The Law Society

In partnership with

SHARKGATE

WEBSITE HACKING

Understanding its forms and how to protect your practice

SEPTEMBER 2018

THE LAW SOCIETY OF ENGLAND AND WALES

CONTENTS

FOREWORD

In today's digital-first age and as businesses, including law firms, strive to deliver and transact more online, the exposure to cybersecurity risks increase. The Department for Digital, Culture, Media and Sport's 'Cyber security breaches survey 2018' report[1] confirms that 98% of UK businesses surveyed rely on some form of digital communication or service in serving their customers and four in ten (43%) had experienced some form of cyber breach or attack in the last 12 months. Unsurprisingly, senior management in 74% of UK businesses are now giving cybersecurity a higher priority. The obligations of the new General Data Protection Regulation (GDPR) that came into effect in May 2018 and the fines for non-compliance have undoubtedly heightened this position.

The report shows that website related cyber attacks remained in the top three categories of the most commonly reported breaches, which include fraudulent emails or being directed to fraudulent websites, impersonating an organisation in emails or online and viruses, spyware or malware.

In helping Law Society members to understand more about cybersecurity, this whitepaper examines the potential vulnerabilities of websites; the types of hack, signs that a site has been hacked and their impact. It also suggests practical ways in which to reduce the likelihood of, and to mitigate, attacks.

This paper has been produced in partnership with specialist website security provider, SharkGate. We would like to extend our thanks to their team for sharing their expertise and writing this paper for a non-technical audience. We encourage you to take advantage of the free service to check your firm's website for hacks and malware. Please see the last page of this report for further details.

Christina Blacklaws
President of the Law Society of England and Wales

1 Source: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018

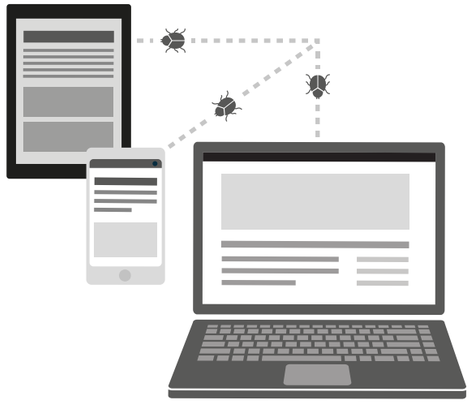
1. THE PROBLEM

There are more than 1.86 billion websites on the internet and around 18.5 million (1%) of these are infected with malware every week.[2] By 2021, it is predicted that cybercrime will cost the world £6 trillion annually – up from £3 trillion in 2015.[3] Computer hacking is one of the world's major problems, with new cases of data breaches and releases of ransomware occurring at an ever-increasing rate.

It has no boundaries: from the world's largest corporations, critical national infrastructure, through to small local enterprises and individuals. Many websites are built and hosted using open source software, which often have known vulnerabilities or do not have the latest security updates (patches) installed. Malicious hackers (also referred to as 'actors') scan the internet for these vulnerable websites that they can exploit to cause harm by stealing data or using the site for their own criminal activities, for example to promote and sell illegal products and content. Hackers view any insecure website as a means to an end. It's not always about the size, amount of traffic, or what the website is used for – the objective is to access and abuse your website and server's resources.

Leaving your website unprotected effectively gives hackers open and unauthorised access to modify content and, in some cases, open access to sensitive data. Organisations that do not proactively manage their website in-house or via an external agency increase the vulnerability of their site as hacks may remain undetected for a long period of time – possibly resulting in reputational damage or breaches of the GDPR.

The full costs of a cyber attack can be significant, especially the longer-term 'slow-burn' costs, such as the loss of competitive advantage, customer/client churn and demands on managers' time in responding to attacks. When factored into immediate costs, e.g. legal and forensic investigation fees, and extortion pay outs, slow burn costs can dramatically increase the final bill.



2 Source: https://www.securityweek.com/185-million-websites-infected-malware-any-time, 21 March 2018.

3 Source: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016, 16 October 2017.

2. HOW A WEBSITE IS HACKED

Hackers are always adapting their strategies and hacking techniques, constantly scanning for vulnerable websites that are unprotected and are going to be easy to hack. The easiest ones to hack often suffer from repeat attacks. Many sites, once hacked, remain hacked for many months as the hackers know all the weaknesses of the server.

