PROFiT
Prevention of Fraud in Travel

THE COUNTER FRAUD CAMPAIGN 2019

PART 14: PROTECTING WEBSITES

Prevention of Fraud in Travel (PROFiT) and the Fraud Intelligence Network (FIN) are working with the City of London Police to reduce fraud in the travel industry. In PART 14 we look at how you can take measures to protect your domain name and website to prevent it being used by criminals.

PROFiT is the only official travel industry counter fraud body. We work on your behalf to carry out analysis and research, disseminate best practice and disrupt crime.

Find out how you can join the fight against crime. Contact via: contactus@profit.uk.com

WHY YOU NEED TO SECURE YOUR DOMAIN NAME AND WEBSITE

1.0 We have seen in the last two issues of the email campaign how criminals, including some employees, have been found to clone websites or copy the branding and imagery to launch their own pages, commit fraud and steal customers from travel companies. In the last issue we looked at securing the content of your website. Today we are looking at how you can harden your website to make it less vulnerable to being hijacked, copied, cybersquatted or cloned.

1.1 Your website is one of your most valuable assets as the window that customers see you through as well as being the main transactional portal for most organisations. One of the most common crimes reported to PROFiT is that a website has been copied or cloned, or that someone using a similar email address is scamming customers. Hardening your website will help safeguard your brand and protect customers. Below we examine a few of the methods that you can use in order to reduce the risk of having your website compromised.

1.2 **If your website is subjected to cybercrime** including using one of the methods outlined in this email campaign issue, then report it to **ACTION FRAUD**.
USE THE ONLINE REPORTING TOOL: https://reporting.actionfraud.police.uk/login
OR CALL ACTION FRAUD: 0300 123 2040 **(**Monday to Friday 8am - 8pm)

PROTECTING YOUR WEBSITE FROM HIJACKING OR UNAUTHORISED TRANSFER

2.0 **ICANN** (Internet Corporation for Assigned Names and Numbers), the International body that oversees Internet Protocols (IP) and Domain Name Systems (DNS) recommends the following as basic measures all organisations should take to protect their websites from hijacking and unauthorised transfer.

USE DIFFERENT DOMAIN NAMES AND EMAIL ADDRESS

2.1 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. For instance, if your domain name is example.com, a best practice is to use an address in WHOIS that is **not** user@example.com.

2.2 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.

CREATE A STRONG, UNIQUE PASSWORD

2.3 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 who may attempt to hijack your domain name using the information you provide for other accounts. You can avoid this type of compromise by creating a strong password that you use exclusively for your domain name account.

2.4 You are responsible for the security of your domain name. You should never give anyone the login information to your online account. This includes web hosting providers or web designers as well as friends and colleagues. ICANN do not recommend that you list website designers, hosting providers, or any other third parties as the registrant(s) of your domain name. If you choose to do so, seek legal advice about contractual obligations that third parties should adhere to with regards to the administration of your domain.

APPLY A TRANSFER LOCK

2.5 You can request that your registrar put a *transfer lock* on your domain name. Putting this lock on your domain name is not a fail-safe way to guard against unauthorized transfer or hijacking of your domain name, but it could be another layer of security. Each registrar has a different way of implementing the transfer lock. Some require two-factor authentication to remove the lock; some simply require authorization from the registrant. Check with your registrar about their policies regarding transfer lock and decide whether it is a service that's right for you.

EXPLORE MUTI STEP AUTHENTICATION

2.6 Some registrars can offer you the ability to implement a multistep authentication when accessing your account. This provides added protection by requiring a unique security code, in addition to your username and password, to access your online accounts. Refer to the terms of your registration agreement to see if multistep authentication is available.

WHOIS DATA REMINDER POLICY

2.7 Whatever email address(s) you provide as contact information when you register your domain; you must be sure they are active accounts and that you check them regularly. You want to keep your contact information up to date to be sure that you receive WHOIS Data Reminder Policy (WDRP) notifications, renewals, and other important notices from your registrar.

WHAT TO DO IF YOUR DOMAIN IS TRANSFERRED WITHOUT YOUR AUTHORISATION

2.8 If you believe your domain name was transferred to a new registrar or registrant or if your account information was modified without your consent, immediately contact your registrar. Don't delay! The sooner you contact your registrar, the better. If you wait, your domain name may be transferred again and again, further complicating the process and making it harder to retrieve your domain.

