Putting your foot down with a take-down

Mastering the complexities of online brand enforcement for brand owners

Introduction

Due to recent world events, brand owners are increasingly turning to the online channel to maintain and build brands and their businesses. Well-known bricks-and-mortar retail brands, such as Debenhams and Topshop have now been purchased by online retailers including Boohoo and ASOS. The new owners are bringing down the shutters on these giants of the high street and relocating their brands exclusively online. This opens up a whole host of opportunities and threats for these newly virtualised businesses.

Does an end to the high street mean an end to store crime?

Despite UK online retail sales tripling over the past 3 years, which is mirrored in many other countries, it is wrong to think that moving a brand entirely online will bring about the end of revenue and reputation sapping criminal activities. While petty and opportunistic crime, such as shoplifting, may be eliminated by removing goods from the high street to a warehouse, this opens up a much more serious and damaging opportunity for organised crime.

In CentralNic's experience, moving a brand online at best only swaps one type of criminality for another.

In terms of physical theft of goods, distribution channels are now aggregated and stock is concentrated in fewer warehoused locations but with much more complex end-consumer distribution networks making it an even more attractive target for organised crime rather than petty criminals in-store. This, at least, is something most retailers understand and can deal with.

When moving a brand online, a whole host of different criminal activities are faced by brand owners that the majority are ill-prepared to deal with. Fortunately, Debenhams and Topshop have been acquired by major online brands, which are experienced dealing with online criminality. These brands have already invested a great deal of money and resources in developing online brand protection programmes. They already operate a robust internet infrastructure to minimise losses from attacks such as Distributed Denial of Service, which would take the website offline.

Who are the victims in online crime?

When a crime, such as shoplifting, is perpetrated in a bricks-and-mortar store, typically it is the brand owner that suffers direct revenue loss, not the consumer. Of course, in the end, consumers end up paying a bit more for products in order to offset the brand owner's losses through theft.

Online, however, this situation is usually reversed.

Unlike with in-store shoplifting, the consumer is directly and immediately out-of-pocket. But so is the retailer, as it has missed out on revenue it would otherwise have received. It's doubly damaging for the online retailer since it may also suffer from reputational damage. This is because often the consumer is completely unaware that they have been duped and blame poor quality and missing shipments on the innocent and unsuspecting retailer.

Protecting a brand online is a costly but necessary business. While in-store shoplifting accounts for 0.5% of revenues, one study put the cost of online fraud at 7.6% of an online retailer's revenues due to the wide range of potential attacks against the brand.

What about smaller brands?

One of the advantages of doing business online, is that, with a little creativity and a great web-designer, the little guy (mom and pop store) can successfully go head-to-head with the large brands. Unfortunately, cyber-criminals know this. They also know that these smaller brands are less-well prepared and much less-well funded to be able to counter the types of criminality listed above. This makes them an even more attractive target to the criminals than the big brands.

Often smaller brands are not even aware that criminals are targeting them because they have little or no visibility on online activities outside of their own website. It is only when their brand has been suffering reduced traffic and revenues from month-on-month that these smaller online retailers cotton on to the fact that they have become prey to sophisticated online criminals.

Even if they suspect they are being targeted, the majority do not have the experience or in-house resources to deal with the problem. Many admit to feeling lost and helpless in the face of a well-coordinated and well-funded criminal attack, which may well destroy their revenues and reputation.

The very real challenges that online retailers face online

Online crime may seem at first sight to be a victimless crime. However, two main themes emerge when talking to the corporate victims of cybercrime:

Loss of consumer trust

When a shopper visits a mall they visit retail outlets that spend millions on location, building, fixtures and fittings as well as staff and stock. This capital outlay at the very least should reassure the shopper that they are shopping in a legitimate establishment owned and operated by a trusted brand and selling legitimate branded goods.

The cost to criminals faking bricks-and-mortar establishments, and the ease with which they are identified and shut down, is part of the reason that there have been so few cases of it happening - with a few notable exceptions.

