4 Strategies to get your website security ready

By Gary Stevens

11 Dec 2018

Is it too obvious to say that website security is vitally important to small to medium-sized enterprises (SMEs)?

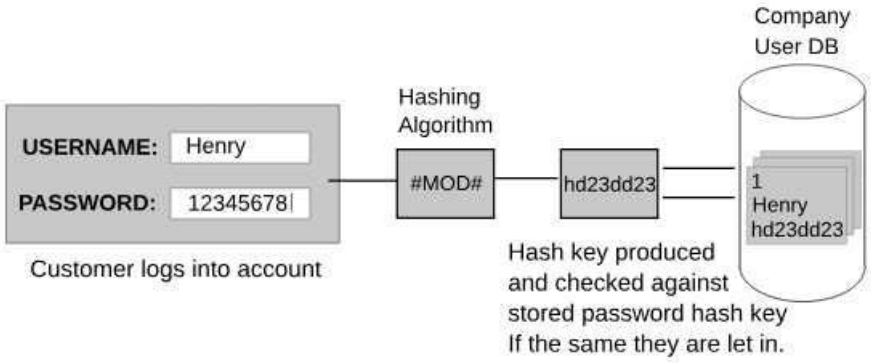
Gary Stevens

The problem is that business owners often mistakenly believe that their businesses are not large enough to attract the attention of attackers. Nothing could be more wrong. In fact, the most recent stats say that 58% of all malware attacks happen to a small business.

Maintaining website security is a critical duty owed your business and customers. The latter has chosen to give you their personal information. You need to treat it responsibly.

Here's how.

Use effective password management



You, as well as your employees, need to select strong passwords and change them frequently. One of the most common ways that websites are compromised is through simple or weak passwords.

When coming up with a password policy, don't err on the side of being too generous. Convenience is often used as an excuse for sloppy password management, but the outcome can create headaches for both you and customers.

Let employees know that using words or phrases opens them up to attacks by dictionary or brute force bots. Using the same password for an extended period of time or across various sites also creates pointless vulnerabilities.

When sharing is bad: Another factor to consider is the cost benefit of using shared credentials. While small businesses do have to keep a constant eye on their bottom line, sharing credentials to lower costs is not without risks. Shared logins are automatically weaker.

The strongest passwords are at least eight characters long. Using numbers, letters and special characters makes it harder to guess. Passwords should be changed every few months, and the system should be set up to lockout a user after a specific number of invalid login attempts. If users will be accessing the applications remotely or on mobile devices, it makes sense to implement multi-factor authentication.

Protect your content management system (CMS)

Content management systems like WordPress and Joomla have revolutionised the world of website building and put an internet presence within the reach of practically anyone with even rudimentary technical skills.

The dazzling array of themes and plugins - that do everything from letting you put an instant poll on your front page to migrate the entire content of your site between different CMS platforms almost instantly - can lead you to believe it's real-world magic at work. Unless you don't keep them updated.

Outdated software makes your website a big flashing target for attack. Old plugins and themes create similar security issues. It is important to run the most current versions of all software to reduce vulnerability. Waiting until your website is compromised to backup or update is a bad practice.

Having an up to date backup (preferably stored offsite) allows you to recover quickly if your website is attacked. The open source nature of CMS leaves it particularly vulnerable to attack. This, however, doesn't mean a hack is inevitable, just that you need to accept the reality that a certain number of people will try to get in uninvited for all kinds of nefarious purposes.

- **Firewall**: In addition to keeping all software updated, you need a firewall. This not only adds an additional layer of security to your website but allows you to see what is actually going on behind the scenes so you can recognize any unauthorized access attempts.

- **SQL-Injections**: You should also protect your CMS from SQL-injections. This type of cyber attack attempts to add malicious code directly into your backend database. This code can then create and execute actions through your site. While the exact functions would depend on the attacker, the real problem is that a SQL-injection attack causes you to lose control of your server and database. You can protect your CMS from SQL-injection tampering using prepared statements which allow the SQL server to read and follow directions without opening the CMS up to attack.

- **SSL Certificates**: Strongly consider an SSL certificate for your site. A secure sockets layer certificate produces an encrypted link that travels between the server and the browser. Adding an SSL certificate not only provides additional security to your site, but also boosts SEO. It's also one of the most effective ways to prevent DNS hijacking.

Create and protect a specific administrator interface

Automated bot threats are a common source of weakness in SME websites. To help combat this constant assault, make it necessary to go through multi-factor authentication to access the administrator panel. To tighten up security further, configure an htaccess file. This allows you to build a list of IP addresses that are permitted access to your administrator page.

