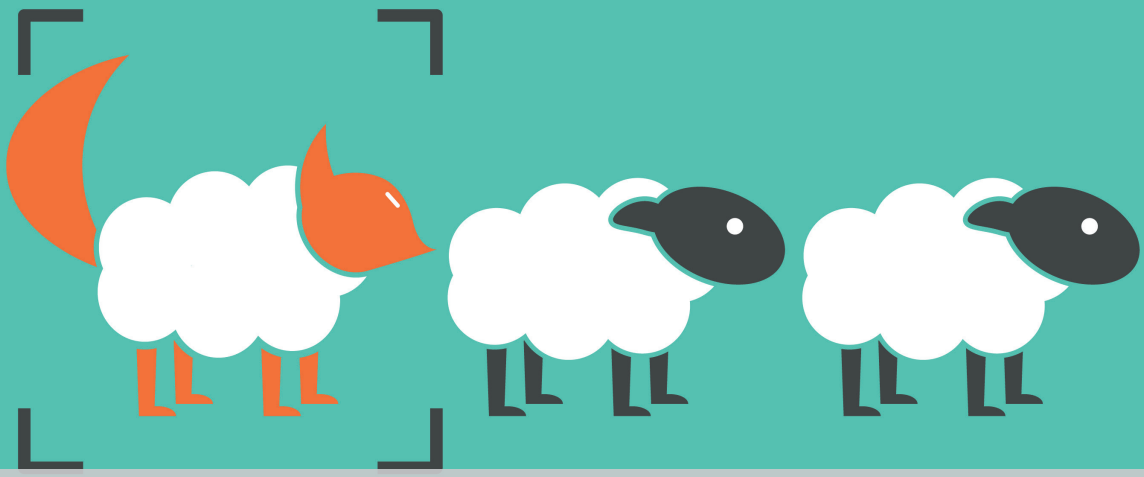
WTR
World Trademark Review

Anti-counterfeiting and Online Brand Enforcement 2021



Industry Insight

CSC

Elliott Champion

A Global Guide

ACG THE ANTI-COUNTERFEITING GROUP

INTA

ICC INTERNATIONAL CHAMBER OF COMMERCE

Internet threats go viral – companies must react to keep brands secure

Author
Elliott Champion

The events of the global coronavirus pandemic have forced significant changes in the way that we live our lives, how we work, socialise, shop, bank and consume media. With restrictions on people's ability to interact face to face, there has been a digital surge resulting in significant shifts in consumer behaviour:

- There are 4.66 billion active internet users – an increase of 690 million since 2019.
- Mobile is the most important channel for internet access worldwide, with mobile internet users accounting for 91% of the total number.
- Covid-19 has accelerated retail trends by nearly five years.

On top of this, bad actors have also reacted to the increased usage and reliance on the Internet. Over the course of 2020, there was an increase in fraudulent domain registrations, phishing attacks, hacks and hijacking attempts, and the sale of counterfeit goods. Companies must react and not simply keep up with the new face of commerce, but protect themselves from revenue and reputational losses, as well as the risks of data breaches that are found in the shadows of digital progression.

Online transactions have accelerated, but fraudsters are keeping pace

With the world's high streets shutting their doors, there has been a need for companies to embrace the Internet as a more prominent revenue channel.

In the retail banking sector, for example, there has been a marked increase in the uptake of online banking. According to the World Retail Banking Report 2020, 57% of global consumers prefer internet banking now, up from 49% pre-covid-19. Naturally, mobile banking apps have also increased in popularity. This rise in usage has not gone unnoticed by fraudsters, who are capitalising on the world's increased reliance on online transactions. Research has highlighted a marked increase in the number of non-legitimate domain registrations featuring well-known banking and finance brands.

Why is this a worry? Quite simply, domains are the key requirement for any bad actor to ply their trade. When we see a surge in domain registrations for a particular brand or industry, especially those that either contain related keywords (eg, for banking these might be 'mobile banking', 'app', 'online' or 'internet', among others) or that have mail exchanger records (meaning that they are set up to send email), it is a strong indicator that such domains could be used to conduct fraud. And a vast amount of them are doing just that. By November 2020, Google had registered 2.02 million phishing websites – around 20% more than the whole of 2019.