Online however it is a completely different matter. Online criminals can rapidly and cheaply create an online web-store that mimics a well known brand and offers counterfeit goods or captures payment cards and other personal details. If discovered, the cost of setting up another similar site is minimal.

Revenue diversion

The amount of footfall in a bricks-and-mortar store normally equates to revenues. Fewer in-store visitors means fewer sales and less revenue. Online however it is completely different, web visitors may intend to shop in a particular web-store but often get diverted to a completely different web-store due to misleading adverts, confusingly similar web addresses or fake online offers of sale on social media. There are many web-visitors who end up shopping on fake websites honestly believing that they are shopping at a legitimate store and ending up out-of-pocket and disappointed with the brand when the products they receive are substandard.

What is in the cybercriminals' tool bag?

The relatively high costs of online brand protection are incurred by the retailer having to counter a wide range of attacks on their brand including

- **Domain fraud** - using a domain name to defraud web-visitors by pretending to be a well-known brand.
- **Domain Hijacking** - compromising a domain name and repointing it to a website selling counterfeit products or perpetrating phishing schemes. Alternatively, repointing a domain to another website in order to extort money from the brand owner for its safe return.
- **DDoS Attacks** - causing a website to be unavailable by sending a large and sustained number of DNS requests effectively overloading the DNS servers' capacity to respond.
- **Traffic diversion** - Using similar but different domain names, social media posts and potentially web advertising to divert web traffic away from the intended landing page.
- **Copy-cat sites** - Creating a replica or look-alike website on a different domain name to fool the internet user into believing that it is the legitimate brand.
- **Fake offers of sale on Social Media** - Using social media to platforms to post highly attractive advertisements and offers that when clicked upon diverts the internet user to a website selling fake merchandise or collecting user and payment details (phishing).
- **Phishing attacks via email** - Sending mass emails falsely claiming to be from a legitimate brand ,such as a bank or a government department, to entice recipients to click on a link contained in the email. Links will take the user to a fake website, attempt to capture login or payment details or download spyware or malware.
- **Fraudulent apps on mobile app stores** - increasingly, as internet traffic is moving onto mobile devices, apps containing malware or spyware are finding their way onto legitimate App Stores.

- **Payment fraud** - Use of fraudulent websites claiming to be a legitimate brand to perpetrate financial fraud by capturing payment details of internet users.
- **Fake reviews** - (sometimes called fliking) The creation of many fraudulent reviews to imply that the product or seller under review is legitimate or higher quality than it actually is. Also used to divert revenue and traffic away from legitimate products by creating poor reviews.
- **Hoax web stores on marketplace sites** - The creation and operation of a fraudulent webstore or seller page on well-known marketplace sites such as Amazon, eBay or Alibaba. These pages are often supported by many fake reviews.
- **Counterfeit product lines** - Marketing and selling fake products either as a direct, usually poor quality, replica of a well-known, legitimate brand or using a well-known brand or trademark on a product which is not produced by a brand owner.

How to take on the cybercriminal

While it is tempting to try to take down the criminal and win a moral victory, simple practicality suggests smaller brands in particular should simply attempt to push the criminal off of their brand and claim a commercial victory. The following tiger related anecdotes can also be applied to cyber-criminals:

You don't need to run faster than the tiger

The following anecdote makes a practical point:

> *Two men are walking through a forest. Suddenly they see a tiger in the distance, walking towards them with an intent look on its face. One of the men takes some running shoes from his bag, and starts putting them on.*
>
> *"What are you doing?" asks the other man. "Do you think you will run faster than the tiger with those?"*
>
> *"I don't have to run faster than the tiger," he says. "I just have to run faster than you."*

With thousands of brands online acting as a potential target for criminality, it is sufficient to make your brand a more difficult target such that the criminals switch their focus to an easier target.