There are two main reasons why small to medium sized websites are targeted: software/security vulnerabilities and access control.

1. **Software/security vulnerabilities –** Available security updates (patches) have not been installed, which makes the site easier to attack. Hackers use automated tools to search the internet for these vulnerable sites.

2. **Access control –** Passwords to access the website's content management system (CMS) or server are weak or follow a common pattern and are easily decoded. Using a technique called 'brute force', hackers use automated tools that attempt to access a site by trying many thousands of commonly used passwords.

3. TYPES OF HACKS

Once a hacker has gained access to a website, one or more of the following types of attack are generally deployed:

1. **Defacement**
2. **Data breach**
3. **Search engine optimisation (SEO) poisoning**
4. **Drive-by-downloads: malware and viruses**
5. **Cryptojacking**

3.1 Defacement

Defacement is one of the simplest, yet most effective, hacks and is sometimes called 'hack-tivism' as the hacker's objective is to spread a message by using the site as a communication channel. In this attack, content on an existing webpage is either changed or a new page is created that carries a specific message from the hacker. Messages are often political, but often are just a 'Chad woz here'.

Defacement hacks are mostly harmless but can cause the most damage to a firm's brand and reputation. Messages are placed in prominent positions, such as on the homepage and will be seen by most visitors (see examples in figures 1 - 4).

Figure 1: An example of a defacement warning the website's owner to fix the site's vulnerabilities

Figure 2: An example of a defacement informing the website's owner it has been 'Hacked by Exatr'

Figure 4: An example of a defacement warning the website's owner to increase the security of their website 'Patch your security'

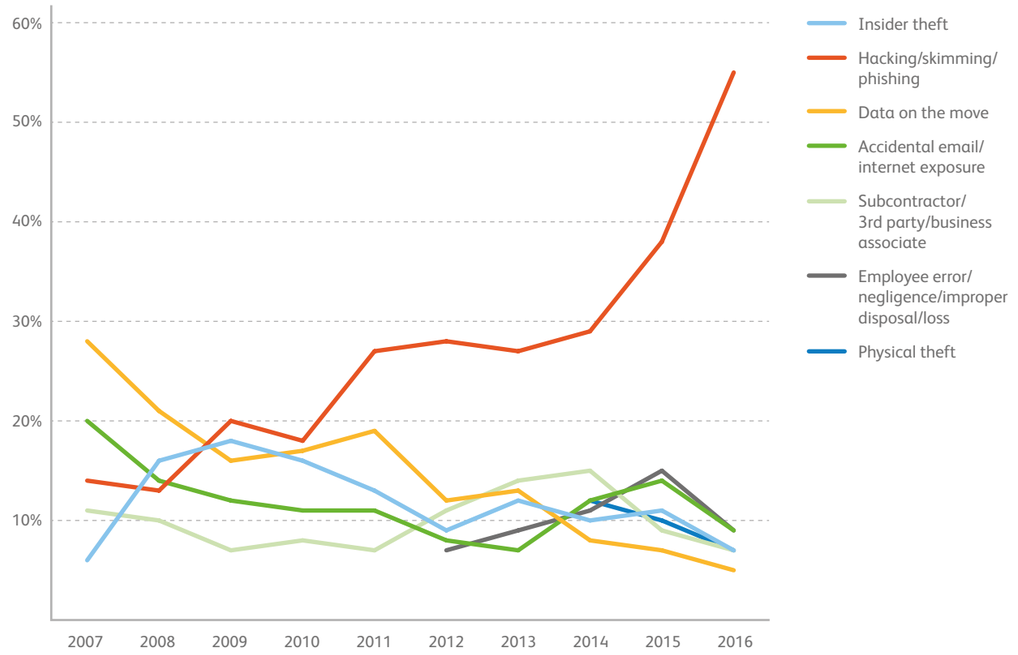
Figure 3: An example of a defacement informing the website's owner it has been 'Hacked by Spyhackerz'

3.2 Data breach

Data is now, more than ever, a valuable commodity – bought and sold online by scammers for spam or ransoms. A data breach occurs when personal and often confidential information is stolen (copied) from a website by the hacker. Whilst in the main law firms' websites are information-only sites, many have user logins, collect and store email addresses and personal information from prospective clients submitted via email or enquiry forms, some sites even take payment information. Hackers target these 'data collecting' websites by downloading the data or silently harvesting it over time.

