approximately 19% of breaches in 2022 were a result of stolen or

3 **https://ieeexplore.ieee.org/abstract/document/9519384**

4 **https://www.imperva.com/resources/reports/2022-Imperva-Bad-Bot-Report.pdf**

5 **https://haveibeenpwned.com/**

compromised credentials, and phishing was the second most common cause at 16%.[6] With this in mind, mitigating these key threats and other common attack approaches will significantly improve an organization's security.

HOW THIS GUIDE WILL HELP

This guide provides an overview of common cybersecurity risks associated with nonprofit websites and how to mitigate these risks effectively. The guide also outlines the key activities you can undertake to protect your organization's website and ensure that you have the language to communicate knowledgeably with staff, volunteers, consultants, and vendors regarding the security needs of your website.

A checklist and practical steps to take regarding preparation and response to a security breach are included. Finally, there is guidance to help ensure that your organization's website is better protected against cyber threats.

nten

ABOUT NTEN

We are creating a world where missions and movements are successful through the skillful and equitable use of technology.

We build transformative power by connecting people who are putting technology to work for social change. We strengthen their individual and collective capacity for doing good by offering expert trainings, researching effective approaches, and providing places where relationships can flourish. We relentlessly advocate for the redesign of the systems and structures that maintain inequity.

NTEN reports support the growth and development of the sector through benchmarking the technology goals and challenges of nonprofits and by identifying areas of need.

For more, visit **nten.org/publications**.

6 **https://www.ibm.com/downloads/cas/3R8N1DZJ**

ABOUT PUBLIC INTEREST REGISTRY

Public Interest Registry (PIR) is a nonprofit that operates the .ORG top-level domain—one of the world's largest generic top-level domains with more than 10.8 million domain names registered worldwide. PIR's .ORG Family of Domains, including .CHAIRTY, .FOUNDATION, .GIVES, and .GIVING, is open to everyone, providing a global platform for organizations, associations, clubs, businesses and individuals to bring their ideas to life. PIR has been a champion for a free and open Internet for two decades with a clear mission to be an exemplary domain name registry, provide a trusted digital identity and help educate those who dedicate themselves to improving our world. PIR was founded by the Internet Society (**internetsociety.org**) in 2002 and is based in Reston, Virginia, USA.

Visit **www.TheNew.org** for more information.

Common nonprofit website security myths

Some prevalent myths can stand in the way of meaningful work advancing website security. By better understanding the myths and the realities behind them, nonprofits can more effectively address website security.

Myth: We aren't famous or doing controversial work, so no one would attack us.

Reality: Your data doesn't need to be particularly interesting to an attacker. As long as your data is valuable to you, that is a sufficient rationale to stage an attack. Whether it is an attempt to gain sensitive information, inject malware onto your site, or sell the data to other malicious actors, there are many reasons that a motivated attacker may have to compromise your website. In addition, attacks may also be automated through malicious bots, which can quickly scan millions of sites for vulnerabilities.

Myth: You have to be a trained technologist to address website security.

Reality: While technical knowledge is helpful, many steps for securing your website do not involve writing code or having an extensive technical background. Many basic security measures can be undertaken to improve your website's security significantly. In addition, many non-technical processes can be implemented by staff members to enhance website security.

Myth: We don't have the budget for it.

Reality: Many basic security processes and practices can be implemented cost-effectively to mitigate risk to an organization's website. Budgeting for website security may also take the form of nonprofit staff resourcing and training. While website security is an investment, the costs of remediating following an attack are much more expensive.

Myth: The software we use will automatically take care of it.

Reality: While many software providers will address security within their products, it is also essential to continuously verify the requirements for your organization, as cyber attackers are constantly evolving their tactics and discovering new vulnerabilities. Nonprofits also need to ensure they understand and advocate for their needs from their software vendors and push for continued improvements and security.

Myth: Cyber insurance is only for large organizations.