Always keep your eyes on the tiger

In rural India it is common practice for people to wear a painted facemask on the back of their head in the belief that it will protect them from a Tiger attack. The theory goes that, since a tiger is an ambush predator, if it believes its victim is aware of it then it will look for a less vigilant and therefore easier victim. By wearing a mask with eyes on the back of their head it tricks the tiger into believing that it has been spotted.

For online brands, implementing low-cost domain monitoring will actually spot potential online criminal activity before it becomes a real problem. Before launching a look-alike website, or an email phishing attack, criminals need to register a domain name which is confusingly similar to the brand that is being targeted. Spotting these registrations as soon as they happen and blocking, suspending or recovering the domain is usually enough to deter the criminals from persistent attacks.

Domain monitoring typically costs a few thousand dollars a year and can save brand owners many times that in lost revenues.

When facing a tiger, use the right equipment

Back in the early 19th and 20th century, when big game hunting was not considered a deplorable practice, tiger hunts used to be staged on the back of elephants among other animals such as camels and horses. The height and robustness of an elephant made it a much safer platform from which to spot and hunt such a dangerous creature, its sheer power coupled with its formidable tusks made it a useful defensive platform and it could traverse dense jungle in a way that other transport could not.

When combatting a cyber-criminal, it is tempting to bring out the big guns immediately, such as a Uniform Domain-name Dispute Resolution Policy. A UDRP is a legal recourse method of contesting legitimacy and recovering a domain name. It is a highly effective mechanism, but a slow and costly one. However, there is an array of faster and less costly enforcement mechanisms which can be deployed to achieve the ultimate result - for the cybercriminal to abandon their attack and look elsewhere for an easier target.

Mechanisms and techniques to combat cybercrime

Do nothing

In many cases, a domain name will be registered with the intention of using it to perpetrate a crime against a brand owner. With so many potential targets available to the criminal, it is not unusual for the domain to expire before the criminal has gotten around to exploiting it. Sometimes a wait-and-see approach is the best and cheapest option for the brand owner. However, it is essential to continue to monitor the domain for potential activity until the domain has expired.

Typical cost: $

Snap-back

Also called a back-order, a snap-back is an automated mechanism where a domain name is monitored until it expires. As soon as it expires the snap-back mechanism triggers and automatically registers the domain name on behalf of the brand owner.

Typical cost: $

Cease & Desist

If the brand owner believes that a domain name (and more importantly the website that uses the domain name) is infringing on its intellectual property rights it can issue a cease and desist notice to the domain owner. This is normally done by its in-house counsel, IP law firm or via a specialist brand protection provider, such as BrandShelter, a CentralNic Group company. The notice will detail the ways in which the brand owner considers that its brand is being infringed illegally and outline the action that it requires the domain owner to take and the date by which it requires action to be taken. In some cases, it will also outline its intended actions should the domain owner not comply.

Typical cost: $$

DMCA notice

The Digital Millennium Copyright Act is a special standard type of Cease and Desist notice. It tells a company, webhost, search engine, or internet service provider that they are hosting or linking to material that infringes on a copyright. The party that receives the notice should take down the infringing material as soon as possible. If the site owner doesn't comply, the ISP can forcibly remove the content on behalf of the brand owner.

Typical cost: $$

Dehost

Website hosting providers provide shared disk space on which a user can create and host a website. When a brand-owner identifies an infringing domain name or website, contacting the Hosting provider with a DMCA or other cease and desist notice can permit the hosting provider to suspend or close the web-hosting account rendering the website unreachable. This measure can yield rapid results. However, it is usually short-lived since the website owner can simply move their website to another hosting provider at minimal cost. Despite this, moving the website from place to place will cost the cybercriminal time and money, which may be sufficient to stop their activities against the brand owner.

Typical cost: $$

Domain suspension by Registrar

By engaging with the domain registrar through which the cybercriminal has registered the infringing domain, a brand owner may persuade the registrar to suspend the domain name or the account that it belongs to. Suspending the domain name will stop the domain name from resolving to the website and even if the cybercriminal moves their website to a different hosting provider, the domain remains unreachable. Registrar domain suspension is best handled by an IP law firm or specialist brand protection provider such as CentralNic as direct communications with known individuals in each registrar can improve the chance of achieving a successful suspension.