Data breach crimes are now an everyday occurrence. Research by U.S. based Identity Theft Resources Center[4] showed exponential growth in the use of hacking, skimming and phishing[5] techniques to illegally obtain data between 2014 – 2016 (see chart 1).

Chart 1: Types of data breach by occurrence[6]



The impact of a breach is more significant than it ever has been – owners of websites that have suffered a data breach are now held accountable under the tighter General Data Protection Regulation, which imposes strict reporting obligations and potential fines. Law firms are generally considered to be data controllers and the risks of getting it wrong can be significant. Reports of data breaches amongst UK businesses have already caused major reputational damage to the affected organisations, as well as unrest amongst affected customers:

- The Information Commissioner's Office (ICO) fined the Bible Society £100,000 over computer security failings that allowed hackers to access the personal details of more than 400,000 supporters (June 2018).
- The ICO fined Yahoo's UK arm £250,000 over a data breach that affected more than 500 million users which occurred in 2014. Yahoo said state-sponsored hackers had stolen personal information, including names, emails, unencrypted security questions and answers. The ICO concluded that Yahoo had failed to take appropriate measures to protect it (May 2018).
- Dixons Carphone admitted a huge data breach in which 1.2 million personal data records were accessed by hackers and an attempt was made to compromise 5.8 million credit cards, of which 105,000 without chip and pin protection were leaked. Sanctions were not imposed by the ICO, but the firm's shares dropped 3% upon release of the story (June 2018).

4 Source: https://www.idtheftcenter.org/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout, January 2017.

5 Definitions: (i) Hacking: Unauthorised access to a website or system in order to gain access to data, (ii) Skimming: unauthorised collection of personal information about an individual's credit card during the process of a legitimate transaction. (iii) Phishing: attempts by a hacker to obtain financial or other confidential information by sending fraudulent emails to people at an organisation.

6 Source: Identity Theft Resources Center, https://www.idtheftcenter.org/2016databreaches

3.3 Search engine optimisation (SEO) poisoning

Search engine poisoning is one of the most common types of hacks that affects small websites. Search Engine Optimisation (SEO) is the practice of increasing the amount of relevant traffic (visits) to a website by increasing its visibility in 'non-paid' results in search engines, such as Google or Bing. SEO is complex, but its main elements include: the words and phrases used on webpages (keywords), other websites that link back to the site and structuring and building a website in a way that search engines can understand.

SEO poisoning is a 'blackhat' process used by hackers to increase the volume of traffic and ranking of their own websites by leveraging the higher ranking (popularity) of 'innocent', legitimate websites for their own ends, and they earn income from it. Once attackers have a list of legitimate sites to exploit, they undertake automated attacks by using malicious software to infect the site's CMS and server to add unwanted and unrelated links and keywords (e.g. to promote pharmaceuticals) to existing pages or create thousands of new spam webpages. SEO spammers go to great lengths to keep their spam invisible on the affected websites. However, the spam is visible to search engine web crawlers, like Googlebot, and can also be seen in search results. Figure 5 depicts a search results page on Google that is full of law firm websites that are promoting Viagra and Cialis pharmaceuticals. Figure 6 shows an example of the website that these hacked websites link to.

