Is Your Brand COVERED during COVID19?

Tuesday 7 April, 2020

The global bricks and mortar world has gone into hiding with shops and businesses shutting down.

It has changed the way we do business by moving our world online.

We no longer eat out! We order **Uber Eats**
We no longer buy groceries! We order **Ocado**
We no longer buy instore clothes! We clothe ourselves with **Boohoo / ASOS**
We no longer go to the movies! We watch **Netflix** and **Amazon Prime**
We no longer meet friends! We **Facebook** and
Instagram
We no longer chat! We **WhatsApp** or **Facebook**
We no longer visit our doctor! We consult with an online **Vitality GP**
We no longer visit the bank! We transact with **PayPal**
/ **Monzo / N26**
We no longer go to school! We **Zoom**
We no longer go to the office! We **Webex**
We no longer cycle or gym! We **Peloton**

These online services are our connection to one another and the rest of the world.

Each of the above services is identified by its domain name, it is now the businesses' "online trade mark" that we use and recognise rather than the store front.

The online world is no longer the reserved territory of Millennials (1980-1994) and Generation Z (1995-2012), it has pushed reluctant Generation X (1965-1979), Baby Boomers (1946-1964) and the Silent Generation (1928-1945) online.

Those generations that are not aligned with technology are now forced to quickly learn how:

- online ordering works;
- online banking functions;
- online communications are set-up and operate;
- to engage with online businesses; and
- to interact with family and the outside world online.

The younger generations that have grown up with technology intuitively understand new online services without much need for explanation or support. The "older" generations, over the last few weeks, have had to take-off into the online world with a shortened runway. This can expose them to a variety of online scams ranging from phishing, direct messaging via Facebook, SMS or WhatsApp and email scams.

While most of the online scams are recognisable, it will be less obvious for the new wave of older Internet users that are only now surfing the web. In some cases, the scams or fraud can fool the most cautious user.

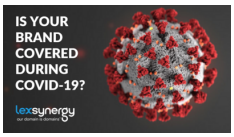
Deliveroo, for those outside the UK, is an online food delivery service that competes with Uber Eats. The company's main domain name is deliveroo.com but if you add the letter "S" to the domain name **deliveroos.com** will direct to a dynamic page that changes content each time the page is refreshed making it easy to click on a link that could download malware or infect your devices.

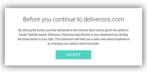
A notice appears asking you to accept and install a "Safe Browsing" Extension. The accept button is a similar colour to the Deliveroo branding. It is safe to assume that most users will not read the notice and click accept thinking it is one of those annoying cookie notices we receive due to data privacy laws.

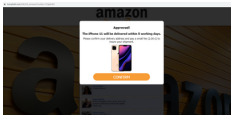
Sainsbury is the second-largest supermarket chain in the UK and is undertaking an employment drive to meet the demand placed on the retail supermarket sector. A Sky news article reports that jobs have been applied for and accepted within three hours (source https://bit.ly/3aor3hz).

The official Sainsbury recruitment page is **www.sainsburys.jobs** but the fraudsters are also recruiting at www.sainsburysjobss.com**.**

Media:







Related Sectors:

Business & Finance :: Consumer Technology :: Coronavirus (COVID-19) ::

Related Keywords:

Trademarks :: Domain Names :: Domains :: COVID-19 :: Coronavirus :: Scams :: Brand Protection :: Phishing ::

Scan Me:

The speed within which we read online content makes it difficult to identify subtle points that would lead us to be suspicious of the website we are visiting. This fraudulent Sainsbury website has a misspelling using a double “S”. A Whois (record of domain information) search reveals that the domain name was registered by Babaar Axmed on 7 February 2020.

Domain Name: SAINSBURYSJOBSS.COM
Registry Domain ID: 2489900632_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.beget.com
Registrar URL: www.beget.com
Updated Date: 2020-02-07T20:31:24Z
Creation Date: 2020-02-07T20:31:23Z
Registrar Registration Expiration Date: 2021-02-07T20:31:23Z
Registrar: Beget LLC
Registrant Name: Babaar Axmed
Registrant Street: panpidova d5 kv20
Registrant City: klan
Registrant State/Province: moskovskioblis
Registrant Postal Code: 141407
Registrant Country: RU
Registrant Phone: +7.9030000108
Registrant Email: beget2017@mail.ru

Amazon has its fair share of fraud as can be seen by the fraudulent prize which is, at the time of publishing, still live at https://www.lumphalt.com/UK/UK_amaoni/?uclick=37ghb42t.

The types and variations of online fraud via domain names can no longer be ignored or be treated as trivial. Businesses have a responsibility to police the use of its brands online and to take appropriate enforcement action to protect its customers in the same way as they currently protect the more vulnerable, during COVID-19, by allowing them to shop in their stores before opening to the general public.

A business cannot prevent fraud from happening but can take certain strategic steps to mitigate the risks of doing business online. This includes implementing appropriate measures to increase responsiveness and to identify as many infringements or abuses as possible.

At Lexsynergy we advise our clients to develop a domain name management and enforcement strategy and policy to tackle domain name abuse, addressing a variety of aspects some of which are listed below:

- Ensure that there are no gaps in your domain name portfolio. If you own mybusiness.uk do you also own mybusiness.co.uk and mybusiness.london
- Implement a domain name watch service to identify identical or confusingly similar domain name registrations
- Conduct regular domain name audits for each brand to maintain the balance between registering domain names and the enforcement of your rights online.
- Prioritising the takedown of fraudulent websites
- Recover relevant infringing domain names
- Monitor less important or less serious infringements as you need to pick your battles
- Centralise the management of your domain names so infringements are easily identifiable.
- Communicate your domain name and enforcement strategy to relevant staff and external providers to avoid unauthorised registrations.

Domain names are not necessarily indicators of origin, but rather indicators of destinations so exercise care and diligence when accessing websites to make sure you land up at your intended destination.

If you are concerned about domain name abuse or online fraud and infringements reach out to our team for guidance or assistance at brandprotection@lexsynergy.com, +44 20 313 70459 (UK), +1 858 225 1318 (US) or +27 10 500 3913 (ZA).

Company Contact:

Lexsynergy Limited

T. +44 20 313 70459
E. info@lexsynergy.com
W. https://www.lexsynergy.com/

View Online

Additional Assets:

Newsroom: Visit our Newsroom for all the latest stories:
https://www.lexsynergy.pressat.co.uk