Reality: Cyber insurance can be beneficial for nonprofits of all sizes. When evaluating the costs of extended liability coverage for an organization, cyber insurance may provide financial risk mitigation and support in the event of a cyber incident, covering the costs associated with data recovery, investigation, and more.

Assessing and improving your website security

The following seven sections cover website hosting and domain name system records and security, as well as website security threats, detection, and response. We have organized these sections with a priority on the order of information that may be needed for general knowledge and management of your organization's website. There are recommendations included in the following sections that are truly universal. While we have included them where we felt they naturally fit from a nonprofit organization's management perspective, we hope you can apply the recommendations broadly across your systems, including emphasizing strong passwords, investing in training, and completing regular monitoring.

WEBSITE HOSTING

The foundation of your website starts with where it is hosted. When it comes to hosting from a third-party provider, there are generally two types: unmanaged and managed. Unmanaged hosting means your organization leases a server and handles its maintenance and security updates. Unmanaged hosting is typically suitable for organizations that require a high degree of customization and configuration for their website and have internal support in their organization that is familiar with backend server maintenance. While organizations hosting their website on unmanaged servers may find some usefulness in this guide, the content is primarily intended for those using managed hosting services.

For most nonprofit organizations, managed hosting services are more appropriate as they ensure that routine security and maintenance tasks are handled continuously. For many nonprofit organizations, managed hosting will help mitigate the costs and risks of website security.

Regardless of the type of hosting you use, some additional considerations are helpful to keep in mind. While many of the functions and services listed below may be available through your hosting provider, you may also find these services available as standalone offerings through specialized vendors.

Support

The level of support from a web host is an important consideration if you need to reach out to address website security issues. If you are in a situation where you need to reach support urgently, it is vital to ensure that you can get connected with a representative in a reasonable amount of time. When researching the available support, confirm the available channels, such as chat, email, phone, and the expected response times for each. It is also recommended that you verify each support channel firsthand to get a

sense of the actual response times. Generally, hosting providers that offer responsive support often come at a higher price point.

Backups

Web hosts may offer automated backups as part of their service offerings, which helps restore a website in case of a security incident or other disaster. In addition to daily backups, weekly and monthly snapshots can save significant amounts of time by allowing your organization to quickly roll back a website to a specific date as part of a remediation effort. In addition to backups that a web host makes, some content management systems also offer plugins that allow the website to be backed up to an organization's cloud storage. You should also confirm where the backups are stored so that if you need to roll back your website or access a backup file, you know how to do so. Backups should be stored in a separate location from where you may otherwise be locked out in the event of a breach.

Monitoring

Active, automated monitoring ensures a website's overall health and security. In addition, this allows your organization to be alerted to any anomalous traffic patterns or user behavior that may signal a security incident.

- **Uptime monitoring:** This type of monitoring regularly checks your website to ensure it is running and accessible. This may be included in hosting packages, with many free and affordable options online. In addition, this type of monitoring is helpful to ensure that your organization can respond quickly to address the causes of website downtime, which may include security incidents.
- **Resource monitoring:** This type of monitoring checks the usage of server resources such as CPU, memory, and disk space. This helps identify website performance issues and provides an early warning if malware has been installed and is consuming significant resources. An example of the type of malware this may detect is cryptojacking malware which uses a server's resources to mine cryptocurrency. Many web hosts will have this information available in their control panels.
- **Log monitoring:** Regularly monitoring your website's traffic and server logs may help identify unusual patterns. This includes reviewing login attempts as well as unusual traffic patterns, which may signal possible security issues. Many website hosts will provide access to logs and may also offer additional visualization tools to help analyze the data.

Security and software updates

Your web host and vendors must be aware of and consistently apply security updates to your server's software, as vulnerabilities are constantly being discovered and exploited.

Malware scanning

Some web hosts may offer active malware scanning, which will automatically detect the presence of malicious

applications or code and facilitate quarantining and removal of these files.