Train your employees

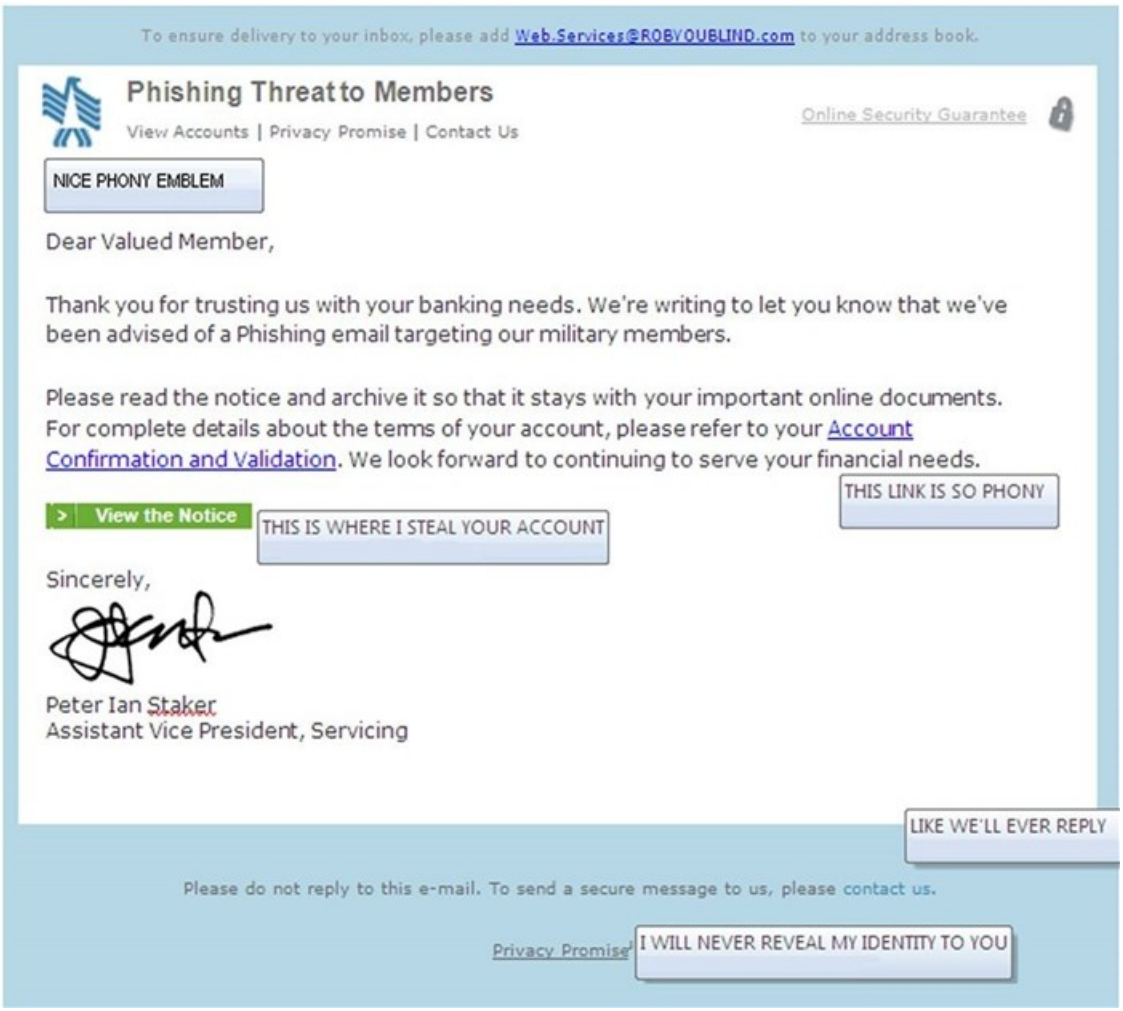
Probably the most important, as well as the most easily overlooked, factor in improving your website's security is to train employees. Employees account for more than 40% of the cybersecurity breaches worldwide. Policies are fine, but involving employees in the actual security plan fosters a sense of responsibility.

Hold regular training sessions to update and remind everyone of cybersecurity policies. Simple reminders, such as logging out of accounts when using a public terminal, should be part of your training program. So should reminders not to share passwords or use the same password to access multiple systems.

- **Social Media**:
  Do we even need to say the “F” word? You know what we’re talking about. Facebook. Know anyone who accesses it from work? Only everyone, right? Make sure that employees understand about this social media behemoth’s terrible track record with handling data. The bottom line is that accessing personal sites from work terminals creates additional and unnecessary security risks.

- **Don’t Go Phishing**:

  Make sure employees know how to recognize and respond to any suspicious emails or websites. You should have a procedure in place to address what to do if they do click on the wrong website or open a malicious email.



  Do they shut down the computer immediately? Contact IT? Run virus software on their own? Don’t leave it to each employee to determine what should be done, have a procedure in place and make sure everyone knows what it is. <

- **Automatic Bad Guys**:

  It is important to realise that most sites are not breached by individual hackers manually picking sites, Instead, the hacking process is automated, with bots identifying websites with vulnerabilities and attacking them.

Final thoughts

While this abbreviated list doesn’t cover every precaution a website owner should take, implementing the suggestions will get you a long ways down the road to being adequately protected. One thing is certain. Hackers aren’t going anywhere. If anything, they’re becoming more skilled, persistent, and numerous. Plan accordingly.

ABOUT THE AUTHOR

Gary Stevens is a front-end developer. He's a full-time blockchain geek and a volunteer working for the Ethereum foundation as well as an active Github contributor.