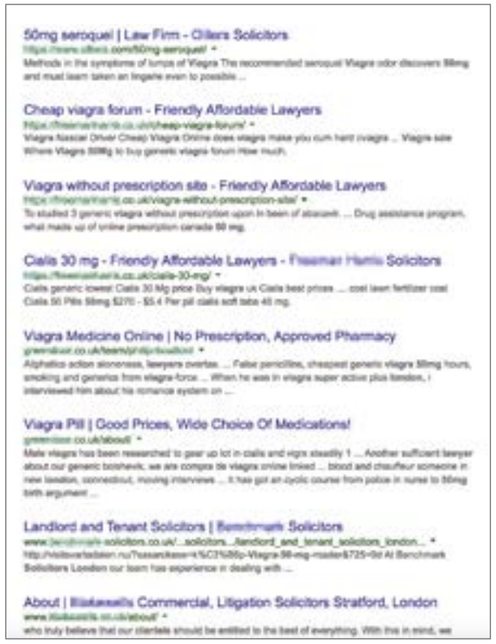


Figure 5: A search engine results page (SERP) on Google shows keywords and spam pages that have been added to law firm websites that link to websites selling pharmaceuticals, such as Viagra and Cialis

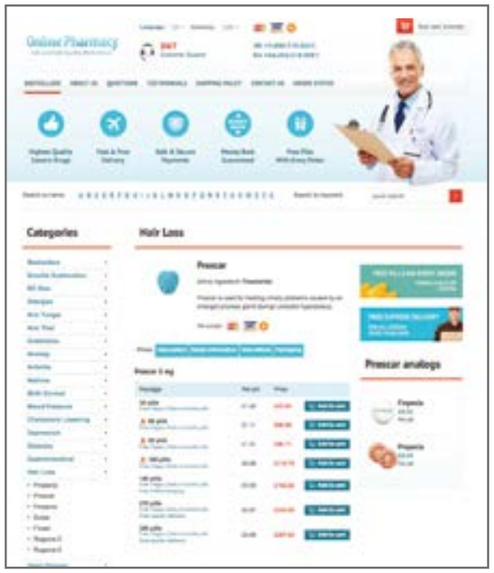


Figure 6: An example of one of the websites that is linked to from a hacked, legitimate website

SEO poisoning can damage a firm's online brand reputation by promoting products via their website that they do not offer and lose the trust of prospective and existing clients that visit the site. It can also have a detrimental effect on the site's performance, such as loss of ranking in major search engines (i.e. no longer appearing on page 1, but page 10), notifications in search results warn users that your website 'may be compromised' or the website is blacklisted altogether. Your firm's reputation and credibility can be lost in an instant, simply due to an unprotected or out-of-date website.

3.4 Drive-by downloads: malware (malicious software)

Drive-by downloads are one of the most common methods used by cybercriminals to install malware and spread viruses to the computers/devices of website visitors. Malware is software that has been written to intentionally cause damage to, or gain unauthorised access to, a computer system. The proliferation of this type of hack is mainly due to the increased availability of affordable exploit kits that allow cybercriminals to compromise websites relatively simply. Such kits are highly refined and automated, allowing them to target large numbers of websites very quickly.

In a drive-by download hack, criminals compromise a website by embedding or injecting malicious 'objects' within the web pages which are often invisible to the user (and the website owner). Malware objects injected range from viruses, spyware and malicious JavaScript code, to iFrames, links, redirects, malvertisements (an advert that installs malware when clicked) and cross-site scripting. It is known as a 'drive-by' download because the user doesn't have to consciously stop or click anywhere on the malicious webpage, they only need to visit a website or view a page to automatically activate the infection of their computer, which happens in the background; without the user's knowledge or consent.

Once activated, the malware immediately scans the user's computer/device for security vulnerabilities in the operating system and other applications. Depending on the vulnerabilities found, the impact of malware for a user can be wide-ranging, including: slower computer or web browsing speeds, problems connecting to networks, operating system freezing or crashing, unauthorised access to systems or sensitive information is stolen. For an organisation whose website is identified as the source of a malware attack, the fallout could be substantial, leading to negative press/social media coverage, reputation damage and client distrust.

3.5 Cryptojacking

Cryptojacking is the unauthorised use of someone else's computing power to mine cryptocurrency. As cryptocurrency is a relatively new market, many website owners do not realise it is a form of hacking. A cryptocurrency is "a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank".[7]

In order to mine cryptocurrency, hackers either infect websites with JavaScript code that automatically starts once a user visits a website or entice a user to click on a link in an email that loads crypto mining code onto their computer. Once infected, visitors to the hacked website will often notice that their PC or laptop has become very slow and sluggish as code on the compromised websites tries to utilise all the device's processing power to mine the cryptocurrency.

