THE 5 LAYERS OF WEBSITE SECURITY

It’s Not Just In The Media

As a business owner, you’ll hear stories about website security breaches in the news on a more and more frequent basis. The last few years have brought significant breaches to a number of multinational companies.

Those breaches aren’t resigned to just large companies. Businesses of all sizes face website security problems on a daily basis. There’s no discrimination based on profits or number of employees.

There’s one single thing that leads to more website security issues than anything else. It’s the humble human being.

Seems hard to believe, doesn’t it? In the media or movies, you’ll see it portrayed as a “hacker” or an “evil intruder” who is breaking into a website. In reality, it’s usually someone taking advantage of a security lapse, which was the result of human error.

So how do these security lapses take place?

The first and frankly most common cause is through an insecure website. Many websites run on what are known as CMS (Content Management System) platforms. These are self-hosted and need to be kept up to date through regular maintenance. Outdated code can be vulnerable to security threats.

Password security is crucial in your business. Whether that’s internally within your team or if you have hired a contractor or team external to your business. You must use secure passwords that are unique. Re-using passwords or not running password audits regularly leaves an attack opportunity to malicious actors.

Every website should be using an SSL certificate right now. That’s when your web address starts with HTTPS and there’s a padlock visible in the browser. Using HTTPS encrypts website traffic and provides security to your visitors.

You may have heard of Firewalls previously, through your Internet provider or your home / business computer security. For a website, you’ll use a Web Application Firewall (WAF). These help to limit access to your website from malicious or automated (bot) traffic.

The final issue comes through social engineering. Phishing attempts where attackers pretend to be a trusted employee or company are common. It’s extremely important to be vigilant at all times.

It’s important to note that you can never be 100% safe from security breaches in business. What you can do is take action to make your website and business as safe as possible. In this guide, we’re going to walk you through common issues and how you can prevent these in your business.

1 Website Maintenance

For most businesses, your website is one of the most important parts of your business. Without it, you may not be able to sell or advertise your products or services.

Many websites run using a self-hosted Content Management System (CMS), as we mentioned on the previous page. Examples of these include WordPress, Joomla, Drupal, Magento and Prestashop.

Platforms such as Squarespace, Wix and Shopify also offer CMS functionality but as they are hosted platforms, the maintenance and software updates will be taken care of by the platforms themselves.

When you have a self-hosted website, this means that the website is hosted with a hosting provider that either you or your web agency are paying for. It's these websites that need to be maintained and updated on a regular basis.

In our example here, we'll focus on WordPress as it's a very popular platform that powers over 35% of the websites in the world today.

With WordPress, there are three main areas that need to be updated:

- **Core WordPress Files -** These are the files that control the WordPress software. Core updates happen on a regular basis to add in new features, provide bug fixes and for security updates.

- **Plugins -** Plugins add functionality to your website. An example of this could be a contact form plugin, used for adding a form on your 'Contact Us' page for your visitors to send you a message. Plugins are regularly updated to add new features, resolve any bugs and most importantly, to fix known security issues.

- **Themes -** A WordPress website uses a theme to display the content on your website in a pleasing way. Your website will either use a theme that is commercially available or your web agency will have designed a bespoke solution for you. Themes will also be updated to add features and fix bugs or security issues.

Just like any other self-hosted CMS platform, WordPress should be updated regularly. We would recommend weekly updates as a good rule of thumb. To carry out updates, you would first ensure that a backup of your website has been taken and then proceed through the WordPress admin dashboard to carry out any updates.

Failing to keep your website maintained and updated will leave it vulnerable to attacks. These attacks can include data theft, installation of malicious software or defacement of your content, to name just a few.

TIP: Assign at least one member of your team to be responsible for maintaining your website on a regular basis. If your web agency offers a "Care Plan" or "Maintenance Plan", it's strongly recommended that you consider this, as it will bring you peace of mind. For a low monthly fee, the web agency will keep your website backed up and updated.

2 Password Security

Passwords are very much like your keys. Without them you're going to struggle to access information that you want. Thankfully, it's a little easier to reset a password than it is to visit a store and get a replacement key.

In today's modern world, every password that you create and use should be secure. More importantly, it should be unique and not one that you've used anywhere else online.

Reusing a password is a mistake that a lot of people make when they're setting up a new account. Every time you use the same password again, you're adding a potential point of failure.