Distributed denial-of-service (DDoS) and bot protection

DDoS attacks and bots result in millions of attempts to brute-force websites to gain access to sensitive administrative areas or clog up a website. DDoS attacks may also be coupled with ransom demands by directing enormous amounts of traffic at a website to make it inaccessible until a ransom is paid.[7] Your website hosting provider may offer features and solutions, such as a content delivery network (CDN), that may help mitigate against DDoS attacks. In addition, it is helpful to clarify with your web host whether bot traffic counts towards your traffic totals, especially if your hosting package is measured according to the number of visitors to your website.

Web application firewall (WAF)

A firewall is helpful on a web server to mitigate emerging vulnerabilities in popular content management systems and plugins. Firewall rules can be an extra measure of protection, especially in instances where security updates may not have been released yet to address known problems. Firewall rules allow you to inspect the origin of the incoming traffic and offer options such as allowing the traffic to flow through, blocking it, or challenging it with a CAPTCHA. Some WAFs can also prevent brute-force login attacks by limiting the number of times an IP address can attempt to log in.

SSL certificates

Secure sockets layer (SSL) certificates ensure that the data transmitted between a web server and a browser are encrypted, secure, and private. This is most easily identifiable in a browser using https:// and is often denoted by a padlock icon in most web browsers. As a result, SSL certificates are often bundled with most web hosting packages. In addition, free SSL certificates are available through Let's Encrypt, a nonprofit certificate authority.[8] However, the setup and renewal of these certificates may require advanced technical setup to ensure they are implemented effectively.

Staging sites

A web host that provides an integrated content staging area ensures that your organization can test and review changes like security updates in an isolated environment. This helps mitigate the risk of deploying breaking changes to your live website.

WEBSITE SECURITY FUNDAMENTALS

While a wide variety of software and content management systems may be used for your organization's website, some fundamental security considerations are important to consider.

7 **https://blog.cloudflare.com/ddos-threat-report-2023-q1/**

8 **https://letsencrypt.org/**

Strong passwords

When a malicious bot discovers where administrative login pages are located, it may attempt to brute force administrative access in various ways. The first is raw brute force, which attempts to cycle through all possible password combinations rapidly. Generally, this is not particularly effective as an attack vector because web hosts often detect this intrusion and apply a block or rate limit the connection. However, a more effective method of attack that may be employed is credential stuffing. Credential stuffing refers to using compromised passwords from other breaches and trying the same username and password on other sites. Using the same username and password across multiple sites can pose a significant threat to your organization.

Generally, having a strong password unique to each site with at least 16 characters and a combination of uppercase, lowercase, numbers, and symbols is crucial. The more characters you have, the better. Passwords that are eight characters or shorter are at significant risk of being easily compromised.[9]

Changing the default login page URL

Content management systems like WordPress have default login page URLs such as sitename.org/wp-admin, making it easy for bots to find and target. Changing the default login page URL can provide mitigation for basic automated bot attacks.

Principle of least privilege

If you have multiple contributors to your website, only grant access to specific areas users need to work on. When provisioning access to your website, users should only have permissions according to the principle of least privilege. This means that users should only have as much access as they need to perform their tasks. For instance, users who update the website's content should generally not be provisioned with access to administrative or billing areas. When the principle of least privilege is applied, this helps to limit the impact of a potential breach or misuse of access. Additionally, a good practice is to provision a separate account used solely for administrative changes to the website. Generally, an administrative account should not be used to make day-to-day updates on a website.

Multi-factor authentication

Multi-factor authentication, also known as MFA or two-factor authentication (2FA), requires users to provide two or more forms of authentication when logging into a website. This extra layer of security makes it more challenging for attackers to gain unauthorized access to your website, even if they have obtained a user's password. Even with strong passwords in place, MFA is an important part of securing your accounts.

For instance, an attacker may access a user's password, but the user has a second authentication factor, such as a physical security token or an authentication app on a

9 **https://www.security.org/how-secure-is-my-password/**

mobile device. In the example above, an attacker would need access to a user's password and physical security token or mobile device to log in. Multi-factor authentication can be a very effective security measure to mitigate credential-stuffing attacks that might otherwise be successful.

