First published as part of the email campaigns of 2014 and 2019 and now codified into a guidance note 2023.

PROFiT
Prevention of Fraud in Trade

INDUSTRY GUIDANCE NOTE

IMPROVING WEBSITE SECURITY

Every month cyber criminals register around 1.4 million phishing websites many of which are spoofed, cloned, or copycat websites designed to be like legitimate websites.[1]

Not only does this enable the criminals to commit fraud and cause legitimate organisations reputational damage, but it can also be devastating to operational effectiveness.

This GUIDANCE NOTE written in easy-to-understand language will help to secure your website and improve resilience against compromise.

WHAT'S IN THIS GUIDANCE NOTE

Website Security, The Basics

Let's start with some basic security measures that make it harder for criminals to attack your website. This is by no means a comprehensive list but will help you to defend your website from attack.

1. **OBTAIN A VALID SSL CERTIFICATE**

   A Secure Sockets Layer (SSL) certificate is coding that validates the identity of a website and encrypts data, including logins, sent between the website and its users.

   The SSL certificate is sometimes called a 'digital handshake' because during the process of initiating contact the server presents its SSL certificate to the client as proof of its identity. Whilst an SSL certificate helps keep data safe, they do not in themselves, prevent hacking.

   Most organisations now have a valid SSL Certificate in place, but if you have not yet managed to get one you should do so now. This will enable you to move from **http** to **https**, which gives confidence to others, and helps your position in search results.

   An SSL Certificate can be obtained in several ways. A simple option for small or medium sized organisations is to use a Certificate Authority (CA) such as **Cloudflare** or **Let's Encrypt**. Cloudflare includes free SSL certificates with its service plans Let's Encrypt is a not-for-profit Certificate Authority providing certificates to millions for free.

2. **INSTALL A WEB APPLICATION FIREWALL**

   Sitting between the web application and the internet the Web Application Firewall (WAF) separates the server from the internet. It filters incoming and outgoing traffic to protect web applications from some types of attack.

   Every website needs to have a WAF in place to keep it safe from certain types of attack including Distributed Denial of Service (DDOS), Cross-Site Scripting (XSS), and SQL injections.

   Some Cloud based services offer Web Application Firewalls as part of their standard packages.

3. **MAKE USE OF ANTI-MALWARE SOFTWARE**

   Anti-malware (malicious software) software tools protect websites and are essential because they monitor web traffic and block suspicious activity.

   Designed to protect websites from malware, phishing, and ransomware attacks, anti-malware software scans websites for malware and malicious code and keeps site visitors safe from harm.

   Some Cloud based services offer Anti Malware Software as part of their standard packages.

4. **MAKE REGULAR BACK-UPS**

   Running regular back-ups of websites is crucial for data protection and business continuity. Websites store a lot of critical data and files that are essential to the website's operation.

   Without back-ups, data loss is much more likely to happen. Back-ups will help your organisation get the website back up and running whether the website suffers a hardware failure, enabling organisations to reverse problems caused by software updates, ransomware attack, software issues, accidental deletion, or cyber-attack.

5. **KEEP ALL SOFTWARE UPDATED**

   Software updates ensure that your systems and applications are secure and functioning optimally.

[1] Source: ZDNet https://www.zdnet.com/article/1-4-million-phishing-websites-are-created-every-month-heres-who-the-scammers-are-pretending-to-be/

Updates often include fixes for known vulnerabilities in the software that otherwise could let in malware or be exploited by hackers.

Malware Some Facts

Several organisations specialise in analysing and reporting on malware activity whose reports help to understand the threat landscape. A few statistics are listed below.