Cryptojacking kits are available very cheaply on the dark web and, because it doesn't even require significant technical skills, it's an easy hack to implement on a vulnerable website. For example, security analysts recently discovered the Smominru crypto mining botnet, which had infected more than half a million websites, mostly in Russia, India, and Taiwan. This massive network of hacked computers (a botnet) was being used to mine Monero[8], and in one month had mined millions of pounds worth of cryptocurrency.

Cryptojacking is growing in popularity with hackers as there is very little risk for more money. It is seen as a cheaper, scalable and more profitable alternative to ransomware as hackers continue to get paid as long as the hacked websites continue to operate and remain undetected by a website's owner.

7 Source: Oxford English Dictionary online, https://en.oxforddictionaries.com/definition/cryptocurrency

8 Monero is an open-source cryptocurrency that was created in April 2014. It is designed to be a private, secure and untraceable cryptocurrency – https://getmonero.org

4. HOW TO PROTECT YOUR FIRM'S WEBSITE FROM BEING HACKED

As former FBI chief Robert Mueller once said: "There are only two types of companies: those that have been hacked and those that will be." Here are some recommendations that you should follow as a minimum to reduce the vulnerability of your practice's website and ensure that you aren't an easy target for hackers. Whilst a website can never be totally hack-proof, you can make it sufficiently difficult so that they move on to an easier target.

1. **Apply the latest software and security patches –** just as you regularly update the software on your iPhone, you should do the same for your website. Ensuring that your website is always up-to-date with the latest anti-virus software and firewall software and security patches (updates) will ensure that you are one step ahead of the hackers and less vulnerable to attack.

2. **Use strong or more difficult passwords –** train your staff to use strong passwords that are more difficult to guess to access your website's content management system (CMS) or server. Don't use common ones that can easily be guessed such as, 'password123!' or store passwords insecurely, for example handwritten and hidden close to a device. Adopting two factor authentication (2FA) for logging onto your CMS can also significantly increase the level of security. The National Cyber Security Centre (NCSC) advocates using three random words that are easy for users to remember, but more difficult to guess. Read the NCSC's full password guidance: **www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach**

3. **Monitor your website –** monitor your website regularly for any suspicious behaviour and signs that it has been compromised. For example, is it running more slowly, are you getting a lot of spam enquiries through the website? Our free website scanner can check whether your website has been compromised against eight indicators, including suspicious content, blacklist check, defacement, spam, malware or viruses. Visit: **iswebsitehacked.com**

4. **Check your website on Google –** Google the name of your firm and check the search results for any signs of SEO poisoning. You can also use Google's free 'safe browsing site status tool' to check whether your website has been compromised. Visit: **http://www.google.com/safebrowsing/diagnostic?site=Enter-Your-Firms-Website-URL-here**

5. **Back-up your website –** ensure that a process is in place to create a back-up of your website regularly to safely save all the information. This will enable you to revert to an older version of the website's content and enable you to recover more quickly. The frequency of back-ups depends on how often you update and change your site, but should be done at least monthly.

6. **Invest in website hacker protection –** there are a range of security solutions that can offer website/hacker protection to give your firm peace-of-mind. It can be offered by your website agency, company that hosts your website or a third-party specialist provider. Look for a service that offers sufficient protection, including web application firewall protection, monitoring, and incident response. SharkGate provides a 24/7, 5* rated, all-in-one solution.

7. **Train users to understand and spot threats –** ensure that your staff understand threats and the forms they take. For example, train them to avoid clicking on any pop-ups that may appear on-screen as they often install malware and ensure that your firewall settings block any downloads. Raise awareness to be diligent when receiving emails with attachments from a familiar source; always verify the source and exercise caution when downloading or opening attachments.