Multi-factor authentication is a feature offered by many web hosts and website software providers. It should be enabled if it is available. In addition, open-source content management systems may also have plugins that help to facilitate multi-factor authentication functionality.

Multi-factor authentication may include an SMS text message, a physical security token, or an authenticator app on a mobile device. While SMS text message authentication is widely available, other multi-factor authentication options are preferable since SMS messages are vulnerable to SIM-swapping attacks.[10]

Security updates and plugins

Security updates are generally regularly released when using a reputable vendor-supported content management system. They may include bug fixes, patches for vulnerabilities, and security improvements. These are often implemented in the background, and verifying the patch schedule for your vendor is good practice.

For popular open-source content management systems such as WordPress or Drupal, automated updates are an option that may be enabled. This ensures that software is automatically updated when a new release is available. If your organization is using an open-source content management system, it is important to ensure that there is a plan and process in place to ensure regular maintenance and security monitoring of the core software, as well as the plugins.

A leading cause of compromised websites is plugins that are out of date.[11] Plugins are third-party modules installed to provide additional functionality to a website. However, there is a wide variance regarding the level to which authors monitor, maintain, and update their plugins. Third-party plugins should only be installed from trusted sources and regularly reviewed to ensure they are maintained and updated. According to Sucuri, it was "found that 36% of all compromised websites had at least one vulnerable component present in the environment".[12] Unpatched plugins can present an avenue for potential exploits to be carried out on websites.

Various security plugins and services are available for open-source content management systems that provide website owners with additional security functionality, such as web application firewalls, malware scanning, multi-factor authentication, and vulnerability alerts.

10 **https://en.wikipedia.org/wiki/SIM_swap_scam**

11 **https://blog.sucuri.net/2023/04/balada-injector-synopsis-of-a-massive-ongoing-wordpress-malware-campaign.html**

12 **https://sucuri.net/wp-content/uploads/2023/04/Sucuri_2022-Website-Threat-Research-Report.pdf**

DOMAIN NAME SYSTEM (DNS) RECORDS AND SECURITY

Your organization's domain name is a critical piece of your website infrastructure as it provides important direction to website visitors regarding where to direct website traffic and email, among other things. When a visitor enters your organization's URL into a browser, a lookup is performed and translated into an IP address, allowing the browser to connect to the correct website server.

DNS security is vital because these records control traffic flow to your website, can serve as verification for your organization, and secure it against email spoofing and spam impersonation attacks.

Typically, the DNS records for your organization will be administered through an interface provided by a domain name registrar. Many web hosts may bundle domain name registration and hosting together. However, your domain names may be registered with a domain name registrar that is different than your web hosting provider. Regardless, it is important to ensure that the login to access the domain name information is secured with a strong password and multi-factor authentication and that the principle of least privilege is employed.

Updated domain information and domain privacy

It is vital to ensure that the contact information on your organization's domain name is current to ensure that domain renewal notices are received and acted upon promptly. Keeping this information up to date also prevents unauthorized transfers.

The Internet Corporation for Assigned Names and Numbers (ICANN), which oversees domain name registration, requires that registrars collect the phone number, email address, and mailing address of those registering a domain name. This information used to be made publicly available in the WHOIS directory, a global public database of domain name registrants, but since May 2018, this has changed to comply with a European privacy regulation with global reach.[13] The standard practice is now to redact personal data from registration data lookups.[14] In addition, many domain registrars offer domain privacy or proxy features that provide forwarding addresses and prevent personal information from being shared publicly via WHOIS or even directly with the registrar. These domain privacy features also can help mitigate the risk of attackers easily finding and using personal information.

Domain lock

A domain lock can prevent unauthorized or accidental transfers of your domain name by requiring an extra step

13 **https://lookup.icann.org/en**

14 ICANN Temporary Specification for gTLD data: **https://www.icann.org/resources/pages/gtld-registration-data-specs-en**

to unlock the domain before changes can be made. When a domain lock is turned on, transfers and deletions of a domain name are prevented, as well as modification of the contact details.