Worldwide there were approximately **5.6 billion malware attacks** in 2020. (**Source:** SonicWall, Cyber Threat Report 2021) https://www.sonicwall.com/2022-cyber-threat-report/sonicwall-cyber-threat-report-thank-you/?TR_name=asdas

During 2020 there were **4.8 Trillion intrusion attempts**. (**Source:** SonicWall, Cyber Threat Report 2021) https://www.sonicwall.com/2022-cyber-threat-report/sonicwall-cyber-threat-report-thank-you/?TR_name=asdas

3.849 million browser warnings were shown to **users trying to enter sites deemed dangerous** by Safe Browsing between 1 January and 7 August 2022**.** (**Source:** Google, Transparency Report 2022) https://transparencyreport.google.com/safe-browsing/overview?hl=en_GB&unsafe=dataset:1;series:malwareDetected,phishingDetected;start:1148194800000;end:1612080000000&lu=unsafe

Approximately **236.1 million ransomware attacks** worldwide occurred in the first half of 2022. (**Source:** Statista) https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

15.3 billion spam emails are estimated to pass through the internet every day. (**Source:** Slashnext.com, The State of Phishing Report 2022) https://www.slashnext.com/the-state-of-phishing-2022/

6. **MAKE ACCESS UNCRACKABLE**

Traditionally passwords are used to keep access to systems and accounts secure. In an ever-escalating cycle, passwords are becoming more and more complex as criminals find ways to counter the latest standards**.**

Due to the increasing need for password complexity, PROFiT continues to urge all organisations to move away from traditional passwords and replace them wherever possible with either Multi Factor or Biometric Authentication.

Advice on password policy is available from the National Cyber Security Centre which recognises the proliferation and increasing demands on people's ability to retain complex passwords: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

Multi Factor Authentication (MFA) is rapidly replacing passwords for accessing systems and applications a move we continue to endorse.

MFA involves a user registering a mobile device and when they require access to an online secured account or application a unique, one-time, passcode is sent to the registered device which the user must enter into an access gateway box before they are allowed into the application.

The National Cyber Security Centre issues advice on MFA: https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services

7. **ENCRYPT PERSONAL & FINANCIAL DATA**

Despite organisations taking security measures a security breach can sometimes occur and systems become compromised.

As custodians of personal and financial data that users entrust your organisation with, it is incumbent upon you to adopt robust measures to secure all such information.

All personal and financial data should be encrypted so that if your security is violated the data is still protected. This is due to the harm a data breach can cause for the individuals concerned.

Some Cloud based services offer encryption of data as part of their standard packages.

The Effect of Domain Scamming

Criminals use look-a-like domains to trick internet users for a variety of different reasons, including financial, informational, and sometimes both.

Scamming: A look-a-like domain could be set-up to create a website like a legitimate organisation's website with the goal of scamming customers or employees. For example, they could create a fake bank website tricking people in to entering their account details, and then use that information to commit fraud.

Phishing: A look-a-like domain could be set-up to create a website with a fake login page aping a legitimate website, to trick people into entering their login details. The attacker could then use those details to access personal accounts like emails, bank accounts, work accounts and contacts.

Alternatively, A look-a-like domain could be set-up to send phishing emails without bothering to set-up a website.

Malware distribution: A bogus domain could be used to create a website like a legitimate download page for a popular software program or app, but which contains malware. When people download and install the program, they inadvertently install the malware on their system.

Reputation damage: A domain name could be created similar to a legitimate organisations' domain name, to damage the reputation of the victim brand. For example, if someone sets up a fake domain like a well-known brand and uses it to spread false information or engage in illegal activities, it could harm the victim brand's reputation.

Domain Intelligence

Ongoing visibility of newly registered and existing domain registrations helps to proactively identify unauthorized domains. Large organisations have multiple sources that their security teams use for domain detection, but these are probably beyond a small or medium sized organisation:

- Top Level Domain (TLD) zone files list every active, registered domain for that specific TLD created daily.

- Secure Sockets Layer (SSL) certificate transparency logs present domains, subdomains, etc. for new SSL certificates that are issued.
- Domain Name System (DNS) traffic contains domain names being queried and can be monitored for new domains.
- DNS queries can be performed using multiple variations of your domain name to check for hostile registrations.

Domain Intelligence Methods For Everyone

There are several tools that anyone can use to monitor the internet for domain names like yours. A few are listed here.