Malicious attacks that lead to data theft on a large scale, have happened a number of times over the last few years. When these attacks include password data, attackers who utilize the data will attempt to break-in to popular services such as PayPal. If you are someone that reuses passwords and someone is able to successfully log-in to your PayPal account, you can imagine the type of chaos that could happen next.

Of course, you may find it hard to remember all of the unique passwords that you'll be creating. That's understandable. It's not easy to remember a single series of letters, numbers and special characters for one password.

Thankfully there are password manager tools that will help you to securely save your passwords. Each of these tools is accessed via a master password - which is the only one that you'll ever need to remember. In addition, they also integrate with your web browser. This helps you to easily log-in to websites and online services.

Here are three password management tools that we recommend:

- **1Password -** https://1password.com
- **LastPass -** https://www.lastpass.com
- **Dashlane -** https://www.dashlane.com

If you have a team that needs shared access to passwords, each of the three recommended tools offer a plan for teams, which are charged per user.

When it comes to working in teams, it's a smart idea to give each user on your team their own access and password. You should also utilize any functionality that allows for different access levels - whether this is on your own website or a third party service. If you have any employees leave, it's much easier to disable one account than reset a password for every user.

Finally, make a plan to review your passwords on a regular basis. A good rule of thumb would be to review passwords every 3-6 months. At these points, update your most important passwords and help to keep your business secure.

TIP: Review your existing passwords. Ensure that you're using strong, unique passwords for every account. Update any passwords that are reused. Set you and your team (if applicable) up with a password manager, for easy storage and retrieval of passwords.

3 Website Hosting

Website hosting is one of the most common digital services that a business will purchase. In fact, it's a necessity if you want to have people visit your site and learn about your company.

There are thousands of hosting providers around the world, and one thing that we can tell you for certain is that not all web hosting companies are equal. The quality and speed of the hosting, as well as the service that you'll receive, can vary wildly.

The cheapest hosting accounts are likely on what is called a "shared environment". This is when hundreds or thousands of websites are all on the same hosting server. It provides a benefit to the hosting company as they can make more money through selling at scale, but there are downsides for your business.

When you use shared hosting, you're sharing the same resources as thousands of other websites. If those resources are stretched too thin, this can lead to your website being offline for short periods of time.

There are security implications to consider when you're using shared hosting. When a website is hacked on a shared hosting server, there's an increased risk of this also affecting your website. If your website is hacked, it can go offline, data could be stolen or it could directly impact your customers through hidden malware.

Finally, shared hosting servers mean that thousands of websites are assigned to the same IP address. If one of those websites is hacked or carries out activities such as sending spam emails, this can cause problems for your website and emails too. Your website can be blacklisted and it can even affect your rankings in the search engines.

The bottom line here is simple. Shared hosting is not the safest or most secure option for your business. We highly recommend ensuring that you use a high quality web hosting provider - buy the best you can afford. This will help to keep your website and customers safe.

Is your website currently using a security certificate? The easy way to tell is if your web address starts with "HTTPS", or if you can see a padlock in your browser when you visit. HTTPS is crucial as it provides a secure connection to your website for your customers. Not only this, but it also provides benefits to your Google search engine rankings.

SSL certificates should be provided by your hosting provider. They are usually free. If they're not, ask why. Cheap hosting companies are liable to need to recoup costs elsewhere, forcing customers to pay for SSL certificates.

Finally, we need to talk about firewalls. A firewall sits between the Internet and your website, protecting you from security threats. You likely won't need to worry about a firewall as these will usually be part of the security defenses that your hosting company provides. If your hosting provider doesn't have a firewall in place, there are third party options available such as Sucuri or Cloudflare.

TIP: Ensure you're using the best hosting provider that you can afford. Try to avoid shared hosting. Make sure that you are using an SSL certificate and that your website address starts with HTTPS. Ask your hosting company about what sort of firewalls and security they have in place to protect your website.

4 Website Backups

Website backups are absolutely essential for your business. A backup is a snapshot of your website taken at a point in time.

The reason these are so important are that if your website develops a problem or has a security issue, you can easily restore a backup and avoid any lengthy periods of downtime.

Backup frequency will depend on how often you update your website. If you make content changes infrequently, you would likely be okay with daily or weekly backups. If you're making regular changes to your website, then you must set up daily backups as a minimum.

Your hosting company will probably take backups of your website, but you should never rely on them for these. Hosting companies are not perfect and there have been many occasions where they either couldn't provide a backup, leaving a business owner with no website.

In addition, if your hosting company ever has a problem and your account isn't accessible - your website will be in limbo until the hosting company fixes the problem.