Email verification via DNS records, SPF, DKIM, DMARC

Sending a spoofed email is straightforward for attackers as it does not require complex tools or advanced knowledge. This allows spammers and attackers to easily attach your website's domain to a sender address and impersonate your organization.

However, there are several measures that organizations can take to make email spoofing more difficult. In addition, many email services now penalize domains that do not have a sender policy framework (SPF) and DomainKeys Identified Mail (DKIM) records set up. Organizations that do not have this set up risk a greater likelihood that their email may be flagged as spam. The reason why SPF and DKIM are needed is that these records help to prevent malicious actors from posing as your organization. SPF provides a public record that identifies authorized senders and decreases the likelihood that your email addresses can be spoofed.

SPF records are typically set up via a TXT record in your DNS and will look similar to the following example below:

```
v=spf1 ip4:192.168.0.0/16 include:_spf.example.com ~all
```

The record above is purely an illustrative example and will not actually work. Your organization will need to customize an SPF record with the appropriate IP addresses and domains to fit your use case. In the illustrative example above, the SPF record would authorize email senders with an IP address between 192.168.0.0 and 192.168.255.255, as well as _spf.example.com.

DKIM is an email security standard that verifies that a message was sent from a server and was not altered along the way. DKIM records function by providing an organization with a way to sign a message, and mailbox providers can verify that someone from your organization was sending the email. DKIM records confirm that you are a legitimate sender. In addition to providing increased security, it ensures that your messages are more likely to be delivered.

Properly configured SPF and DKIM records will also help improve the email deliverability of outbound messages for your organization.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) allows organizations to identify vulnerabilities and improve email security. To use DMARC, SPF and DKIM records must be set up first. A properly configured DMARC record will provide instructions for email servers on how to handle unauthenticated emails. DMARC can also be set up to receive reports from servers that receive spoofed emails from your organization's domain. These reports can provide helpful information to identify unauthorized senders and incorrect SPF/DKIM configurations.

Managing and securing similar domain names and expiring domain names

A possible attack approach is using domain names similar to your organization. Suppose your organization is sitename.org, and the domain names may be available for .com or .net or other potential domains that may be confused with your organization. In that case, it may be worth securing those domains to protect your organization's brand and security.

Another attack method is using expiring domain names. When a domain expires, it is available for anyone to register after certain grace periods elapse. Reclaiming an expired domain can be time-consuming, requiring you to prove ownership of a registered trademark and undertake a lengthy process set by the Uniform Domain-Name Dispute-Resolution Policy (UDRP) as adopted by ICANN. Setting up domains to auto-renew (and maintaining payment information) can avoid this.

When considering purchasing domains for specific projects or events, it is vital to consider the potential long-term maintenance of these domains.

Managing and monitoring expiry dates of domains and certificates

When registering domain names and SSL certificates, part of the long-term ongoing maintenance involves renewing them. Domain names can be registered for up to ten years (one registrar even offers a 100-year registration service), and it is essential to include renewals as part of regular maintenance and review schedules. This helps prevent registration lapses which may subsequently pose a security threat. In addition, SSL certificates can also be a cause of unanticipated site downtime and pose security risks for your website. Therefore, it is recommended that organizations configure their web host provider or set up internal processes to generate and renew SSL certificates automatically.

Domain Name System Security Extensions (DNSSEC)

DNSSEC is an advanced configuration that prevents attackers from redirecting your internet traffic to malicious websites. It does this by signing DNS records and authenticating them to verify that they have not been modified in transit. DNS spoofing attacks are uncommon, but they may be of concern to high-profile websites or organizations that may be more susceptible to targeted attacks. DNSSEC provides an extra layer of security in that regard. To set up DNSSEC, your domain registrar and DNS hosting provider must both support DNSSEC.

