Online Brand Enforcement 2018

Protecting Your Trademarks in the Electronic Environment

Going phishing: countering fraudulent campaigns

CSC

Malia Ladd

World Trademark Review®

In an ever-changing online world, trust your digital brand with CSC®. Our experts will consolidate and secure your digital assets, optimize and promote your digital portfolio, and monitor for threats and enforce your rights.

Digital Asset Management

CSC has the solutions to manage your company's digital assets and protect you against cyber crime across every platform, from your web domain names to social media handles.

Online Brand Protection

CSC specializes in enhancing and securing your intellectual property with Internet monitoring for brand infringements and counterfeiting, as well as enforcing your rights online.

Cyber Security

CSC's proven services can help reduce risk to your digital assets, thus protecting you from DDoS attacks, expired SSLs, phishing, and email fraud.

For more information, please visit cscdigitalbrand.services or register for a complimentary cyber security audit of your digital assets at cscdigitalbrand.services/freeaudit

Contributing firm
CSC

Going phishing: countering fraudulent campaigns

Author
Malia Ladd

They are in the news every week – data breaches. They happen to our favourite stores and also our trusted email providers. Our credit card information can be stolen – or even worse, our personal data. Two new policies going into effect soon underline the fact that the phishing attacks and spoofing that lead to data breaches are only increasing in frequency – and there is no slowing down in sight.

In early October 2017 the US Department of Homeland Security directed all government agencies to implement Domain-based Message Authentication Reporting and Conformance (DMARC) by January 14 2018 – as well as secure federal website connections (HTTPS instead of HTTP) by the following month, and implement an enforcement policy within 12 months to protect citizens from phishing, email fraud and government agency impersonation.

On May 25 2018, the EU General Data Protection Regulation (2016/679) will go into effect for every company that deals with EU consumer data. This measure is intended to strengthen and unify data protection, giving control back to consumers and setting the standard for holding businesses accountable for data breaches. Companies will be fined €20 million or 4% of annual global revenue – whichever is greater – for any data breaches that occur after May 25. And there are also hefty fines for not being in compliance by the due date.

According to the Anti-phishing Working Group's (APWG) *Phishing Activity Trends Report Q4 2016*, phishing attacks increased 65% between 2015 and 2016 – reaching a total of 1,220,523 – and the most targeted industries were still retail, service and finance. Symantec has calculated that one in 131 emails contained malware in 2016, which was the highest rate of malware emails in five years. It also notes that fake invoice emails are the number one phishing lure (26%). Generic documents (13%) and mail delivery failure (10%) are also popular.

The data proves that phishing attacks which lead to the sort of data breaches that are appearing in the news daily make phishing the most common type of malicious cyberattack. Phishing remains an all-too-common vehicle for corporate data breaches, credit card fraud and identity theft, with scams getting more innovative and costly every year.

Here, phishy phishy phishy

Most phishing attacks are as typical as any other email you receive. That is why they are so prevalent. Cybercriminals have gotten more sophisticated, and gone are the days of phishing emails containing misspellings, improper English and incorrect brand colours.

Cybercriminals now nearly perfectly match brand logos, colours and email tone, and use meaningful messaging to match legitimate messages. It is called 'spoofing' – and customers are falling for it, which makes it extremely difficult for brands to combat on their own. Hence the new US and EU mandates intended to set the foundation for brand security.

Some of the most well-known brands around the world have experienced breaches resulting from phishing – and each crisis has reverberated around the globe. No one can forget the series of data breaches (plural) revealed by Yahoo! in 2016, which were collectively noted as one the largest data breaches to date. Early reports revealed that the breach affected over 1.5 billion users around the world, putting its business acquisition plans at stake. More recent reports say that every single Yahoo! user was affected, spanning Yahoo! Mail, Tumblr, Fantasy Sports and Flickr – which puts the number of consumers breached at 3 billion.