Dnstwist is a free tool that applies random permutations to your domain and identifies good candidates for defensive registration and can identify lookalike domains that have already been registered. https://dnstwist.it/

PhishLabs has a tool that provides ongoing visibility of newly registered and existing domain registrations, which is necessary to proactively identify unauthorized domains.

PhishLabs tool also sources and develops domain intelligence to identify potential threats and compile sufficient evidence for takedown. https://www.phishlabs.com/blog/how-to-detect-look-alike-domain-registrations/

KnowB4.com is a free tool called Domain Doppelganger to enable you to monitor for look-a-like domain registrations. https://www.knowbe4.com/domain-doppelganger

Securi SiteCheck is a free scanner which identifies if your site has been hacked. https://sitecheck.sucuri.net/

NB Some of these tools do not work with Amazon Web Services (AWS) cloud hosting.

Company Website Impersonation

Malicious domains are behind a wide variety of cyber-attacks capable of undermining a brand's credibility. Spoofed domains are simple to create and a major source of malicious email campaigns and phishing sites. To detect and disrupt domain threats targeting your organisation, you need to establish processes for self-defence.

There are a massive number of suspicious domains across the threat landscape and criminals are increasingly enhancing look-a-like domains to promote their trustworthiness. Among the methods used to evade detection is the growing use of SSL certificates for phishing sites. In one quarter almost 80% of sites were recorded abusing this security feature.
https://info.phishlabs.com/blog/apwg-ssl-certificates-no-longer-indication-of-safe-browsing

To effectively protect against the high volume and growing sophistication of suspicious domains, organisations need to develop their own domain intelligence to identify potential threats and gather sufficient evidence for takedown.

Look-A-Like Websites

It has long been the case that people will set up a website copying a successful brand and manipulate search results to steal customers and commit fraud.

In the past the only way to deal with this was to pay an organisation such as Nominet to look at it or report it to Action Fraud and hope that they dealt with it. This is becoming less of an issue in recent years as criminals migrate to the less regulated realm of Social Media.

The Industry Intelligence Hub gives free access to the Global Cyber Alliance **Domain Trust** system which enables organisations to report and search for look-a-like and brand spoofing websites.

This will potentially give you the capability to stop someone using and operating a look-a-like website and impersonating the legitimate company website or brand with criminal intent.

Preventing Browser Hijacking

Follow these safety tips to keep your devices free from browser (search engine) hijackers:

- Do not click on suspicious links, including those in emails, text messages, or pop-ups.
- Keep your operating system and browser patches (software updates) up to date. Search engine hijackers can take advantage of operating systems and browser coding issues. Always install software updates to ensure your security systems are operating safely and efficiently.
- Install antivirus software to monitor for hijackers and malware.
- Be cautious when downloading software read licensing agreements and terms and conditions before downloading software to check that it's not bundled with a browser hijacker.
- Don't run freeware programs that unload unexpected software after they've been installed.

Website Account Takeover

In the first instant it is better to secure your website than to try and get it back once it is hijacked. This section explains how to reduce the risk of a website being hijacked to impersonate a legitimate organisation.

1. **USE A DIFFERENT EMAIL ADDRESS TO THE DOMAIN**
   ICANN advises that when you register your domain name, you will be asked to provide contact information, including your email address. This information goes into the WHOIS record for your domain name, which might be viewed publicly.

   It is best practice to use an email address that is NOT associated with the domain name you are registering. This means that if you have a website, for example; www.example.co.uk you should not use an email associated with www.example.co.uk in the contact information.

   ICANN explain that if your domain name is hijacked by someone who has gained access to your account with the Registrar, that person will probably alter the WHOIS information to remove you as the registered holder of the domain name.

If you used an email address that is not associated with your domain name in WHOIS, you will be able to provide that email address as evidence to the Registrar that you were the registered holder of the domain name before it was altered by unauthorized access to your account.

2. CREATE STRONG AND UNIQUE PASSWORDS

ICANN recommends that you protect your domain name from cybercriminals by creating a unique, strong password. Online services are compromised frequently, making usernames and passwords available to criminals that you provide for other accounts.

