PROFiT
Prevention of Fraud in Travel

THE COUNTER FRAUD CAMPAIGN 2019

PART 13: PROTECTING WEB CONTENT

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 13 we look at how to secure your web content to make it harder for criminals to copy or clone the content for criminal purposes.

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 SECURE THE CONTENT THAT YOU USE

1.0 We have already seen in the last issue 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. It is therefore incumbent on all travel companies to harden their websites to make it as difficult as possible to misuse their branding to commit scams.

1.1 Making it harder to copy your content will help protect your brand and protect potential customers. Below we examine a few of the methods that you can use in order to reduce the risk of having your content compromised.

PROTECTING CONTENT

ADDING A DMCA PROTECTION BADGE TO YOUR PAGES

2.0 One method of protecting webpages is to add a Digital Millennium Copyright Act Services (DMCA) badge to your website https://www.dmca.com. This will inform you if someone steals your web pages and DMCA will take down the stolen pages for free.

2.1 The process of adding a DMCA badge is relatively easy to do:

1. Register for free http://www.dmca.com/badges.aspx?ref=solc53c. Registering does not cost you anything and you will get a complete list of all of your protected website pages.
2. https://www.dmca.com/Users/Login.aspx?Redirect=%7e%2fProtection%2fdefaultaspx%3fr%3dsolc53c lists all the webpages of your website that are protected by the DMCA Protection Badge. In order to get your pages on this list each webpage must have a DMCA.com Protection Badge on it.
3. Once registered - log into the **DMCA Protection Portal**.
4. Go to "**My Protected Pages**".
5. Click "**Add New Page(s) to My Protection Plan**".
6. Pick a Badge that you like. **Note:** if you do not pick the badge code when you are logged into the Protection Portal none of the pages your badge choice is placed on will be indexed to your DMCA.com Protection account.
7. Copy the embed code and paste it either in the footer of your website (to protect all pages with that footer), or on certain pages that you specifically want protected.

8. Badge code embed best practices:
    a. Make certain the DMCA.com code is "view-able" within the source code of your webpage
    b. Do not remove the GUID or Unique alphanumeric tracking and status page code.
    c. Do not remove the status page link. It is preferable that users see your protection status than the DMCA.com home page.
    d. Make certain the webpage(s) you are placing the badge on is free of validation errors. Check your webpages through a mark-up validation service
    e. Get Verified Status http://www.dmca.com/Solutions/View.aspx?ID=271356dbed9d-4f31-a585-e0eaa1062148&ref=solc53c by far the best option for your website is to have a fully verified website certificate and status page. The website certificate and status page are connected to your Protection Badge.
9. Every page that contains a DMCA Protection Badge will be automatically added to your protected pages list.
10. New web pages with the DMCA Protection Badge are detected instantly and generally appear in the secure DMCA Protection Portal Protected Pages list within 24 hours after placing the DMCA Protection Badge on your webpage.
11. Placing the DMCA.com Protection Badge on your webpage triggers the DMCA.com crawling / indexing systems to come check your page as it is requested.

GOOGLE ALERTS

2.2 Google Alerts https://www.google.co.uk/alerts is a free service to monitor the occurrences of key terms such as your brand name, your exclusive properties, or ATOL or ABTA membership number being used online and takes seconds to set-up. Once you register the term you wish to be alerted about then every time it is mentioned online you should receive an email warning you.

SECURING TEXT

3.0 Certain text is essential to all legitimate websites. Criminals may copy your text and change contact details and names to clothe themselves in your brand whilst they commit fraud. You can make it harder for criminals if you convert to images the following information:

- Contact Details,
- Terms and Conditions,
- Cookies Policy,
- Privacy Information, and
- Flight, Property and Resort Descriptions

so that it is harder for criminals to copy them and change the details when cloning your website.

3.1 Converting the text to a GIF, JPEG, or PNG file does not make it impossible to copy using online tools but it does make it harder to amend them to edit out your company branding. Criminals will tend to go for the easy option and so converting text to image may have a useful deterrent effect.

SECURING IMAGES

4.0 Criminals copy and use company logo's, scheme membership badges, accreditations and other hard-won symbols of integrity to lend credibility to their scams. Key images of exclusive properties, resorts or vessels are also valuable as they can be used multiple times on metasearch, price comparison, or aggregator website thus allowing the same image to be used multiple times for fraud simultaneously. Companies make it easy for those intent on breaking the law to do this by failing to take measures to secure integrity symbols and key images.

DISABLING THE RIGHT CLICK

4.1 The easiest way to for anyone to download your images is by right-clicking on them and selecting "save image". While it's still easy enough to download images in other ways, if you disable this capability, you'll put off less web-savvy image thieves and people who can't be bothered with the hassle of looking at your HTML or searching the browser cache.

4.2 A simple way to achieve this in WordPress is by using the No Right Click Images Plugin https://wordpress.org/plugins/no-right-click-images-plugin/. This plugin uses Javascript to disable the contextual menu when you right-click on an image. It only affects right-clicking on images, so if users right-click on a link to open it in a new tab, for example, this won't be affected. You can also choose to display a copyright message or another image when an image is right clicked.