2.9 There are specific rules that govern the transfer of domains that are designed to protect you. 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. Ask your registrar to request a copy of the form used for authorizing the transfer.

2.10 The registrar that the domain name was transferred to must be able to produce a copy of this documentation when it is requested. Failure to do so is grounds for reversal of a transfer in the event that a complaint is filed under the **Transfer Dispute Resolution Policy**. If you've contacted your registrar and they are unable or unwilling to assist you, submit an **Unauthorized Transfer Complaint** with ICANN. ICANN will review your situation to see if they can assist you in recovering your domain.

2.11 The following documents may help you:

- ICANN Transfer Dispute Policy: https://www.icann.org/resources/pages/tdrp-2012-02-25-en

Whilst ICANN's Security and Stability Advisory Committee have produced these guides:

- SAC040: Measures to Protect Domain Registration Services Against Exploitation or Misuse
- SAC044: A Registrant's Guide to Protecting Domain Name Registration Accounts

PROTECTING YOUR WEBSITE FROM BEING CLONED

SECURE YOUR CODE

3.0 If you are working with a developer, ask them if they have added security measures to protect your site from potential theft. If they have not, they should encrypt the code and add layers of protection to keep your site 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.

COPYRIGHT YOUR WEBSITE PAGES

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

3.2 To give your online content a measure of enforceable protection in the US you need to register your website's copyright with the US Copyright Office: https://www.copyright.gov. Non-US citizens can register at the US Copyright Office and the US has a longer span of protection for the works than in the UK. To register a copyright, you must either be the author of the content or have rights granted by the author.

3.3 One way to check whether your website has been cloned is to use Google Alerts which allow you to search the Internet to see if your content is in other places than just your domain. To start, simply go to https://www.google.com/alerts, copy and paste your company name and/or a distinctive portion of your website text into the search query and provide your email address when prompted so that Google can email you the results of the search. You can adjust the settings in Google Alerts to notify you on a daily, weekly, or real-time basis. You can create as many alerts as you like.

3.4 In addition to Google Alerts, there are several other online tools to help keep your online content safe and secure. https://www.copyscape.com is a free plagiarism checker. It is a detection service that allows you to check whether your text content appears somewhere else on the internet. Try looking for your ABTA or ATOL number.

WHAT TO DO IF YOUR WEBSITE IS CLONED

3.5 Search the cloned site for any contact information of the user that has copied your content. If you cannot find the owner or contact information of the person that has copied your content, contact the website hosting service that hosts the site. To find this information, go to https://www.whoishostingthis.com, type in the URL of the cloned site, and the search results should return the web hosting service responsible for hosting the website.

3.6 Typically, web hosting services will take down the 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 and submit to ensure you are the rightful owner of the site.

DMCA is the Digital Millennium Copyright Act. The law was enacted on October 28, 1998 to create an updated version of copyright laws to better regulate digital material. A DMCA takedown is a content owner's right to request that material be taken down if the owner's property is found online without permission. To learn more about DMCA takedown, please see: https://www.dmca.com/faq/What-is-a-DMCA-Takedown.

PROTECTING YOUR WEBSITE FROM CYBERSQUATTING

4.0 Cybersquatting, also known as domain squatting, is a specific type of cybercrime activity covered

by specific US legislation called the Anticybersquatting Consumer Protection Act 1999 (ACPA). The Act established a cause of action for registering, trafficking in, or using a domain name confusingly like, or dilutive of, a trademark or personal name.

4.1 In plain English, cybersquatting is the act of registering, using, or trying to sell a domain name which is confusingly similar to an established company or businesses domain with the intention of generating revenue by piggy backing upon it. Typosquatting is similar to cybersquatting but the criminal uses a domain name that relies upon common spelling mistakes of an established domain to generate revenue. Another name for typosquatting is 'fat finger fraud'.

4.2 There is no direct equivalent to the US legislation in the UK and so it is doubly important that all organisations take measures to reduce the risks from cyber and typo squatting.

MONITOR FOR DOMAIN NAME REGISTRATIONS

4.3 Th earlier that you become aware of a potentially malicious registration the easier it is to deal with it. There are several free monitoring services that will issue alerts if someone registers a domain like your domain. Many registrars also offer this service, although some charge. Free services include:

- https://www.ultratools.com
- https://www.whoisxmlapi.com
- https://www.freedomainmonitor.net
- https://www.networksolutions.com/manage-it/keyword-login.jsp?bookmarked=ef98712a507865e346e50158f36a.059

NOTE: PROFiT does not vouch for the security or efficacy of these 3rd party tools.

