

Logo fraud: the curse of fraudulent websites

David Holman, First Cyber Security

Fraudulent websites are not new, but their capability to appear genuine continues to become more sophisticated. So why do they fool us? Web 2.0 technology supports the functionality to make websites look and feel more interactive. And tools used in the design of these websites are easily available and require less training to create an acceptable result. In short, we have de-skilled the ability to create a reasonably acceptable site thanks to improvements in technology. However, good-looking sites are not the only issue for increased fraud, nor are they the major driver.

Looking for help

It is good practice to look for help when making decisions on website authenticity. Many organisations, including government, will suggest looking for https in the address bar and the presence of the padlock to show that data is encrypted on its journey to the server. However, training users who just want to shop to review these aspects – not just on every site but every page – is a step too far, which is why stories of consumers being ripped off by buying fake or undelivered goods are commonplace.

In any event, an SSL connection can be bought for as little as £5 a month – a drop in the ocean compared with the money that fraudulent sites can rake in. And all it proves is that your information goes securely to the web server. If that server happens to belong to a fraudster, a consumer can take little comfort in knowing that their data will be safe all the way to the fraudster's site.

Better ways

There are better ways to encourage all Internet users to assess their security before shopping, which would solve the problem.

The security industry, led by such companies as VeriSign and McAfee,

have developed 'seals' – logos which, when added to a website, are an indication that the site is using an SSL certificate and therefore the consumer has to worry less about remembering to review the address bars. These logos become 'trust symbols' in their own right. Most people would agree that it is far easier to notice these logos in the course of a customer journey through a website as they appear on each page. But, of course, the fraudsters know this as well. Copying these logos or even the entire site containing these logos is relatively easy. Sadly the industry has known this for some time but often the drive for revenue has continued to forge the sale of technology, irrespective of the value to the consumer.

Recognising the difficulties involved in Internet pharmacy certification, John Chave, the Secretary-General of the Pharmaceutical Group of the European Union (PGEU), recently said: "The idea that you can get around online counterfeiting through certification is quite difficult. An EU authenticity mark would be immediately faked. We would be asking patients to differentiate between genuine and forged logos."

Clearly, more had to be done to make things more difficult for the



David Holman

fraudster, and hence safer for the consumer. And so security companies added additional functionality into their seals, either streaming them dynamically as the web page was viewed or adding certificates that could be accessed by clicking on or selecting the logo.

Although, from a technology perspective, this does require more thought from the fraudster, it also requires more involvement from the consumer, who really doesn't want to have to do anything other than shop. Downloading the logo dynamically as each page is viewed might technically be more difficult to achieve, but if the consumer sees a logo, dynamically delivered or present on the page as a static graphic file, they will look pretty much the same to the untrained eye. It can also increase the perceived download time of the page, a critical factor for retail sites.

"Life is made even easier for the fraudster by the fact that the consumer has no way of knowing beforehand exactly what the certificate should look like"

The addition of a certificate that is visible when the logo is selected is not problem-free either. First, the consumer has to click on or select the logo; and second, this certificate could also be fraudulent. Life is made even easier for the fraudster by the fact that the consumer has no way of knowing beforehand exactly what the certificate should look like.