Our advice remains that where possible move to Multi Factor Authentication which will make it more difficult for you access protocols to be compromised. If you are unable to do so you can avoid this type of compromise by creating a strong password that you use exclusively for your domain name account: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

Responsibility for the security of your domain name rests with you so never give anyone the login information to your online account. This includes web hosting providers and designers as well as family, friends, and colleagues.

ICANN recommend that you never list website designers, hosting providers, or any other third parties as the Registrant(s) of your domain name. Use of

If Your Website Is Hacked

If your website is hacked, you can take the following steps to take back control:

- Ask your hosting provider for details about the hack including how they believe the site was hacked.
- Request that your hosting provider removes all unauthorised content added to your website.
- Resolve site warnings in **Google Search Central** (formerly Webmaster) Tools: https://developers.google.com/search and resubmit your site for Google's review once the hack has been resolved.
- Change appropriate passwords and review who has access.
- Backup the whole of your website.
- Trace your actions back to try and find the hackers access point.
- Investigate recent breaches online to gather more information.
- Report hacks to **Action Fraud**. http://www.actionfraud.police.uk

3. APPLY A TRANSFER LOCK

Website owners can request that the Registrar puts a *transfer lock* on their domain name. Putting a lock on your domain name is not guaranteed to prevent an unauthorized transfer or hijacking of your domain name, but it is another layer of security.

Find Out If Your Domain Has A Transfer Lock

To check if your domain is unlocked, you can follow the instructions provided by your domain Registrar. Here are some tips:

1. Sign into your domain Registrar's website.
2. Navigate to the domain management section.
3. Look for an option to manage domain locks or transfer locks.
4. If the domain is locked, you will need to unlock it before transferring it to another Registrar.

Here are some links that might help you with locking/unlocking your domain:

- For **GoDaddy** domains, you can follow the instructions provided in: https://www.godaddy.com/help/unlock-or-lock-my-domain-410.
- For **Google** domains, you can follow the instructions provided in: https://support.google.com/domains/answer/3251178?hl=en.
- For other domains, you can refer to the instructions provided in: https://www.domain.com/blog/transferring-domain-name-ownership-everything-you-need-to-know/, and https://monsterhost.com/locked-domains-and-how-to-unlock-domains/.

There is no standard method for a Registrar to implement a transfer lock. Some require two-factor authentication to remove the lock; others require authorization from the Registrant. Ask your Registrar about transfer lock policies.

4. DOMAIN HAS BEEN HIJACKED

If your domain name was transferred to a new Registrar or Registrant or if your account information was modified without your consent, contact your Registrar immediately.

Contact your Registrar as soon as you become aware to prevent your domain name being transferred again and again making it harder to reclaim your domain.

There are specific rules designed to protect you that govern the transfer of domains. A Registrar may only initiate a transfer if it has obtained a completed **Form of Authorization** (FOA) from either the Registrant or the administrative contact for the domain. https://icannwiki.org/FOA.

If your domain has been transferred without your authorisation, ask your Registrar to request a copy of the form used for authorizing the transfer.

The Registrar that the domain name was transferred to must be able to produce a copy of FOA when it is requested. Failure to do so is grounds for reversal of a transfer if a complaint is filed under the **Transfer Dispute Resolution Policy**. https://icannwiki.org/Registrar_Transfer_Dispute_Resolution_Policy

If you've contacted your Registrar and they are unable or unwilling to assist you in recovering your domain, submit an **Unauthorized Transfer Complaint** to **ICANN**. **ICANN** will review your situation to see if they can assist you in recovering your domain.

However, **ICANN** does not have contractual authority to require a Registrar to transfer a domain name back to a different Registrar or Registrant, even where a transfer was through an unauthorized access to your email account or login credentials.

Website Account Cloning

One method of impersonating a company is to clone the website. Cloning is when an unauthorised person scrapes the content and publishes it on a similar sounding website. The following will help reduce the risk of cloning by criminals impersonating your organisation.