MONITOR KNOWN MALICIOUS ACTORS

4.4 A powerful way to stay informed about the online activities of an organization, individual, or even a location, is to watch for changes to the monitored registrant information as reflected in the Whois records. Use this to track a specific registrant or to alert you to new online holdings before they become active or are publicly announced. https://research.domaintools.com/monitor/registrant-monitor/

TRADEMARK YOUR ASSETS

4.5 There are a number of legal issues surrounding takedown requests. For example, DMCA requests can't always be issued as they relate to copyright issues instead of trademark issues. You need to have a registered trademark of your brand name (or other assets) to be able to request a trademark infringement takedown. To register to add a Digital Millennium Copyright Act Services (DMCA) badge to your website visit https://www.dmca.com. The DMCA have a takedown facility where a trademark is involved but they will not get involved in copyright disputes.

HAVE A CLEAR INCIDENT ESCULATION AND RESPONSE POLICY

4.6 When they notice cybersquatting your teams need to know the correct path of escalation as well as people in change of the response. Furthermore, have a single point of reference for coordinating actions taken on these incidents. Responsible parties should be aware of the actions that need to be carried out to investigate and remediate the problem.

WHAT TO DO IF YOUR WEBSITE IS CYBERSQUATTED

4.7 It is not easy to have a malicious domain used for cybersquatting removed as domain name registers need to be certain that you have a proper case when deciding who is right, so it is important to set out your complaint clearly and provide evidence. It may be good enough to just say that the malicious domain has been set up for criminal purposes or is defrauding your customers, but you probably need to go much further when claiming an abusive registration.

4.8 To give yourself the best chance of success we offer the following advice to prove your rights and show the register that the person complained of is bogus giving yourself the strongest possible chance of success:

- Use the WHOIS service to identify the cybersquatters domain registrar.
- Your complaint should be addressed to the domain registrar that you have identified as they are responsible for having it removed or deactivated.
- Your complaint should show how you have used your trading name(s) or mark(s) in question for a significant period and to a significant degree (e.g. by way of sales figures, company accounts etc).
- Show how the trading name or mark in question is recognised by the purchasing trade/public as indicating the goods or services of you as the Complainant (e.g. by way of advertisements and advertising and promotional expenditure, correspondence/orders/invoices from third parties and third party editorial matter such as press cuttings and search engine results).
- If possible, show that your trading mark is registered at Companies House under the name [name] and has been since [date] (attach evidence e.g. Companies House printouts, company books, letterhead and records).
- Where applicable show that it has the following registered [UK/Community] trademark(s) (detail marks, date of grant and provide copy certificates or printouts from the Patent Office/OHIM - www.patent.gov.uk, www.ohim.eu.int/en/).
- Explain that the complained of registration is abusive because it was primarily registered to unfairly disrupt your business or threatening to unfairly disrupt your business because… (explain how the registration disrupted your business, how the Respondent is to blame, and provide evidence to show this). And/or;
- Explain that it was used by the Respondent in a way which already has confused people into thinking that it was controlled by you. That an Internet user seeing the domain name or the site to which it is connected will believe or be likely to believe that "the domain name is registered to, operated or authorised by, or otherwise connected with your company – complainants to you are god evidence of this (explain the confusion, how it has been done (web site/email?), who has been confused and provide evidence to show this). And/or;
- It was one of a series of registrations that the Respondent has made, which because of their number, type and pattern prove that the Respondent is in the habit of making registrations of domain names which correspond to trademarks or other well-known names in which the Respondent has no apparent interest. (explain how you know this, which registrations you are talking about, what the pattern is, how this name fits into that pattern and provide evidence of it).
- Explain what outcome you want. Do you want the domain name removed, transferred to you, or do you want the domain name and the abusive website contents transferred to you?
- Explain whether there are outstanding legal proceedings (a register may decline to act if legal action is ongoing).

4.9 If the registrar is unresponsive or if there's a need for urgent action, other parties can step in, such as CSIRTs http://www.csirt.org/services/ or CERTs who are used to dealing with domain takedowns. They also have the social network to help speed things up. Registrars accredited by ICANN are obliged to provide contact information and address reports of abuse or compromise.

Like what we do to protect you?

We are always short of funds and need your support.

Find out how you can join PROFiT and fight fraud by emailing contactus@profit.uk.com.

Next Week: Part 15 DDOS ATTACKS & HACKING