The BrandShelter five step guide to avoid becoming a victim of online crime

By Stuart Fuller

Stuart is the Head of Brand Services at CentralNic Group and has more than 10 years' experience in the Domain Name Industry.

We all love grabbing a bargain, but sometimes things that seem too good to be true, are exactly that. Our suspicious natures seem to disappear in the face of online discounts or adverts on Social Media where we are seduced by rock-bottom prices.

The growth in the digital economy continues at a pace, now estimated to be over $25 trillion, but how can brand holders, and consumer, be sure that the cash is being spent on genuine goods and not fuelling the illicit trade in counterfeit goods and online fraud. Counterfeiting is a $500bn problem alone for global brands today in Europe, according to the Organisation of Economic Co-Operation and Development (OECD), with no sign of it decreasing despite the huge efforts that organisations and authorities put into trying to mitigate the risks for customers.

"If it looks too good to be true, then it probably is" is an old mantra but it still holds so much weight in today's digital economy. Whilst some brand holders will go to great lengths to ensure that they stay protected online today, few take the step to educate consumers how to stay safe whilst looking for the online bargains at any time of year. To try and stay ahead of those who are intent to defraud, BrandShelter recommends following the five steps to stay ahead of the bad actors, phishers and cyber criminals in the digital world today.

1. Be socially aware – Cyber criminals use exactly the same methods as brand holders to drive traffic to their websites and to ultimately buy their products. This includes the use of Social Media to hook unsuspecting consumers, lured by fantastic offers. Social Media networks do not discriminate when someone wants to initially set up sponsored advertising campaigns. So whilst it may appear on your timeline, look carefully at the wording of adverts. Many that are placed by those maleficent individuals will have spelling mistakes, poor grammar or even using Homograph domain names that mix Latin and Cyrillic scripts to decept – for instance adverts for bargain Moncler products on Instagram in the past have contained such errors as referring to the brand as Moncle, Moncleur and Monclerr, or using mixed script such as Monclear (the "l" is actually a capita"I"). Global brands do not make spelling mistakes like this in their advertising. Also, be conscious of following shortened URLs, especially on social media as you have no idea where you could end up in the digital world.

2. Trust no-one – Social Media expert Erik Qualman estimates that 90% of our buying decisions are influenced by peer reviews. The biggest opportunity and risk to the travel industry is TripAdvisor where independent,

individual, customer reviews can make or break a restaurant, bar or hotel. Likewise, our growing dependency on Social Media interactions leads us to let our guard down when dealing with a company who have a strong digital footprint – Twitter followers or Facebook and Instagram likes. Unfortunately, it is all too easy to simply buy a footprint in a matter of minutes. For just a few hundred dollars anyone can buy 5,000 Twitter and Instagram followers, 500 retweets, 5,000 Facebook likes and 50 Facebook comments. Their return on investment in some cases is just one sale. Likewise, fake positive reviews can also be bought online – one for TripAdvisor can be bought for just $20.

3. It's in your domain – The domain name used by organisations gives some very strong hints about the intentions of the seller. Cybercriminals will either use domain names that look like they belong to a famous brand, using mistypes such as MoncIer (the 'I" actually being a capitalised 'i') or Monc1er in advertising or use some of the new gTLDs which haven't yet been registered by the brands, such as dotBlackFriday or dotSale. One other tell-tale sign is when the domain name was initially registered. In most instances, domain names that are used by cybercriminals are registered within a couple of days of the launch of their "campaigns". Use a website such as www.whois.com to check a domain name that you suspect could be used for a cybercrime.

4. Secure your financial information – All reputable online retailer now use SSL protocol (HTTPS) on their log-in and payment pages to ensure that any personal and financial information transmitted across the internet is encrypted and away from snooping eyes. In July 2018, as part of their Chrome 68 update, Google changed its policy on ranking websites, meaning only those who use SSL are classed as being secure. This now means any visitor to a website can easily tell if a website uses SSL by either the words "not secure" in the browser bar, or if using a browser such as Safari or Internet Explorer, the presence of a padlock in the browser bar. However, there have been a growing number of cases where websites being run by cybercriminals have also been able to gain an SSL certificate so this check should not be used in isolation.

5. If it looks too good to be true – It probably is. Many high end, luxury, brands do not "do" sales, especially those that offer huge discounts promised by adverts on Social Media. These brands do not register domain names featuring the words "cheap", "discount", "outlet" or "sale". If you see a product being sold for significant discount, look at other websites and check how much they are selling the item for. Most genuine sale items will be sold within a small range of discounted pricing – anything significantly outside that cluster should set alarm bells ringing.

Cybercrime is an unwanted part of our everyday digital world and it is important that brand holders take the necessary steps not only to protect their revenues but also their reputations. By following these steps above, customers become part of the solution rather than the problem of the ever-growing counterfeiting economy.

Why use BrandShelter?

For over a decade, BrandShelter has been working with some of the most recognisable brands on the planet, to deliver domain name, security and brand protection solutions, advice, and create effective and risk mitigating policies. Our priority is to help our clients meet their digital and business objectives, using our industry expertise and knowledgeable staff to craft solutions that deliver.

About BrandShelter

BrandShelter manages hundreds of thousands of domain names for organisation across the world, providing expert guidance and a range of value-added products including SSL, Registry Locks and Brand Protection services. With global customer support desks, enterprise and premium DNS solutions and flexible billing options, BrandShelter is the natural choice for ambitious brands wanting to secure their online presence whilst taking advantage of the opportunities the global digital economy brings.

To find out more, contact:

Bonnie Wittenburg
Executive Vice President
Key-Systems USA, Inc.,
885 Harrison St. SE, Leesburg, VA 20175
Tel.: +1 703 297 8151
Email: bwittenburg@brandshelter.com

Andreas Soll
Business Unit Manager
Key-Systems GmbH, Germany
Im Oberen Werk 1, D-66386 St. Ingbert
Tel.: +49 (0) 6894 9396 930
Email: asoll@brandshelter.com

Web: www.BrandShelter.com
www.key-systems.net
Social: LinkedIn | Twitter