Typical cost: $$$

Marketplace sites

While not a domain name dispute, brand owners often find counterfeit products offered for sale on marketplace sites such as eBay or Alibaba. Most reputable marketplace sites have their own anti-abuse programmes such as eBay VeRO programme. These programmes allow legitimate trademark owners to request delisting of fraudulent or illegal adverts. Due to the number of infringing listings that are normally discovered it is more cost effective for a brand owner to work with a specialist brand protection provider such as CentralNic in an ongoing programme of discovery and takedown. Takedowns are usually rapid and protect consumers immediately. Counterfeiters and cybercriminals will normally continue to attempt to sell infringing products on these platforms unless it proves too costly for them at which time they will target a different brand.

Typical cost: $

Payment gateway account suspension

If a brand owner can prove fraud then a payment gateway will automatically suspend a merchant account. Almost all payment gateways have well established mechanisms in place to assess and suspend accounts that perpetrate fraud. These mechanisms are rapid and well practiced and, like most anti-fraud mechanisms, require submission of proof by the brand owner. Due to the number of payment providers and complexity of the process it is normal for brand owners to use a specialist brand protection company, such as CentralNic.

Typical cost: $$$

Uniform Rapid Suspension

The URS process is a dispute policy that allows a brand owner to file a complaint and obtain a temporary domain name suspension. While the domain name ownership is not transferred, the domain is suspended until it is due to expire. Cybercriminals will give up on a domain name that they continue to own but cannot use. The typical time to conclude a URS case is around three weeks.

Typical cost: $$$$

UDRP Recovery

Many Top Level Domains offer a formal abuse mechanism known as a Uniform Domain-name Dispute Resolution Policy (UDRP) with the domain registry to recover a domain name that has been registered fraudulently. If the UDRP case is won by the brand owner, the domain name is transferred into the brand owner's portfolio ensuring it doesn't not return to the available domain pool unless released by the brand owner. A UDRP case typically takes from 6 - 12 weeks and throughout the case the domain name will continue to resolve. While it is perfectly possible for in-house counsel to file a UDRP it is more normal for a brand protection specialist, such as CentralNic, to undertake this on behalf of the trademark owner in order to maximise the chance of a successful outcome, reduce costs and speed up the process.

Typical cost: $$$$$

Anonymous Acquisition

If it is deemed important to recover the domain name into the brand owner's portfolio, one option is anonymous acquisition. Typically a domain registrar or brand protection specialist will engage in dialogue with the domain owner and negotiate a price to purchase the domain, without disclosing the identity of the potential buyer. Once negotiations are complete, monies are deposited in escrow until the domain is transferred to the registrar whereby it is transferred to the seller.

Typical cost: $$$$$

Each enforcement mechanism has its merits and frailties. Depending upon each individual case and the strategy preferred by the brand-owner a different mechanism may be selected. It is important to consult with online brand-protection specialists in order to ensure that the right mechanism is selected for each case so that costs can be minimised and a takedown can be affected expeditiously.