McAfee developed a technology for checking the integrity of a site using the

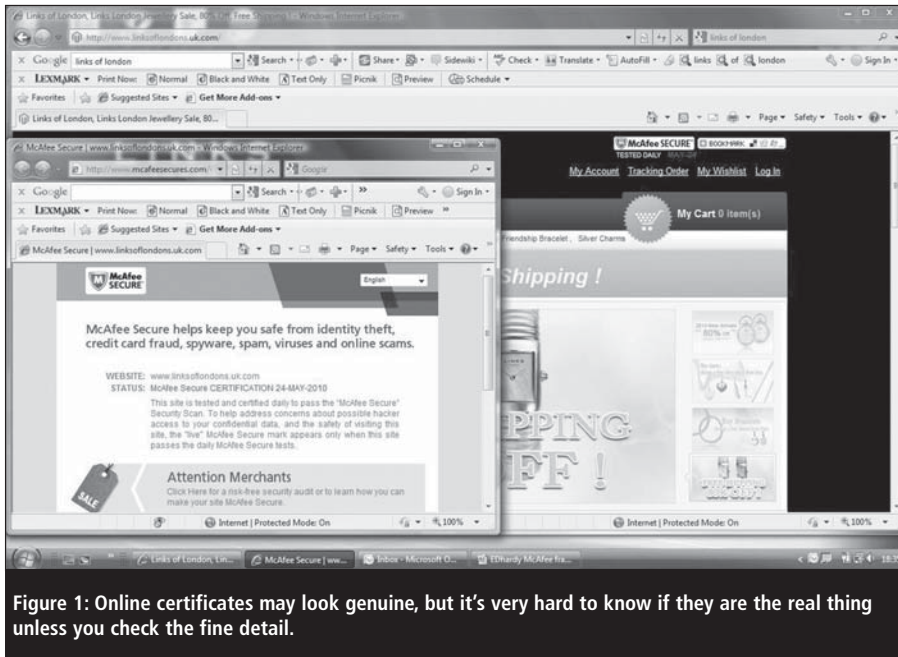


Figure 1: Online certificates may look genuine, but it's very hard to know if they are the real thing unless you check the fine detail.

manage the legal processes involved up to and including getting the sites closed down, if previous legal activity has not succeeded in stopping the fraudster from trading online.

“Even obvious copies of legitimate websites such as online banks, can take many days or weeks to be removed from the Internet. This can take many months if the website has been set up in a foreign country where the authorities have no jurisdiction”

This enforcement action may be a necessary ‘policing’ of the Internet but it suffers from a significant problem. Like most legal processes, it takes time. Even obvious copies of legitimate websites such as online banks, can take many days or weeks to be removed from the Internet. This can take many months if the website has been set up in a foreign country where the authorities have no jurisdiction. Once shut down it is common for them to relaunch under a slightly different URL almost immediately.

It’s a battle that is constantly waged but is unlikely ever to be won. A UK bank could have to contend with over 100 fake sites at any one time.

Unfortunately, while these legal processes are ongoing, such fake websites continue to operate and the consumer is still very likely to be tricked into buying counterfeit goods, losing their personal information or paying for goods that never arrive. While current advice is to buy using credit cards to ensure that the consumer does not lose out, neither does the fraudster. Additionally, these types of fraud increase the cost of credit cards for us all.

Secondary authentication

The credit card companies themselves have tried to reduce online

‘McAfee secure’ logo, encompassing the current day’s date backed up by a certificate which the consumer sees when clicking on the logo. This should be a significant comfort to the consumer wishing to buy from a website. As can be seen from the example in Figure 1, the date is correct and the certificate is authentic and shows all the data the consumer would expect to see to confirm provenance. But on closer inspection of the URL in the address bar, it can be seen that rather than www.mcafeesecure.com – the authentic site for this certificate – the actual URL is www.mcafeesecures.com. The addition of a extra ‘s’ is likely to be overlooked by even knowledgeable IT consumers. This is possible simply because there are few checks conducted on domain name registrations, let alone subdomains, which are commonly used by cyber-criminals for phishing attacks.

Other trust symbols

Up until now we have reviewed the security industry and its response to the lack of security on websites. But it is not just security logos that consumers view as trust symbols of an authentic and secure website. Logos purporting membership of trade associations, asso-

ciations with major corporations and code approval schemes are also commonly copied.

These additional trust symbols, while not addressing website security, address corporate credibility and rely on creating a false level of confidence in the company as a legitimate supplier. Retail organisations suffer from reduced revenue, increased customer service costs and brand damage from sites advertising products for sale that are counterfeit, stolen or are non-existent.

Ironically, whether or not the brand sells online is irrelevant. For example, Breitling, the luxury watch manufacturer, claims not to sell watches via the Internet. But a quick Google search returns any number of sites selling these watches. Some may be legitimate second-hand sales, but how is the consumer to know?

A number of retail organisations have recognised that protecting their brand online is as important as protecting it in the bricks and mortar world. A number of brand protection companies such as Cyveillance, Mark Monitor and Envisional market and sell ‘reactive’ brand protection services. These services are very focused on detecting the use of brands online, defining a priority for action and assisting organisations to

fraud by coming up with methods to ensure that a secondary authentication is required from the consumer to buy online. Mastercard Securecode and Visa's 3D Secure have no doubt reduced the cost of fraud, particularly when fraudsters use real credit card data to purchase goods. However, these services are advertised on sites by showing a logo, which the fraudsters replicate to create a false sense of security for consumers buying from their sites. The fact that the technology is never used on the site is irrelevant as, by the time the consumer realises (if in fact they do), they have already lost their personal data.

