Demystifying Malware: A Simple Guide for Small Business Owners

In this day and age it's as if our businesses live in two worlds: one physical and the other virtual. Just like in real life your business is vulnerable to online threats in the virtual world. Imagine your online business space as a shop on a bustling high street. When you've finished for the night you'd lock your doors and put the shutters down at night to keep thieves out.

In the virtual world, you ned to do just the same, securing your online 'shop' from cyber threats. One of the most common of these threats is known as malware.

Understanding Malware

Malware, short for malicious software, is like the pickpocket of the internet world. It's a sneaky piece of software that cybercriminals use to gain unauthorised access to your site or steal sensitive data like customer name and addresses, payment information and purchase history, they could even use your site to spread malware to your customers personal devices.

There are many malware variants. This malicious 'pickpocket' can take many forms, such as viruses (which spread quickly), ransomware (which holds your data hostage until you pay a ransom), and spyware (which spies on your actions).

These cyber pickpockets can slip into your online 'shop' in various ways. They might sneak in through an email attachment, hide within a legitimate software download or website plugin, or exploit a weak point in your website's security to gain access to your site and possibly install additional malware.

They can even repoint your website to a malicious website to steal your customers data leaving them at risk of identity theft.

Most people think that malware only targets household computers but thats unfortunately not the case. Websites are a prime target for cyber criminals because of the sensitive data that you hold.

The Potential Impact of Malware on Your Business Website

Imagine waking up one morning to find your shop has been ransacked overnight.

That’s what a malware attack can feel like. Here are some of the ways it can impact your business:

Data Breach

Malware can pick the ‘lock’ of your customer database, stealing sensitive information such as credit card numbers or personal details. This not only jeopardises your customers’ trust in your businesses but can also lead to financial loss and legal trouble. If you think you’re data has been stolen you must inform the Information Commissioners Office.

Downtime

Some types of malware can ‘vandalise’ your website, causing it to crash, slow down or redirect your website to another website where criminals attempt data theft.

Even if you find out early that something is amiss there will inevitably be downtime as you’ll need time to remove malware infection before you can let customers use your site again.

This could mean lost sales and frustrated customers.

Reputation Damage

Just as a physical break-in can damage a shop’s reputation, a malware attack can harm your online reputation. Customers need to trust that their data is safe with you.

If that trust is broken, they may choose to take their business elsewhere and it can take years to rebuild your reputation.

How To Protect Your Business

The cyber landscape changes rapidly but the main thing to remember is that no site is 100% secure. You can take steps though to secure your online ‘shop’ against malware. It’s similar to installing a top-notch security system in a physical store. Here are some steps you can take to help prevent malware attacks:

Regular Updates

One of the most common attacks we see is an attack targets outdated software that have security vulnerabilities.

Websites are software, they run on computers systems called servers just like the software you have on your laptop.

Just like you'd fix a broken lock, keep all your computer systems and software updated. Developers often release updates to fix security flaws that could be exploited by malware and you should ensure your website is up to date. You can read more about website maintenance here.

Install Security Software
Install reliable antivirus and anti-malware software – your virtual 'security guards'. These programs patrol your system, looking out for any signs of malware and removing them before they can cause harm.

There is two sides to this though, some of this will have to be done by your web host as they have access to the server (computer system) so they will need to apply the relevant updates.

However there is security software like Wordfence that you can install on your website as another layer to help prevent malware attacks.

Employee Training
Ensure your staff follow safe online practices. It's like teaching them how to spot a suspicious character or counterfeit money. You should look for online course to educate staff that help them spot phishing attacks and malicious links.

It can be quite difficult however as some of the malicious software pretends to be legitimate software to avoid detection.

If staff have access to your website to make updates such as blog posts, you should ensure that they change there password frequently.

You should also ensure that computer systems that are used to update your website are free from malware infection. If a infected computers are used to update your site you run the risk that the infected device will spread malware to your website too.

Firewalls Encryption
Think of firewalls as your website's 'CCTV cameras', monitoring incoming and outgoing network traffic and blocking threats. Some of this will be done by your web hosting company but you can also install WAF security plugins like Wordfence.

Encryption
Encryption is like a secret code that scrambles your data, making it unreadable to

anyone who doesn’t have the key, bare in mind though if you loose your key you cant get back into the house!

Regular Backups

Regularly back up your website. If your website falls victim to malware, you can restore it to a previous, uninfected state quickly. We wrote a helpful article about website backups here.

With these precautions in place, you can have the peace of mind that your website is protected against malware attacks. However, it’s important to remember that nothing is 100% secure and the best way to protect yourself is by staying vigilant.

Malware Scanning

You should check with your web host if they scan your website to detect malware signatures. We for example run a scans daily to detect malware attacks and alert you if we find something so you can remove the malicious software from your site.

There are many different malware variants that contribute to todays online threats to your businesses, it could be malicious code that starts ransomware attacks to a computer network trying to gain access to your website or malware disguised as legitimate software. It all has the potential to damage your business and your reputation from data theft.

Remember, the best defense is a good offense. By understanding malware threats and taking steps to protect your business such as anti malware software and teaching staff how to spot phishing attacks helping stop malware infection, you can ensure your digital ‘shop’ remains safe and secure.