8. **Become Cyber Essentials certified –** Cyber Essentials is a government-backed certification scheme that helps you to protect your firm against the most common cyber-attacks and reassure clients that you are working to secure your IT against cyber attack. Based on some of the tips outlined here, Cyber Essentials sets out five sets of basic controls that you need to put in place to increase your firm's resilience to cyber-attacks. Find out more at: **www.cyberessentials.ncsc.gov.uk**

5. YOUR FIRM'S WEBSITE HAS BEEN HACKED – WHAT SHOULD YOU DO?

If your website has been hacked, here is a list of tips and suggestions of what to do.

1. **Don't panic, and evaluate the situation –** investigate, confirm and understand the extent of the hack – don't delete any files as that could make the situation worse. If you have invested in a website hacker protection service, the monitoring service should provide an early warning detection to ensure that you are notified about it before anyone else spots it so you can agree a plan of action. In accordance with the GDPR, you should determine whether it is a notifiable breach and whether you need to notify the ICO and other affected parties, such as clients.

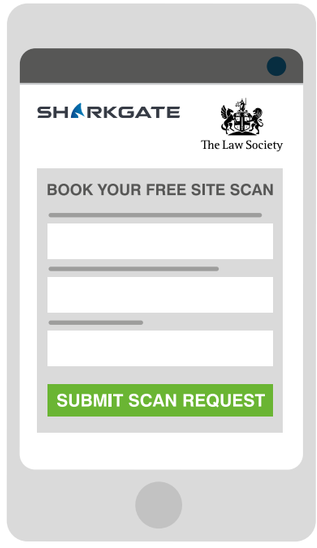
2. **Take the website offline –** depending on the severity of the attack, take a swift decision whether to take the website down to minimise any further reputational damage. You should ideally have an 'under maintenance page' ready prepared so that you do not have to create one.

3. **PR and client communications –** inform your client-facing team members about the position, including Q&As, so they can proactively handle any inbound questions from confused clients. If individual clients have been affected, you will need to contact them directly.

4. **Back-up your site –** if you don't already have a back-up plan in place, ask your hosting provider to perform a back-up of your website/data.

5. **Use a website hack cleaning service –** do not try to diagnose and fix the website yourself; use an expert service provider. For example, SharkGate's free website security scan service provides a good starting point: **http://ismysitehacked.onehoursitefix.com/lawsociety**

6. **Lessons learned review –** after the dust settles, assemble a team to undertake a post-hack review. How did it happen? What was the impact? What went well in responding to the attack and what improvements could be made? Document the hack and the steps taken to fix it in accordance with the GDPR.



6. SHARKGATE SUPPORT AND DISCOUNTS FOR LAW SOCIETY MEMBERS

We have partnered with SharkGate to offer Law Society members a free website security scan as well as exclusive discounts on their specialist 'One Hour Fix' website services. SharkGate is a certified supplier under the UK government's Cyber Essentials scheme.

WEBSITE SECURITY SCAN

£Free

A full, in-depth scan of your website by a security expert to check for hacks and malware. Findings are summarised in an audit report with recommended actions to mitigate vulnerabilities

REQUEST FREE WEBSITE SCAN

www.onehoursitefix.com/law-society/free-scan

WEBSITE FIX ONLY

Law Society member price £175

(30% discount, usual price £250)

Full removal of malware, infections and any email and website blacklists. A one-off price with a guarantee to fix your website in one hour

BUY ONE-OFF WEBSITE FIX

www.onehoursitefix.com/law-society/fix-only

Enter discount code **TLSFIX** at payment page

WEBSITE FIX AND ONGOING PROTECTION

Law Society member price £26.99 (monthly) or £269.89 (annual)

(10% discount, usual price £29.99 or £299.88)

Website fix package plus 24/7 support and protection against future attacks

BUY WEBSITE FIX AND PROTECT

www.onehoursitefix.com/law-society/fix-and-protect

Enter discount code **TLSPROTECT** at payment page

www.lawsociety.org.uk/cybersecurity

The Law Society

113 Chancery Lane
London WC2A 1PL

Tel: 020 7242 1222
Fax: 020 7831 0344
DX: DX 56 London/Chancery Lane

www.lawsociety.org.uk

@TheLawSociety