WEBSITE SECURITY THREATS

When assessing website security threats, it is essential to understand common attack vectors to mitigate the risks they may pose to your organization.

Brute force attacks

Brute force password attacks are when an attacker repeatedly tries guessing a password using trial and error with common passwords or cycling through all the possible combinations of characters. Without appropriate safeguards in place to mitigate against brute force attacks,

a high volume of guesses may be attempted. Brute force attacks may be mitigated by enforcing strong password policies, applying rate-limiting policies to login pages, and multi-factor authentication.

Credential stuffing

Related to brute force attacks, credential stuffing utilizes password databases that have been previously breached and attempts to use the same username and password combination.[15] This attack operates under the assumption that the same username and password combination may be used across multiple sites. This attack may be mitigated by utilizing a password manager to generate unique credentials for each website and multi-factor authentication.

Distributed Denial-of-Service (DDoS)

DDoS attacks refer to instances when a significant volume of traffic is directed toward a website, leaving it inaccessible to staff and visitors. This traffic may be generated from compromised websites or networks of malicious bots. A web application firewall (WAF) configured with policies to block or rate-limit malicious traffic can mitigate this attack. Many hosting providers offer such protection as part of their services.

Malware

Malware generally refers to a website hosting or serving up malicious software. Malware may also refer to plugins that contain malicious code or may have been compromised with malicious codes. Malware may be mitigated with regular security scans, automated updates, and secure authentication practices among staff.

SQL injection attacks

Many websites use databases to store information and use Structured Query Language (SQL) to access this data. A common attack vector on websites is SQL injection attacks, in which attackers attempt to submit malicious code through forms on the website, such as contact forms or registration forms, to gain unauthorized access to information or to bypass security mechanisms. To prevent such attacks, all form inputs on a website should be validated and sanitized before being processed in SQL queries.[16]

XSS attacks

Cross-site scripting or XSS attacks are similar to SQL injection attacks, but the attack focuses on the browser rather than the server. In an XSS attack, attackers will attempt to inject code to maliciously obtain access to information on a browser, such as cookies. This can be mitigated by validating user inputs and sanitizing data to protect website applications from XSS.

15 You can check to see if your email has been part of a known breach here: **https://haveibeenpwned.com/**

16 For a humorous take on SQL injections and input sanitization: **https://xkcd.com/327/**

PREPARATION AND PREVENTION

Organizational preparedness can take the form of implementing basic precautions to mitigate most website security risks.

Incident response plan (IRP)

An incident response plan is a document that outlines organizational procedures in the event of a cybersecurity incident. The incident response plan forms part of an organization's broader governance framework. It includes elements such as how a cyber incident can be recognized, the composition of a cybersecurity incident response team, and the incident handling process. Incident response plan templates are available online.[17]

Cybersecurity incident response team (CSIRT)

Identifying who will be a part of an incident response team that will serve as the primary team remediating the website and lead recovery efforts is helpful. At the very least, a team leader should be designated to conduct the incident response and report to management regarding what is happening. Functions that the team may cover include communications, investigation, and analysis.

Organizational cybersecurity policy

Develop and maintain a robust cybersecurity policy that includes practical steps, identifying assets and risks, and preventative and reactive measures organizations can take for their website security. Here is an **example of a cybersecurity policy that can be used as a starting point**. In addition, an organizational cybersecurity policy that includes guidance for website security can provide clarity for staff around roles and responsibilities, as well as organizational direction.

Cybersecurity training

Providing staff with cybersecurity training is important to strengthening your organization's website security. In addition to ensuring staff are trained in selecting and using strong passwords and multi-factor authentication, training in identifying suspicious and phishing emails and similar social engineering attacks will help prevent potential malware from potentially impacting your website. Various online training programs are available to provide cybersecurity training and ongoing phishing simulations for staff.