The Mirai distributed denial-of-service attack against Dyn, a domain name system service provider, brought the Internet to its knees across the East Coast of the United States in October 2016; it also brought a handful of prominent websites to a standstill, resulting in an immediate loss of about 8% of their business.

In January 2017, hackers attempted to access sensitive information by asking customers to change their Microsoft settings in an email which appeared to be a notification from Amazon.com letting customers know that an order had been shipped. Users were asked to open an infected attachment that would download the ransomware Locky Virus, which took personal documents hostage and demanded payment to have them released.

There was another widely known ransomware attack in May 2017. The WannaCry attack infected over 230,000 computers, bringing the UK National Health Service and other global websites to a grinding halt, before a curious web security researcher unintentionally flipped the kill switch by registering the domain name he found in the ransomware code.

The Google Docs hack is a more recent example of the sophistication of these attacks. Unlike typical phishing attacks, the Google Docs hack did not actually steal credentials; instead, its creators built an app that used Google processes to capture user information when the user clicked a link in the email, giving criminals access to email content, contacts and online documents. The deception spread quickly, with the malware automatically emailing a user's contacts, and about one million Google Docs users were affected within the hour before Google shut it down. It was spread through a believable message from a file sharing system asking users to click on the link to a file shared by a "friend".

When the EU General Data Protection Regulation is implemented in May 2018, companies will become accountable for these security breaches. Many organisations are well versed in the legal compliance with the regulation. However, far more may be failing to consider one of the driving forces behind it: the goal of increased cybersecurity at the foundation level, intended to ward off data breaches – in the form of hacking, phishing or malware attacks – before they gain steam.

What was first announced in May 2016 is now a very real standard with which EU businesses – and any company doing business in the European Union – will be required to comply with in a few short months. If a business falls victim to a cyberattack and a data breach occurs, that business will be paying for it.

Thanks to this measure, and the US Department of Homeland Security's directive for companies to implement DMARC, every corporation will soon have to put the right measures in place to prevent and combat phishing attempts.

> **Securing your digital property will reduce costs, giving you peace of mind that your brand is prepared to face the cyberattacks that will inevitably come your way**

Prevent – detect – enforce

Brands do not have to go about securing their digital assets alone. Using a provider that will first help you audit what you have, so you know what to protect, will go a long way towards keeping your brand and customers secure. A provider should also help you manage those assets, giving you the ability to keep secure sockets layer certificates up to date, as well as any other security measures you have in place. A streamlined approach and a single platform for securing, monitoring and enforcing your brand protections will help you keep track of, add or take away assets, and give you an easy way to keep an eye on things. Securing your digital property will reduce costs, giving you peace of mind that your brand is prepared to face the cyberattacks that will inevitably come your way.

Prevention and detection

Email fraud protection technology enables an email recipient to confirm a sender's identity, increasing the chances of legitimate email getting through while filtering out spoofed messages.

Illegitimate emails are detected by a combination of authentication techniques such as DMARC. This protection allows a sender to indicate that its messages are secured by Sender Policy Framework (a path-based email authentication technique) or DomainKeys Identified Mail (a signature-based email authentication technique), and tells a receiver what to do if neither of those authentication methods passes the message. In short, DMARC looks at active emailing domains and non-sending domains, as well as a company's defensively registered domains. Email fraud protection provides intelligence about all known, unknown and potentially fraudulent outbound mail streams claiming to originate from client-owned domains.

Yet not all domains are within your control, such as lookalike domains, subdomains of another domain and unaffiliated domains, among others. Email intelligence and proactive monitoring are key to detecting what is legitimate and what is not. Some detection techniques include:

- email SPAM traps and fraud feeds – an international network of email honeypots and SPAM traps to detect phishing bait emails as they are transmitted;
- logo matching and analysis – to detect misuse of logos and protected brand images;
- web crawling – a powerful monitoring engine that detects potential attacks as they occur;
- algorithm updates – rules of engagement for threat intelligence should be reviewed and updated regularly as phishing actors change tactics;
- identifying phishing URLs – phishing website URL capture through technology and manual curation of the thousands of results to weed out false positives, leaving a manageable list to decide to action against; and
- filtering for meaningful results – final results delivered through a customer portal for notification and action.