You should be in control of your own website backups. If you have a company managing your website through a Care Plan, that works fine too, but ask them questions and understand just how their backup processes work.

For a WordPress website, you can use a plugin such as UpdraftPlus or WPTimeCapsule. There are also third party services from companies like Blog Vault.

Your website backups should be stored externally. You can use a Dropbox or Google Drive account. These are likely tools that you may already be knowledgeable about and understand. The principle here is that you're storing the data externally, which helps you to get back up and running quickly when you need to restore the website.

If you can, try to store your backups in at least two external locations. This helps to add in some redundancy and provides more security for your website.

Once you have backups setup for your website, you need to test that they are working effectively, by restoring your most recent backup. This is imperative. You must make sure that your backups are working before you ever need to use them.

If you don't test your backup process, you could be left with a very nasty surprise when it comes to a time when you need to restore your website.

TIP: Review your current website backup process. Who is in charge of your website backups right now and what is the process in place? Are you storing backups externally? Have you tested your backups recently to ensure they're in good order?

5 Computer Security

The humble computer you're using every day either in your office or when you work from home, can leave your website vulnerable if you're not careful. Whether using a PC, Mac or a laptop, it's very important for you or your team members to ensure that your computer is updated regularly and has antivirus software installed.

Antivirus software is usually paid for, although there are some free versions available as well. Here's a short list of some recommended options:

- Kaspersky Total Security (Paid)
- Bitdefender Antivirus Plus (Paid)
- Windows Defender Antivirus (Free)
- Avast Antivirus (Free and Paid)
- AVG Antivirus (Free and Paid)

If your computer is not secure, you run the risk of an attack, such as through malware or a keylogger. These could easily siphon login details to your website, as well as any other sensitive data such as bank account or payment processor logins. You've also likely heard numerous stories online about computers being hacked or data being held to ransom.

If you or your team are using a computer on the move, you should be wary of public Wi-Fi connections. For example, at a hotel, airport or coffee shop. Never login to your website, online banking, or any sensitive website when you're using a public Wi-Fi connection. You can leave your data exposed and at risk.

If you must use a public Wi-Fi connection to do work, use it alongside a VPN connection. Using a VPN gives you a secure connection that encrypts your Internet use and stops bad actors from being able to see what you're doing. It will help you to work on the move and give you peace of mind.

The final thing that you and your team should be aware of are phishing emails, in particular something called CEO Fraud. The basic principle of these attacks is that they are a social engineering attack, designed to trick the recipient into taking the desired action. Attacks will usually be targeted towards CEOs, accounting staff and HR staff, but they could reach anyone in your company.

One of the most common attack angles will involve invoices or payment details. As an example, the emailed request might look like it's being sent from your suppliers, with a simple request to use their new bank details when you submit your next invoice payment. Another attack angle could be for an email to look like it's from the CEO / business owner of your company, i.e. you.

Be vigilant with any financial requests received via email, either from an external company or an internal employee. If you're in any doubt, call the person who sent the request and confirm that it's genuine.

TIP: Take some time to review your company's computer security. Are all of your machines running antivirus software? Ensure that everyone in your team is aware of the risks of public Wi-Fi. Finally, sit down with your team and make sure they know how to avoid phishing email attacks.

It’s Time To Take Action

It’s important now that you take action to keep your website secure. You may have had issues in the past, so you’ll know only too well how devastating the impact can be on your business.

If you’ve never had a security issue in your business, it’s very easy to become complacent. After all, why should you worry about something that has never happened?

I can tell you now that it’s this type of complacency that ends up causing huge problems for business owners when something inevitably goes wrong in the future. Without a plan, you’re left fighting fires that can quickly spiral out of control.

Your website is your digital window out to the world. You need to keep it online and in good health, in order for people to visit and find out more about your business. If your website is offline, this can cost you money on lost sales and also damage your reputation.

Schedule in some time over the coming few days to review the tips and action points in the guide, and give yourself the peace of mind that comes with good security.

Finally, as I mentioned at the start of this guide, you can never be 100% safe from security breaches in business.

The actions that you take as the business owner and the preparations that you make with your team, will help to minimize any attacks or damages as much as possible.

Once you have your plan in place, test it regularly. Make sure that you and anyone in your team who is responsible for your website security are prepared and ready, just in case the worst happens.

Keep an eye out over the next few days as I’ll have a few more emails to follow with some additional tips and ideas for you. In the meantime, if you have any questions, please don’t hesitate to reach out!