Increases in phishing attempts that are aimed not at consumers but at the employees

Elliott Champion
Global product director, brand and anti-fraud
elliott.champion@cscglobal.com

Elliott Champion is the global product director for brand and anti-fraud at CSC, where he is responsible for CSC's industry-leading proprietary technology and product strategy. He is also involved in building client-specific strategies, including optimising a brand's online presence, and protecting and evolving CSC brand protection services. Before his current role, Mr Champion advised European customers, built brand strategies and worked as an enforcement analyst from his hometown of Cambridge in the United Kingdom.

of the companies that they impersonate have been widely reported. Tactics include:

- sending fake employee questionnaire emails to gain credentials;
- CEO fraud or spear phishing using social engineering tactics to fool their target into sending money or sharing data/credentials; and
- vishing (voice-phishing) via the now heavily relied on voice over internet protocol (known as 'VoIP') software such as Microsoft Teams and Skype.

Any phishing activity poses significant risks for a brand, such as data loss and breaches, account compromises, and ransomware and malware infections, among other things. The consequences of these can be costly; the average wire-transfer loss from business email compromise attacks in the second quarter of 2020 was $80,183, not to mention the hefty fines associated with any data breaches.

Human error is inevitable when it comes to phishing of any kind. Ongoing security and anti-fraud training for employees is important, but without the correct security measures in place, companies leave themselves wide open to attack. With 96% of phishing attacks arriving by email, ensuring that your company has all email authentication protocols (eg, domain-based message authentication, reporting and conformance (DMARC), domain keys identified mail (DKIM) and sender policy frameworks) in place puts extra layers of protection between staff and the attacker, reducing the likelihood of a malicious email getting through. Worryingly, even Forbes Global 2000 companies have low adoption rates for these key measures – with DMARC adopted by only 39% of these companies, and DKIM even lower at just 10%. If companies are to deal with the uptick in phishing activity, email authentication must be implemented.

Acquisitions expose domain security risks and IP infringements

Brands doing well during the coronavirus pandemic arguably already had an online-only business model or have been able to quickly adapt and pivot their efforts to focus on their internet proposition. However, there are security and brand risks for those businesses that have thrived, especially those that have bought those brands, which found themselves in administration after struggling due to covid restrictions.

In the United Kingdom, for example, retail giants such as the Arcadia Group (owner of apparel brands Topshop, Topman and Miss Selfridge, among others) have gone into administration during covid-19. At the time of writing, other (notably online-only) brands are in negotiations to buy the group, but switches in ownership could bring security risks, loss of key digital assets and potential IP infringements.

If domain portfolios are not centralised, it is not only an administrative nightmare, but also risks domains lapsing and being picked up by a third party. Lapsed or dropped domains are not just a case of lost sales when a consumer-facing website comes down. Domains also host internal protocols, such as email, logistics and manufacturing, which are vital to the

company's infrastructure. Without a full understanding of which domains host which protocols, an incorrectly dropped domain could bring entire internal processes to a halt.

Once a domain drops, it is difficult to reclaim it. Retail registrars are quick to pick up lapsed domains, and in some cases they purchase branded domains themselves, only to auction them at inflated prices – in dropping a domain, you could end up paying thousands for what should be a $10 domain. If they are not auctioned, there are people ready and waiting to pick up your dropped domains, which could be used for phishing or the sale of counterfeit goods. Full accounting of your domain portfolio, as well as that of any company you may be purchasing, is essential.

Counterfeiting remains a threat

It should come as little surprise that the rise in online selling has fuelled an increase in the buying of counterfeit goods – both related to coronavirus (eg, masks, personal protective equipment, test kits and so-called 'cures') and consumer goods more generally.