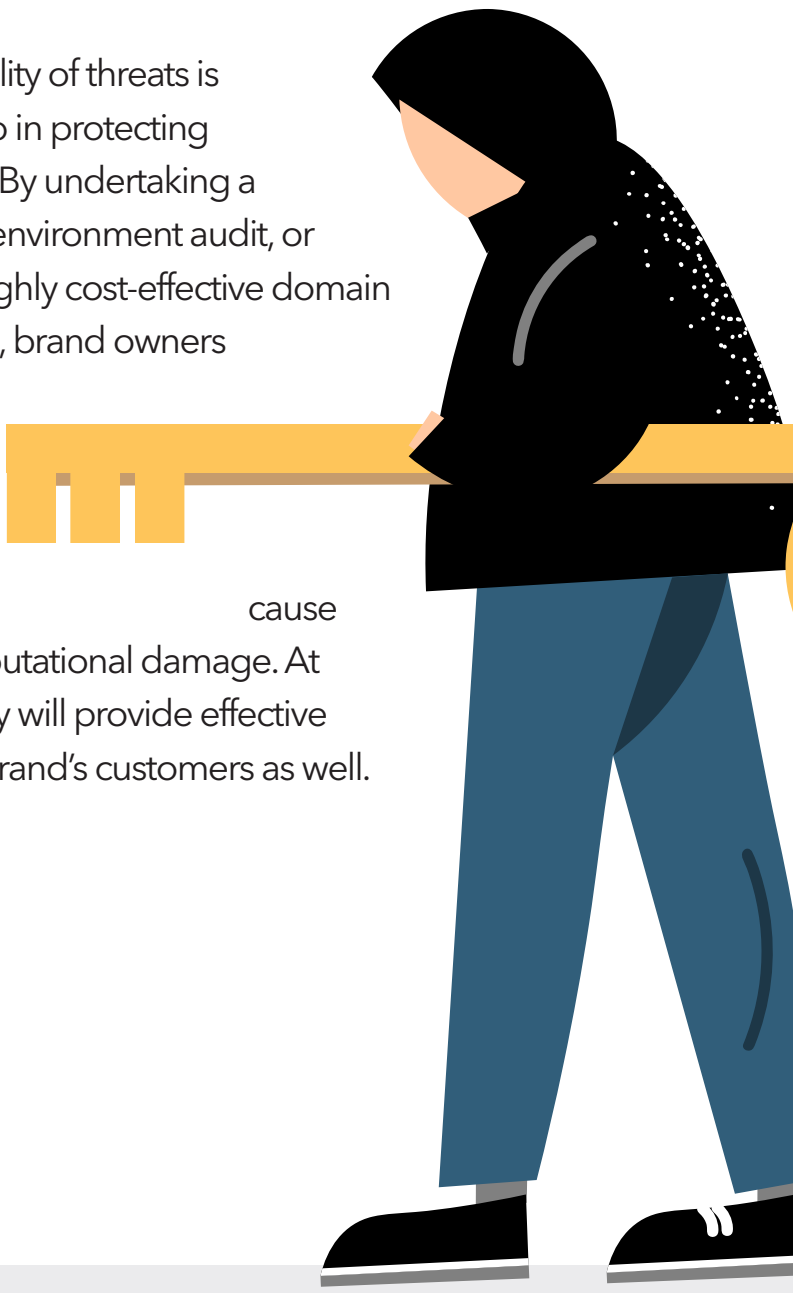
Conclusions

It is clear that cybercrime is an increasing issue for all brand owners and their customers. The rate that businesses are moving online has increased dramatically due to the ongoing pandemic. Cyber-criminals are specifically targeting brands that are moving their operations online.

Most businesses are unprepared for the wide range of sophisticated online criminality that will be launched against them. Brand owners soon find out that it costs their customers money and affects brand owners' revenues and reputation.

Even when a brand owner becomes aware of the threat against their brand, usually they have no idea how to tackle cybercrime, adding to the feeling of helplessness. By simply contacting specialist brand protection firms such as CentralNic, brand owners can find out the extent of the issues facing them, usually at no cost. CentralNic very quickly creates a plan for tackling cyber-criminality against their brand and identifies which measures are likely to provide the most cost-effective results.

Gaining early visibility of threats is always the first step in protecting businesses online. By undertaking a one-time domain environment audit, or implementing a highly cost-effective domain monitoring service, brand owners can quickly identify and deal with threats online before they cause any financial or reputational damage. At the same time, they will provide effective protection to the brand's customers as well.



To find out more, contact:

info@centralnic.com

or visit

www.centralnicregistry.com

Follow us on:

LinkedIn

Twitter

YouTube