Reporting and feedback mechanisms

It is important to ensure that staff have clear direction around where to report and address any concerns regarding cybersecurity within the organization. Staff should be familiar with typical red flags of a compromised website, such as unexpected content, and understand how to report suspicious activity to the organization's website or IT administrator.

17 **https://ised-isde.canada.ca/site/cybersecure-canada/en/certification-tools/develop-incident-response-plan-fillable-template-and-example**

Password managers

Using a password manager within your organization can significantly help mitigate security risks by managing and encrypting passwords. A password manager can generate strong and unique passwords for each website. As a result, if a website is breached, the impact is limited as the password will have only been unique to that website. The centralized aspect of a password manager also ensures that credentials may be revoked from users in the event of staffing or volunteer changes.

Multi-factor authentication

Multi-factor authentication provides an extra layer of security, as noted in the website hosting section. It is a simple tactic that can mitigate the risk of many password-authentication attacks. All staff should have access to multi-factor authentication and corresponding devices to access the verification codes.

Virtual private networks (VPN)

A VPN creates an encrypted tunnel from a device and safeguards sensitive data in transit. When accessing your organization's administrative functions, it is a good practice to use a VPN to prevent third parties from intercepting your data while in transit, also known as an eavesdropping attack. A VPN is particularly important when accessing the internet through untrusted networks, such as public Wi-Fi hotspots.

Scenario testing

A cyberattack on your organization's website can be stressful, and preparation can help ensure an effective response. Just as fire drills ensure that staff members are clear on who is to take charge and what everyone is expected to do, scenario testing for cyber incident responses can help test your organization's preparation for handling an incident.

Scenario testing brings together staff to walk through the steps that would be taken in a hypothetical cyberattack, and the exercise is to identify gaps in the incident response plan. A scenario test will provide a briefing of the scenario and present a situation with a discussion of how everyone will respond. During the exercise, participants will be introduced to additional details of the hypothetical scenario, and further discussion will indicate the actions that will be taken. Following the exercise, a debrief is conducted to evaluate the response, discuss the outcomes, identify the strengths and weaknesses of the existing incident response plan, and review any lessons learned. This allows staff to surface questions and concerns about the organizational response. Subsequently, actions may be taken to address gaps and weaknesses in the established incident response plan. These gaps may be addressed by additional training or documentation.

Tabletop exercise templates are available online on a wide range of scenarios for your organization.

Penetration tests

A penetration or "pen test" is an authorized simulated attack against your website to assess potential exploits and security. Pen tests may be conducted by in-house technical staff within your organization or an external vendor as part of ongoing security testing. Pen testing may also allow you to engage with tech-savvy volunteers interested in contributing to your organization's website security efforts. Pen tests must be documented, outlining the steps to replicate the vulnerability as well as actionable information and recommendations for remediation.

DETECTION

Recognizing the signs when your organization's website security has been compromised is essential, as early detection is critical in mitigating the damage that an attack can cause.

How do you know if your website security has been compromised?

It is important to monitor and analyze your web traffic and server logs and recognize the typical activity patterns on your website. Historical logs will provide a broad understanding of your organization's standard patterns and seasonal trends.

Some indications that your website may have been compromised include the following:

- Unexpected changes to your website's content or layout may indicate that an attacker has gained unauthorized access or that malware may be present.
- Unexplained user accounts.
- Your website is inaccessible.
- Sudden increases in web traffic from unfamiliar sources could indicate that a DDoS attack is underway.

Webmaster tools

Popular search engines such as **Google** and **Bing** have webmaster tools where website owners may register their websites and are provided with reports, tools, and resources to monitor how their website appears on search results. The webmaster tools can also alert you when malware is detected on your website.

Vulnerability databases

When vulnerabilities are discovered and disclosed, they are typically documented in a CVE or Common Vulnerabilities and Exposures report. It is important to have a record of all your software assets and also ensure that there is proactive monitoring of any CVEs that may be related to them.[18]

RESPONSE

When a cybersecurity event has occurred, it is important to stay calm and focus on mitigating the risk to the organization. The following steps provide a broad outline

18 **https://nvd.nist.gov/vuln/search**

of what organizations may consider undertaking following a website cybersecurity incident. Note that steps may not necessarily be sequential and, in some circumstances, be coinciding.