“Common advice given to consumers is to ask the contacts listed on the website if they accept returns; they might as well ask if it's a fake site”

Code approval schemes were put in place to assist the consumer and give them protection in the case of complaint. However, while they are well-meaning, they give fraudsters the ability to hide their trade behind a screen of apparent authenticity. Common advice given to consumers is to ask the contacts listed on the website if they accept returns; they might as well ask if it's a fake site. In order to protect their legitimate members and hence protect their revenue, the logos of code approval schemes have gone in a similar direction to that of the security companies, by adding information to their logos and/or certificates.

Not surprisingly they have had the same result; fraudsters copy these logos and certificates in exactly the same way. This may not appear to be as much of an issue as falsifying the security of a site; but if that logo suggests the fraudsters are members of the Gas Safe Register or the Royal Pharmaceutical Society, then the fraud could have a life and death impact.

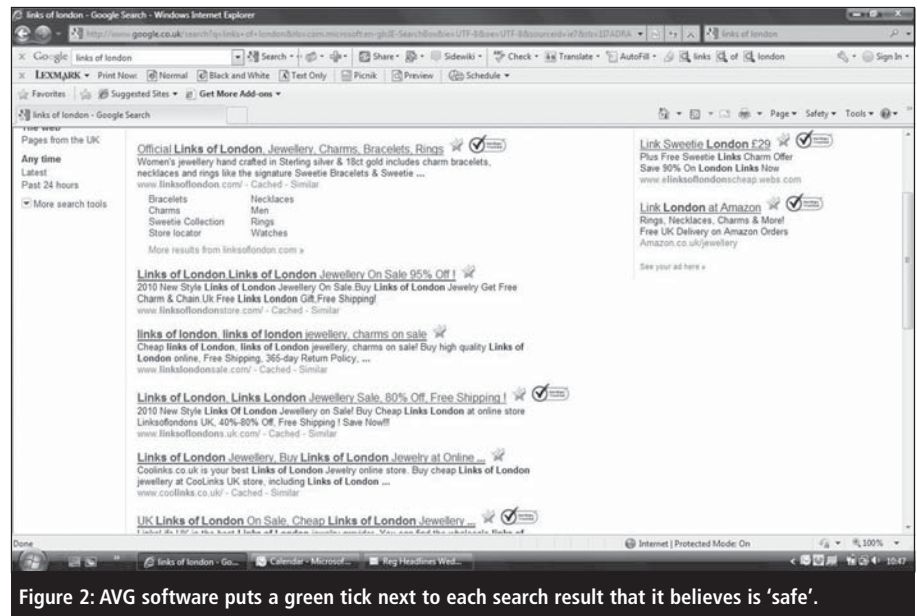


Figure 2: AVG software puts a green tick next to each search result that it believes is 'safe'.

In reality, fraudsters don't just copy security logos, payment card logos or trade association logos – they will copy them all and add them to a visible part of the website in the expectation that a consumer will notice some of them and have the confidence to continue shopping. The plethora of these logos visible on sites tends to give confidence to the unsuspecting consumer.

Search engine hoaxes

Before we even get on to the website it is common practice to use a search engine to review the main sites of interest. The Search Engine Optimisation (SEO) industry is hugely important in assisting companies in getting their websites at or near the top of these results lists. But the fraudsters have found ways to poison these results and add their own fake sites high up in the listings, often referred to as 'searchware hoaxing'. To help the consumer, some companies offer guidance as to whether to trust these sites. The Google search in Figure 2 shows the results of a search for 'Links of London'.

AVG software, a typical anti-virus product, puts a green tick by each of the entries that it has checked. But what has it checked for? In fact, it's only checked that the site does not

contain a virus and/or malware. 'Safe' in this context means safe to visit, not necessarily safe to trade. The green tick might be interpreted that they are all legitimate sites. This is not the case; there are some sites in the list that are selling counterfeit products. Although authentic sites are interspersed within the results, it is hard for the consumer to tell where it is safe to shop. Even the VeriSign logos appearing by some of the sites, presumably designed to offer the shopper assurance, also appear by fake sites.