Malia Ladd
Global director, brand protection and enforcement
malia.ladd@cscglobal.com

Malia Ladd has over 15 years' experience partnering with Global 2000 companies and law firm clients to develop and maintain strong business practices for managing their intellectual property in the online environment. Ms Ladd's prior experience, working in both law firm and corporate environments with responsibilities primarily focused on brand protection and enforcement, has fuelled her desire to develop and implement strategies that make online brand protection more manageable and effective. Ms Ladd presents at numerous industry roundtables and legal events on a variety of topics relating to managing and protecting brands online.

> **Any unauthorised online content can damage your brand, so it is important to be able to remove infringing content without costly and time-consuming legal processes**

Enforcement

Know your enforcement options. For high-priority infringements where enforcement action is needed, brand owners have options for protection against phishing scams. It pays to seek advice from an enforcement specialist to understand when it makes sense to use one of the following enforcement mechanisms.

Website takedowns and after-action monitoring: Find a provider that has an extensive international network to shut down websites quickly, within a few hours of detection. Takedown services can be employed to suspend domain names that have been established for the sole purpose of distributing phishing, malware or other fraudulent content. If a company, as a client of a cybersecurity service provider, has previously authorised automatic mitigation action, the provider should be able to immediately undergo site takedown action, resulting in the removal of content or the suspension of the domain name. Once a takedown is confirmed, a good provider will keep checking for any reactivation.

Domain recovery services: The Uniform Rapid Suspension (URS) introduced by the Internet Corporation for Assigned Names and Numbers is an enforcement tool that offers a "lower-cost, faster path to relief for rights holders experiencing the most clear-cut cases of infringement" across new generic top-level domains (gTLDs). But, analysis shows that many brands are eschewing the URS in favour of the Uniform Domain Name Dispute Resolution Policy for tackling infringements, even in new gTLDs. So work with a partner that knows how to best leverage these policies for phishing domains that have been set up to attack your company. (URS is not a phishing takedown tool *per se*, but is a service offered by some providers.)

Brand abuse and content removal: Any unauthorised online content can damage your brand, so it is important to be able to remove infringing content without costly and time-consuming legal processes. Content removal is not as easy as merely contacting the website or social media platform where your brand information is improperly listed. It is helpful to have a partner that has a relationship with social networks, search engines and online marketplaces to remove infringing, abusive or fraudulent content.

Alert phishing data repositories: Partners within the anti-fraud community (eg, the APWG) should be alerted when sites engaged in fraud are identified. This communication allows for these service providers, antivirus vendors, browser security toolbars and web browsers to implement proactive blocks on sites that are actively engaged in fraud, diminishing the site's ability to collect user details from potential victims. Find a partner that has a relationship with reporting agencies.

Forensics: A good partner should be able to perform post-mortem forensics and data recovery where applicable.

Conclusion

Phishing scams are increasing and becoming more sophisticated, and there are so many ways bad actors are employing phishing that it is imperative that businesses partner with an experienced provider to get secure against these attacks. Scammers are using traditional phishing emails to lure customers, as well as employing SMShing (ie, SMS or text message phishing) and vishing (ie, voice phishing over the telephone).

The US Federal Bureau of Investigation is also trying to combat business email compromise attacks (also known as 'spear phishing' attacks), which target people responsible for wire transfers. Individuals and companies should make sure their devices (including computers and phones) are patched with the latest security updates, to block attacks from every direction. But overall, awareness education for employees regarding how to respond to emails and phone calls requesting personal information, and engaging a provider to take down phishing sites as soon as they are identified, will keep companies secure and minimise any cyberattack impact on customers. **WTR**

CSC℠

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