1. **SECURE YOUR CODE**

   Ask your developer to make sure that they have added security features into the design to protect your site from potential theft, added encryption, and layers of protection to keep your website safe.

   Additionally, your web developer can disable the copy-paste function by adding script in your source code to prevent hackers from copying your content.

2. **COPYRIGHT YOUR WEBSITE PAGES**

   In the UK all works (including software, web content and databases) are given copyright protection automatically but there is no register of copyright works. UK copyrighted works can gain a measure of protection automatically under the Berne convention.

   To give your online content enforceable protection in the US you should register your website's copyright with the **US Copyright Office**: https://www.copyright.gov. Non-US citizens can register at the US Copyright Office where protection lasts longer than in the UK. To register a copyright, you must either be the author of the content or have rights granted by the author.

   Google Alerts enable you to identify unauthorised use of your content. Copy and paste your brand and/or a distinctive portion of your website text into the search so that Google can email you the results of the search: https://www.google.com/alerts, You can adjust the settings in Google Alerts to notify you on a daily, weekly, or real-time basis.

   In addition to Google Alerts, there are several other online tools to help keep your online content safe and secure. **Copy Scape** https://www.copyscape.com is one free tool that enables you to check for your text content in unauthorised locations on the internet.

   Travel industry affiliates of PROFiT can use the GCA **Domain Trust** tool which allows users to report or search the database of reported registered malicious domains. Try searching for your brand to test it out.

Online Safety Act 2023

The Online Safety Act enacted 26 October 2023 contains several new internet related duties on service providers.

The new duty for online platforms requires that they act against illegal or harmful content on their platforms. Platforms failing this duty could be liable to **OFCOM** fines of up to £18 million or 10% of their annual turnover, whichever is higher.

The Act includes controls on '**paid-for**' advertising as well as '**fraud**' provisions. '**Paid-For advertising**' is defined in **section 236** as:

"An advertisement is a "paid-for advertisement" in relation to an internet service if—

(a) the provider of the service receives any consideration (monetary or non-monetary) for the advertisement (whether directly from the advertiser or indirectly from another person), and

(b) the placement of the advertisement is determined by systems or processes that are agreed between the parties entering into the contract relating to the advertisement."

Fraud offences in scope are listed in **section 40**:

Provisions of the **Financial Services and Markets Act 2000**

- contravention of prohibition on carrying on regulated activity unless authorised or exempt (s23),
- false claims to be authorised or exempt (s24),
- contravention of restrictions on financial promotion (s25).

Provisions of the **Fraud Act 2006**

- fraud by false representation (s2)
- fraud by abuse of position (s4)
- making or supplying articles for use in frauds (s.7)
- participating in fraudulent business carried on by sole trader etc. (s.9).

Provisions of the **Financial Services Act 2012**

- misleading statements (s89)
- misleading impressions (s90).

(**Source**: legislation.gov.uk https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted)

According to a 2022 press release: *"fraudulent paid-for adverts on social media and search engines are in scope, whether they are controlled by the platform itself or an advertising intermediary."*

"These companies will need to put in place proportionate systems and processes to prevent (or minimise in the case of search engines) the publication and/or hosting of fraudulent advertising on their service and remove it when they are made aware of it."

(**Source**: .gov.uk, 8 March 2022 https://www.gov.uk/government/news/major-law-changes-to-protect-people-from-scam-adverts-online)

OFCOM will now produce codes of practice to inform everyone how these provisions will work in practice.

3. **IF DOMAIN HAS BEEN CLONED**

   Search the cloned site for any contact information of the user that has copied your content.

   If you are unable to locate the person responsible for copying your content, contact the website hosting service for the offending website. To find this information, go to https://www.whoishostingthis.com, type in the domain address for the cloned site, and you should be served the web hosting service responsible for the offending website.

The web hosting services may take down an entire site that has posted your content if you can prove you have been the victim of cloning. The web hosting service will provide you with a form to fill out. Submit it with your evidence to prove that you are the rightful owner of the content or site.