It is easy for the fraudster because, from a technology perspective, any anti-fraud technology that works solely in the browser is relatively easy to spoof, partly because as consumers we buy online to save time and find the best price and also because the majority of Internet users are not IT specialists, nor should they need to be. Current advice, while well-meaning, is not practical enough for the non-IT specialists who make up the majority of potential Internet shoppers.

Searching for a solution

So knowing the problem, how do we find a solution? Without a solution, the Internet will remain a lucrative playground for fraudsters and will not

give either the consumer or the website owners the benefits they seek, such as lower-cost sales channels. Additionally, strategic investment from governments – such as the UK's Digital Britain initiative – will further emphasise the importance of the Internet for retail sales, banking and delivery of government services.

“Technology solutions will have to be intuitive and rely on delivering trust symbols to the consumer in a new way. Real-time evaluation and validation of the integrity of a web page or logo will be fundamental to underpinning the confidence of any such solution, as will its ability to create a more robust challenge to fraudsters.”

Any anti-fraud solution will have to appeal to consumers irrespective of their IT capability. In addition, affordability is important so that no-one is excluded, especially those who may benefit most from the extended use of the Internet.

Technology solutions will have to be intuitive and rely on delivering trust symbols to the consumer in a new way. Real-time evaluation and validation of the integrity of a web page or logo will be fundamental to underpinning the confidence of any such solution, as will its ability to create a more robust challenge to fraudsters.

Out of bounds

The latter is accomplished by using ‘out of bounds’ techniques, perhaps more accurately described as ‘out of browser’. As previously described, a number of fraudulent attacks occur on the existing trust symbols specifically because the symbol and any validation of it (such as a certificate) are all conducted within the browser environment.

Taking the verification outside of this environment will make it more robust. Authorising the website on behalf of the consumer is not new, what is new is the ability to do this easily, clearly and securely. It is now possible to ask the consumer to do the bare minimum – just look at a small window that appears on the screen for the presence of the website owner’s logo. If it is present, the website has passed the eight-stage validation process and consumers can be confident that they are at the real website of their choice and that no fraudulent activity was detected, hence it is safe for them to proceed.

The website owners’ logo will not be present if any fraudulent activity such as DNS poisoning, frame spoofing, Man In The Middle (MITM) attacks or zero pixel frames are present. In these instances, an alert is sent directly to the website owner detailing the reason for the failure of an authorisation. In fact, the technology can even be configured to redirect the browser to the authentic website if the consumer has inadvertently selected a phishing site. This authentication is repeated, in real time, on each web page visited and is completed while the page is downloaded, the resultant logo, or warning being displayed after the page download is complete. Therefore, it does not reduce the performance of the website. The appearance of the website owner’s logo assists consumers in deciding whether to use the site.

“It is now possible to ask the consumer to do the bare minimum – just look at a small window that appears on the screen for the presence of the website owner’s logo”

This same technology allows the authentication of logos, trademarks, or other entities owned by organisations, such as security companies or

brand owners, in a similar way. Under the control of the trademark or brand owner, not the website owner, these website entities can be validated by hovering the cursor over the entity, no clicking required.

A window containing the brand owner’s logo appears and moves to join the original window outside of the browser environment.

This latter functionality makes the logo verification technology much more secure and similar in operation and understanding to the basic website authentication. There is also the ability to warn consumers where a site is showing an illegal affiliation with another – hugely common in the sale of counterfeit goods.

Again, similar functionality is available for consumers to see ‘official’ websites in search engine results and approved products in auction listings, and both of these examples offer the additional benefit of unapproved sites or listings, perhaps selling counterfeit products, being indicated to the consumer before they are selected from the lists.

Responsible website owners fund the service, enabling the technology to be made available to the general public free of charge.

About the author

David Holman has been a director of First Cyber Security for two years and has worked in IT, defence and security for most of his career. He was previously CEO and co-founder of Becrypt, where he sat on a joint government/industry committee, CIPCOG, chaired by the Cabinet Office, to promote the importance of security products. First Cyber Security (www.firstcybersecurity.com) specialises in Internet security and brand protection. It has been awarded Government Gateway Approved Partner (GGAP) status as part of the Cabinet Office initiative to promote Transformational Government.