Global e-commerce sales in 2020 came to $4.280 trillion, up by 28% on 2019. The eruption of online sales and the loss of physical retail space has instigated a "virtual funneling effect … sending consumers right into product counterfeiters' webs", as Professor Jay Kennedy of Michigan State University puts it. Data suggests that there might not necessarily be an increase in the number of counterfeit products available, but consumers' increased internet shopping means that their exposure to counterfeits will have risen exponentially. With many people losing their jobs or receiving lower wages on furlough schemes, consumers may inevitably search for cheaper alternatives, which falls squarely in the counterfeiters' area of expertise.

In terms of activity, there has been a marked increase in cybersquatting (where third parties register domains including a legitimate brand name and use them to steer traffic away from genuine sites, usually offering significant discounts on the recommended retail price). A high proportion of counterfeit sales start with a domain name being set up to host a fake-branded website, and research shows an increase in the number of domains registered that include existing brands, plus tell-tale keywords such as 'sale' and 'discount'.

Counterfeits put both consumers and brands at risk, and in order to stay on top of the swell in counterfeiting activity, brands must be on top of their brand monitoring and enforcement strategies. Pharmaceutical companies and medical manufacturers will need to be particularly vigilant in their online brand monitoring and enforcement. It is one thing to lose reputation for a shoddy pair of fake trainers, it is quite another if people are sent to hospital or die because they have been sold a fake cure for covid on a site bearing your branding.

Employing partners with sophisticated clustering technologies that connect the dots to help bring down infringing sites *en masse* should be a key consideration. Moreover, having ones with the particular capability to share domain monitoring intelligence with anti-fraud teams kills two birds with one stone.

Comment

The coronavirus pandemic has not so much led to wholesale changes, but rather accelerated the growth of existing trends. It means, unfortunately, that brands do not have the luxury of time to be able to progress their online propositions gradually. Covid-19 has thrown us into the digital deep end – and companies will sink or swim.

Despite this, solid digital housekeeping will leave organisations better equipped to deal with the unfortunate downsides that come with swift online progression and changes in consumer behaviour. Keeping your brand and customers safe can be achieved by simple measures. Our top three tips are:

- Adopt every security protocol available on your vital domains – with vast global domain portfolios, it is sometimes difficult for companies to see which are their most important. For example, at CSC, we collaborate with companies to help them identify their vital domains through the CSC Security Center, which has a predictive-modelling algorithm that assesses more than 20 attributes of a domain name to identify whether that name is conducting business-critical work for your company operations and online brand. Once you know your vital

domains, you will know which ones need appropriate security measures.

- Have good accounting for your domains and register with a security-conscious enterprise-class provider – having good accounting for your domains is not just about knowing which domains you have, it is essential to know what they do (eg, hosting external websites, email, mobile apps, internal APIs), what geographies they cover, who has what access permissions for them, and what security protocols have been applied to them. Having domains registered with numerous registrars makes this difficult, so we advise consolidating with a single provider. We also recommend that you use an enterprise-class registrar, rather than cheaper retail-grade registrars. This way you are working with a partner that is equipped to deal with your most valuable assets – you wouldn't put a $1 lock on a million-dollar house.
- Get ahead of phishers and counterfeiters with proactive monitoring and enforcement programmes – phishing attempts are a certainty; it is a case of when, not if, you will be targeted by phishers. For retail brands, the same is true of counterfeiters – counterfeiters will copy any successful goods sooner or later. Commercial success will always put dollar signs in the eyes of counterfeiters who want to take their piece of the pie. This is why we advocate proactive, strategic monitoring and enforcement programmes across anti-counterfeit and anti-fraud. By doing so, you will avoid the all too familiar 'whack-a-mole' effect that can accompany brand and fraud protection programmes, and achieve mass takedowns to stop the fraudsters before they get going.

In taking these steps, a brand can avoid what may at first appear to be an IT or information security issue from becoming a major legal or compliance nightmare. WTR

CSC
251 Little Falls Drive
Wilmington DE 19808
United States
Tel +1 302 636 5400
Fax +1 302 636 5454
Web www.cscdbs.com