1. Activate the incident response plan and incident response team. Refer to your organization's plan and convene the individuals identified on the team. This may include IT, executive leadership, and legal counsel if relevant. In addition, if your organization has cyber insurance, you may need to notify your insurance provider, and they may also be involved in the incident response.

2. Secure the website. The immediate priority should be safeguarding the website against additional threats and preventing further risk to the organization. This may involve resetting passwords for all users, prioritizing those with administrative access, activating DDoS protection, and modifying web application firewall policies to mitigate against any active threats. Taking down the website entirely while securing it may be necessary.

3. Restore and remediate. After the risks from active attacks on your website have been mitigated, your organization may begin remediating and restoring your website. This may involve restoring the website from a secure backup verified to be free of vulnerabilities.

4. Investigate. Organizations need to determine the cause of a website security incident through an investigation. This may take the form of documenting evidence of the compromised website, including screenshots and server logs, along with an analysis of the data. The documentation may be helpful in further strengthening organizational practices and procedures around website security as well as potential legal proceedings.

5. Communicate. Depending on the type of website security incident that your organization is experiencing, it may require notification to parties who may be impacted, including clients, volunteers, and donors. There may also be regulatory requirements for notification if personally identifiable information (PII) is compromised, depending on your jurisdiction. In addition, law enforcement may need to be notified to report the incident.

Website Security Checklist

Below is a checklist for your organization to consult with your staff or external service providers. This provides a simple reference to key mitigations in securing your website.

Website hosting

- [ ] Automated backups
- [ ] Uptime and resource monitoring
- [ ] Automated software updates
- [ ] Malware scanning
- [ ] DDoS and bot protection
- [ ] Web application firewall enabled
- [ ] SSL certificate enabled

Website security fundamentals

- [ ] Default login URL is changed (if relevant)
- [ ] Password manager
- [ ] Multi-factor authentication enabled

Website security threats

- [ ] Website user inputs are sanitized to prevent SQL Injection and XSS attacks

Domain name system (DNS)

- [ ] Domain contact information is up to date
- [ ] SPF and DKIM records configured
- [ ] DMARC is set up (advanced)
- [ ] Domain name status is locked at the registrar to prevent unauthorized changes
- [ ] DNSSEC enabled (advanced)

Preparation and prevention

- [ ] Incident response plan in place
- [ ] Cybersecurity incident response team identified
- [ ] Organizational cybersecurity policy
- [ ] Cybersecurity training for staff
- [ ] VPNs used by staff
- [ ] Webmaster tools enabled on Google and Bing

Conclusion

As an essential part of a nonprofit's online presence, a website remains a critical resource for organizations. Strong website security offers a solid foundation for your online presence and provides peace of mind, allowing your organization's staff to focus on core activities that advance your mission. However, it is important to remember that website cybersecurity must be a shared and collaborative effort among everyone involved. The strength and security of your organization's website will rely upon the preparedness and vigilance of your organization's staff and partners.

As the online landscape continues to evolve, so do the threats to your website. It's essential to recognize that website cybersecurity efforts should not be taken in isolation as a one-off activity and that ongoing measures, such as education and training, are necessary to adapt and respond to emerging challenges. Website security is a journey, not a destination, as it will require ongoing efforts regarding protection, detection, and response. In that spirit, engaging with others in the nonprofit community and learning about emerging security issues is crucial as you move ahead. Together, we can collectively improve our website security. Stay safe!

Additional Resources

- Cybersecurity for Nonprofits PDF guide
- Cybersecurity Essentials for Philanthropy PDF report
- 2018 State of Nonprofit Cybersecurity Report PDF report
- Tech Accelerate Public Data
- .ORG Learning Center
- The GCA Cybersecurity Toolkit for Mission-Based Organizations