In the United States there exists the **Digital Millennium Copyright Act**. This law created to updated copyright laws to better regulate digital material. Content owners have an absolute right to request that unauthorised material be taken down if the applicant's content is found online without permission. To learn more about DMCA takedown, please see: https://www.dmca.com/faq/What-is-a-DMCA-Takedown.

Preventing Sub Domain Takeover

Here are some steps you can take to prevent subdomain takeover:

1. **Identify dangling DNS entries**: To identify DNS entries associated with your website that might be dangling: https://learn.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover#Remediate%20dangling%20DNS%20entries
2. **Remediate dangling DNS entries**: Once you have identified the dangling DNS entries, remove them from your DNS zone. https://learn.microsoft.com/en-us/azure/dns/dns-alias
3. **Use Azure DNS alias records and Azure App Service's custom domain verification**: This can help prevent subdomain takeovers by enabling you to verify that the custom domain belongs to your organisation. https://learn.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-domain?tabs=root%2Cazurecli

Sub Domain Exploitation

Sub Domains are used by website developers to make navigation around the site easier. However, sub domains remain live even when the purpose for their creation no longer exists, they also can exist outside of the main webpage security hierarchy.

Subdomain takeover is a security threat that can occur when a DNS record points to an expired sub domain enabling nefarious actors to redirect traffic intended for an organisation's domain to a site performing malicious activity including redirecting payments to a criminal's bank account.

Domain Name System (DNS) records point domain names to other domains, when a domain is **abandoned**, that DNS record is said to be 'dangling' and is now called a Dangling DNS record. Because it is abandoned, this domain can be easily hijacked by threat actors and used to gain initial access into a network.

Funded by organisations like yours we carry out research, analysis, disrupt crime and provide free best practice and guidance. Find out how you can get involved with PROFiT and help to make your organisation more resilient against crime.

Email contactus@profit.uk.com for more information.

Help & Information

Cyberattack Assistance

Action Fraud can advise you if your website has been breached and may be able to render free assistance. They cannot get involved in brand matters.
Action Fraud: www.actionfraud.police.uk
Or call **0300 123 2040**

Domain Intelligence

There are many organisations who offer domain intelligence services on the internet. This is a small sample.
Dnstwist: www.dntwist.it
GCA Domain Trust: contactus@profit.uk.com
PhishLabs: www.phishlabs.com
KnowB4.com: www.knowb4.com
SecuriSiteCheck: https://sitecheck.securi.net

Free Apps & Information

The Global Cyber Alliance have a wide range of free to access cybersecurity apps for small and medium sized organisations.
GCA: https://gcatoolkit.org/smallbusiness

NCSC's website has plenty of useful information on cyber security.
NCSC: www.ncsc.gov.uk

Online Security Bulletins

Many tech companies issue security patching updates. Here are some key ones.
Google: https://cloud.google.com/support/bulletins
and
https://cloud.google.com/anthos/docs/concepts/security-patching
Microsoft: https://msrc.microsoft.com/update-guide
Apple: https://support.apple.com/en-us/HT201222

Transfer Locking

A transfer lock does not guarantee that your website won't be hijacked but it does add an extra level of security.
GoDaddy: https://www.godaddy.com/help/unlock-or-lock-my-domain-410

Google:
https://support.google.com/domains/answer/3251178?hl=en

Other Domains:
https://www.domain.com/blog/transferring-domain-name-ownership-everything-you-need-to-know/
and
https://monsterhost.com/locked-domains-and-how-to-unlock-domains/

Website Cloning

Domain Trust: contactus@profit.uk.com
Google Alerts: https://www.google.com/alerts
US Copyright Office: https://www.copyright.gov
DCMA Takedown Service: https://www.dmca.com/faq/What-is-a-DMCA-Takedown

Website Domains Ownership Disputes & Policies

ICANN oversees the operation of the internet. They set policies all domain name suppliers/services must adhere to.
ICANN: https://www.icann.org/
and
https://icannwiki.org/FOA
and
https://icannwiki.org/Registrar_Transfer_Dispute_Resolution_Policy

Website Warnings Resolution

https://developers.google.com/search