Anti-phishing/cybersecurity

Delivering a bespoke anti-phishing solution

Phishing in the delivery sector has increased exponentially during the COVID-19 pandemic with businesses and their consumers being targeted by a range of sophisticated scams. Andreas Juchli explains how Novagraaf's tailored approach to online brand protection was able to help a leading international courier and logistics brand to defend its business and customers from online fraud and phishing scams.

As businesses and consumers have moved online in ever greater numbers to order goods and services during the COVID-19 pandemic, so too has risen the risk of phishing, fraud and other forms of online brand infringement. From fake email alerts to deception through unauthorised apps, new and increasingly sophisticated digital threats are impacting every touchpoint along the online value chain, including the delivery sector.

Case study: Benefits in brief

Through our bespoke cybersecurity solution, Novagraaf was able to deliver an almost 70% reduction in the effectiveness of phishing attacks for an international logistics brand.

Additional benefits included:

- a decrease in fraud-related notifications through customer support channels;
- authentication and, therefore, faster payment of legitimate invoices;
- increased security of digital assets; and
- a diversion of the scammer's attention towards competing brands.

Our tailored solution involves:

- the proactive monitoring of paid ads on social media;
- ongoing monitoring of domain name registrations and phishtanks (directories of phishing scams); and
- the creation and management of a phishing mailbox to which the public can report perceived infringements for rapid action and control.

The company: A giant in its field

The company is a globally famous logistics brand, which is frequently impersonated in scams. Thousands of consumers are being targeted by fake emails purporting to be from this company every day, asking them to click on links to receive information about a pending package or to download a fake app to better track its journey. The sophistication of the deception has misled many email recipients into entering their personal details and, in many instances, making a payment to ensure a fake package's delivery. Many others have been forwarding such emails immediately to the delivery company to verify the email's authenticity before acting, leading to hundreds of emails landing at its customer support inbox.

Such a high volume of emails can pose challenges for any company, as it requires the recipients to verify each alert to gauge whether or not it is legitimate, taking up vast amounts of internal time and resources. Anxious consumers require fast response times, and anything that is not can lead to negative customer feedback. More generally, legitimate communication is also likely to be considered with scepticism by customers and their consumers, as the brand begins to be associated with a high volume of spam. It was clear to the brand owner, therefore, that the issue needed to be addressed.

The challenge: New digital solutions for new digital threats

The traditional focus of online brand protection services has been to identify and takedown infringing products or content online; for example, by focusing on unauthorised domain name registrations or deceptive lookalike sites. While such services still have a critical role to play, Novagraaf understood that in this instance, the client also needed a solution that would also help it to manage and process the high volume of consumer alerts.

Novagraaf
A NovumIP Company

In addition, social media screening identified the activity of scammers on Facebook, Instagram and China-specific apps WeChat, Weibo, and RedBubble. As is always the case with scampages online, it takes multiple and persistent enforcement to stem such activities. Over time, cybercriminals may give up their strategy of setting up social media pages or websites that impersonate a brand, for example, but rather than give up completely, they will typically switch to generic pages that mention the brand in a post ('scamposts') and thus require advertising to grab consumer attention. By adapting our searches, we were able to ensure that our digital monitoring services also included such new scams, even if their creator did not use the brand name as a keyword, but instead used its logo in a post, for example.

We also investigated ways to take the burden off the brand when it came to consumer notifications. Key strategic drivers here, included the need to:

- act quickly against the scams once notified, thereby reducing their effectiveness, as opposed to waiting for the brand owner to identify potential scams and forward them to us; and
- submit the emails as evidence to the internet service providers (ISP) that needed to be informed to shut down the mail servers being used to send the spam emails. ISPs will not accept emails forwarded via a third party as valid evidence due to the potential for them to be edited, but instead require emails to be submitted as digital files for analysis.

The solution: A tailored service

As a result of our analysis, we set up a monitoring service that focused specifically on brand impersonation online and a dedicated anti-phishing mailbox that we manage on the client's behalf.

Domain monitoring quickly yielded early results. Suspicious new domain registrations were identified promptly, added to Novagraaf's brand protection case management system and immediately enforced where signs of malicious behaviour were detected.

Social media monitoring facilitated the enforcement of unauthorised activities, including paid ads, via available tools (such as Facebook's Commerce & Ads IP Tool).

The establishment of the **anti-phishing mailbox** ensured that our team was alerted directly about scampages and other infrastructure-based attacks. Automated enforcement mechanisms were set up, including reporting to the various ISPs, and we also produced a 'how-to' guide for the client's website to guide recipients through the necessary technical steps for submitting the scam emails as evidence to ISPs.

We were able to quickly track success by contrasting the number of neutralised scams against notifications to this inbox. For example, at the start of our work, only 12% of the emails forwarded linked to scam content that had already been shut down. That percentage is now 81%, meaning we have reduced the effectiveness of scams attacking the brand by almost 70%.

In addition:

- Social media scams using the brand have disappeared after over a year of relentless monitoring and takedown. Those scam posts used to have engagement levels with more than 500 'likes', thereby duping many victims.
- By channelling phishing and other IP issues to us via a dedicated mailbox, the workload of customer support personnel has been reduced, enabling them to focus on supporting the needs of actual customers.
- The amount of outstanding invoices has also been reduced, as we forward any 'suspicious content' that is actually legitimate to the corresponding departments who can then directly address the issue with the client one-to-one.
- Corporate domain names and websites have been upgraded with more sophisticated security features, and social media profiles are undergoing verification processes to ensure the brand's outward-facing appearance is more coherent and trustworthy.
- Overall, our constant and consistent approach to enforcement has also reduced the amount of phishing and fraudulent activity, as scammers turn to 'easier' targets.

Based on a thorough assessment of threats posed to this logistics company, we were able to tackle phishing scams effectively via an adaptive, multi-pronged approach that tackled deceptive digital content rapidly and proactively to reduce the profitability of scams.

When it comes to online brand protection, there is no such thing as a one-size-fits-all solution, because every brand owner and its customers can be targeted in different ways. That's why it's important to work with a specialist provider who not only understands the challenges that companies face online, but is also flexible enough to tailor its solutions to meet their exact needs. To find out how Novagraaf could help you to protect your brand and customers online, contact us today at brandprotection@novagraaf.com.

Novagraaf
A NovumIP Company