MARSH & McLENNAN
AGENCY

15 BEST PRACTICES TO PROTECT YOUR WEBSITE FROM MALWARE & CYBER-HACKING

As hackers grow faster, more numerous, and more effective, many companies are struggling to protect their websites from cyber-threats. The statistics don't lie:

- Over 360,000 new malicious files are detected every day
- There were 1,188,728,338 known attacks on computers in 2017
- Damage to businesses by cyber crime is expected to reach $6 trillion by 2021
- Global spending on cyber security will likely exceed $1 trillion between 2017 and 2021

WEBSITE SECURITY **IS CRITICAL**

These staggering numbers clearly demonstrate why organizations must make website security a critical priority. Various types of cyber-attacks and malicious programs exist. It's crucial that every IT department understand the following risks: viruses and worms, Trojan programs, suspicious packers, malicious tools, adware, malware, ransomware, denial of service, phishing, cross-site scripting (SQL injection), brute force password attack, and session hijacking.

When these cyber breach attempts are successful **(which is often)**, the following can occur:

- Website defacement – unwanted content placed on your website
- Websites are taken offline (your site goes down)
- Data is stolen from websites, databases, financial systems, etc.
- Data is encrypted and held for ransom (ransomware attack)
- Servers are misused to relay webmail spam, to serve illegal files
- Servers are misused as a part of a distributed denial of service (DDOS) attack
- Servers are misappropriated to mine for Bitcoin, etc.

MINOR ATTACKS **TO SEVERE REPERCUSSIONS**

While some attacks present only minor threats like a slow website, many attacks result in severe repercussions such as major theft of confidential data or indefinite website failure due to ransomware. With that in mind, here are 15 best practices your IT department should be leveraging to protect your organization from malware and cyber-hacking.

Sources:

-Morgan, Steve. "Top 5 Cybersecurity Facts, Figures and Statistics for 2018." CSO Online, InfoWorld, 23 Jan. 2018, https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

-"Cybersecurity Spending Poised to Rise in 2018, Gartner Reports." Security Intelligence, securityintelligence.com/news/cybersecurity-spending-poised-to-rise-in-2018-gartner-reports/.

-MMA Cyber Security – https://www.marshmma.com/offerings/business-insurance/cyber-liability

1. **Keep your software updated.** It's crucial that you keep your operating system, general applications, anti-malware and website security programs updated with the latest patches and definitions. If your website is hosted by a third-party, make sure your host is reputable and keeps their software up-to-date as well.

2. **Protect against cross-site scripting (XSS) attacks.** Hackers can steal credentials and login cookies from users when they opt-in or register by introducing malicious JavaScript into your coding. Install firewalls and protections against injections of active JavaScript into your pages.

3. **Protect against SQL attacks.** In order to defend against hackers that inject rogue code into your site, you must always use parameterized queries and avoid standard Transact SQL.

4. **Double validation of data.** Protect your subscribers by requiring both browser and server-side validation. A double validation process will help block insertion of malicious scripts through form fields that accept data.

5. **Don't allow file uploads on your website.** Some businesses require users to upload files or images to their server. This presents significant security risks as hackers can upload malicious content that will compromise your website. Remove executable permissions for files and find another way for users to share information and images.

6. **Maintain a robust firewall.** Use a robust firewall and restrict outside access only to ports 80 and 443.

7. **Maintain a separate database server.** Keep separate servers for your data and webservers to better protect your digital assets.

8. **Implement a Secure Sockets Layer (SSL) protocol.** Always purchase an SSL certificate that will maintain a trusted environment. SSL certificates create a foundation of trust by establishing a secure and encrypted connection for your website. This will protect your site from fraudulent servers.

9. **Establish a password policy.** Implement rigorous password policies and ensure they are followed. Educate all users on the importance of strong passwords. In essence, require that all passwords meet these standards:

    - Length is at least 8 characters
    - At least one capital letter, one numeral and one special character
    - Do not use words that can be found in the dictionary
    - The longer the password, the stronger the website security.

10. **Use website security tools.** Website security tools are essential for internet security. There are many options, both free and paid. In addition to software, there are also Software-as-a-Service (SaaS) models that offer comprehensive website security tools.

11. **Create a hack response plan.** Sometimes security systems are averted despite the best attempts at protection. If that occurs, you will need to implement a response plan that includes audit logs, server backups and contact information for your IT support personnel.

12. **Set up a backend activity log system.** In order to trace the point of entry for a malware incident, ensure you are tracking and logging pertinent data, such as login attempts, page updates, coding changes and plugin updates and installations.

13. **Maintain a fail-safe backup plan.** Your data should be backed up regularly, depending on how frequently it is updated. Ideally daily, weekly and monthly backups are available. Create a disaster recovery plan appropriate for your business type and size. Make sure you save a copy of your backup locally and offsite (many good cloud based solutions are available), enabling you to rapidly retrieve an unaltered version of your data.

14. **Train your personnel.** It is imperative that everyone is trained on the policies and procedures your company has developed in order to keep your website and data safe and prevent cyber-attacks. It only takes one employee clicking on a malicious file to create the opportunity for a breach. Ensure everyone understands the response plan and has a copy of it which is easily accessible.

15. **Make sure your partners and vendors are secure.** Your business may share data and access with many partners and vendors. This is another potential source of breach. Make sure your partners and vendors follow your web security best practices, to help protect your website and data. This can be done using your own audit process, or you can subscribe to software security companies which offer this service.

Even a high-end computer system can be brought down quickly by nefarious malware. Don't procrastinate on implementing the above security strategies. Securing your website from hacking and cyber attacks is an important part of keeping your website safe and your business secure.

For more information on cyber related risks and cyber liability insurance, visit MMA's Cyber Liability Online Resources, or contact the Marsh & McLennan Agency. With over 5,000 colleagues in more than 75 office locations, MMA can help organizations with all of their risk management needs. ●

This document is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. Marsh & McLennan Agency LLC shall have no obligation to update this publication and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting or legal matters are based solely on our experience as consultants and are not to be relied upon as actuarial, accounting, tax or legal advice, for which you should consult your own professional advisors. Any modeling analytics or projections are subject to inherent uncertainty and the analysis could be materially affective if any underlying assumptions, conditions, information or factors are inaccurate or incomplete or should change.