4.3 The main problem with this plugin is that it can be disabled by simply turning off Javascript, but most users won't be aware of this or won't bother disabling it unless they really want your image. It's also possible that the Javascript could cause a conflict with some other code in the theme or a different plugin.

4.4 To protect your images more fully, you'll also need to disable the default image linking that occurs when you insert an image in WordPress. To do this select "none" in the "link to" dropdown box when you're uploading your image. Disabling the right click will not stop a copyist from using print screen and cropping the image out.

APPLYING A WATERMARK

4.5 Adding a watermark can be used to protect your images. It is one way to protect your images from theft. And while watermarking won't protect your images 100%, at least it is one more step to deter potential thieves.

4.6 To create a watermark for an image use Photoshop or similar:

1. Open Photoshop and create a new document by going to File>New. Choose the size of your watermark. If you are only watermarking web images size the new document to the size of your web size files. If you plan on watermarking full size images, make your initial file 2500 px by 2500 px for a high-resolution watermark that can be used on full size images.
2. Next, you can either pick out your fonts or copy your logo over onto the new document. You could choose the domain name of the website where the villa will appear so that the customer will spot any discrepancy (hopefully) from the website domain for the website they are on if the image is stolen and put on fraudster's website.
3. Grab the Marquee tool (the dotted square box) and draw a rectangle around your watermark.
4. Next go to Edit>Define Brush Preset. Name your brush and click OK.
5. Your new brush will be in your brush catalogue. You can decrease the opacity of the brush or change the colour. Now watermark your images with a discrete embedded mark which does not detract from the overall feel of your image.

ADD A COPYRIGHT NOTICE

4.7 One way that you can use a watermark is to include a copyright symbol with your company or property name or Web address. Yet again it will not prevent everyone from using your images without permission, but it will stop some people from doing it. And if someone intentionally deletes or hides your copyright notice, it shows intent to commit a crime.

4.8 In many jurisdictions, including the UK and US, every time that you create an image you automatically have the protection of copyright even though it is not registered anywhere. Adding your copyright notice has the effect of discouraging at least some people from casually downloading and using your images.

4.9 Although a photographic work is invested with copyright from the moment of its creation, to fully protect your copyright it is essential to assert it by means of a notice. If you do not do so, and your image is used without authorisation by another person or organisation, they may be able to claim they were an "innocent infringer", thus reducing any damages due to you.

4.10 There is no legally defined format for the copyright notice, so the format is not critical. A common format is:
Copyright © 2017 [Your Company or Property Name], All Rights Reserved [Your Contact Details]

4.11 Copyright – Not all countries recognise the © symbol and they require the word "copyright" to

appear in the notice. Therefore, it is advised to always include the word “Copyright”

4.12 © – Always include the © symbol as it is a recognised shorthand to identify that you care about the content that it relates to and will take steps to protect it. (Open bracket c closed bracket will give you this symbol)

4.13 Year – It is normal practice to enter the year of first publication (NOT creation), and this has been confirmed by the Design and Artists Copyright Society (DACS UK). This is true for both the UK and the USA.

DIGITAL FINGERPRINTING

4.14 Digital fingerprinting is a form of searchable protection that allows you to track its use. To make a digital fingerprint take a semi-random but unique string of characters and numbers (perhaps the company name or your property along with the company registration number and post code), embed that into the image and then search for the string using a regular search engine. Since the string is unique and doesn’t appear anywhere on the site itself, just the feed, only sites that have scraped the feed will be listed and these can be approached for breach of copyright.

4.15 To make a digital fingerprint and embed it into your image:

1. Develop a string of 10-12 characters that is unique to you and can identify your works on the Web.
2. Perform a test search for that string using a tool such as Copyscape https://www.copyscape.com to ensure that no other sites or images contain it.
3. Embed the string into the filename of every image post, ideally right before the extension.
4. Embed the string into the Exif (Exchangeable image file format) as a backup measure.
5. Perform regular searches for the fingerprint or set up a Google Alert. An ideal search string might look something like this: fingerprint – company name:yoursite.com

FINGERPRINTING

4.16 You can add a ‘fingerprint’ into your images so that you can identify where it has been copied from should it turn up somewhere surprising. This is sometimes done by map makers to prove the copyright of their products and often goes unnoticed on the map.

4.17 To add a fingerprint to your images use Photoshop, or a similar package, to add a very small hardly noticeable item, such as a flowerpot, which a copyist will find it hard to identify as a ‘tell tale’ mark but you will know is present. This makes the image unique.

4.18 Use a different ‘fingerprint’ for each outlet where you advertise so that if your image turns up unexpectedly you can see where it was copied from. Don’t forget to keep a record of which fingerprint was used on the image for each place where you advertise it. Obviously don’t tell anyone that you have added a fingerprint to your image. A fingerprint can be used to prove ownership of an image; https://www.theguardian.com/uk/2001/mar/06/andrewclark.

ENCRYPTION

5.1 There are a few commercially available applications that will, for a fee, allow you to control what happens to your images. If someone tries to copy them, they become encrypted, you and also attach copyright information which shows when a right click is made on the image. Some tools also allow you to operate a validation of your images. One such company I called AffirmFirst based in the UK.

Like what we do? We always need support. Find out how you can join PROFiT and fight fraud by emailing contactus@profit.uk.com.

Next Week: Part 14 PROTECTING WEBSITES