BIZCOMMUNITY

Brands continue losing customer loyalty to cybercriminals, report reveals

By Duane Nicol

1 Jun 2021

It's not enough to protect your brands and trademarks in real life if you're a marketer or brand owner in 2021, you have to build a fort around your online assets too. Brand marketers are increasingly losing leads, brand affinity and customer loyalty to cybercriminals who impersonate their brands to scam their customers and prospects.

Photo by Jefferson Santos on Unsplash

Some of South Africa's and the world's best-known brands came under unprecedented attack in 2020. As the world truly embraced digitisation, cybercriminals impersonated trusted brands at increasing rates in their efforts to steal customer information and defraud them.

How big is the problem? Mimecast has released a new report entitled *The State of Brand Protection 2021* that takes a look at the dramatic rise of online brand impersonation and how companies can defend themselves. Data is based on analyses of Mimecast's customer email traffic as well as public data.

The report shows that 94% of South African companies are concerned about counterfeit websites imitating their brands, up from 84% in 2020. Using Mimecast's Brand Exploit Protect (BEP) web-scanning tool, it highlights how monthly email impersonations spiked around the early months of the pandemic.

Companies on the BrandZ Top 100 Most Valuable Global Brands 2020 list experienced a 381% spike in brand impersonation attacks during May and June 2020, over January and February respectively.

Data management is at the heart of cloud security

Johan Scheepers 1 Dec 2020

In Mimecast's *State of Email Security 2021* survey, 73% of South African respondents reported that they were aware of at least one web or email spoofing attack using their domains or lookalike domains. Sixteen-percent said they identified more than 10. And that's only the ones they knew about.

Furthermore, 99% of South African businesses are worried about the risk of bad actors spoofing their company's email domain, up from 78% in 2020. Mimecast threat intelligence shows the number of brand impersonation emails per month detected en route to Mimecast customers globally rose 44% in 2020 over 2019 to an average of nearly 27 million. The unfortunate result: monthly unwitting clicks on dangerous links soared 84.5% in 2020.

The impact of brand exploitation can cause untold damage to brands at a time when many businesses are already suffering due to the pandemic. The effects include a loss of trust, damaged reputation and could create doubt around organisations' efforts at taking all reasonable steps to protect the interest of data subjects in line with PoPIA requirements.

Brands are losing trust - and business leads - to cybercriminals

As harmful as lost trust can be to a brand's reputation, lost business leads are a far more tangible pain point. Every clickthrough from a fake email to a spoofed web page can steal a marketer's lead. In upcoming brand trust research conducted by Mimecast, 50% of European consumers said they would stop spending money with their favourite brand if they fell victim to a phishing attack involving that brand.

All brands are at risk

If your brand has an online presence, it's at risk. Between 1 October 2020 to 31 January 2021, Mimecast found approximately 2.9 million email phishing attempts that impersonated a top 100 brand - an average of 715,600 email phishing attacks every month. Smaller organisations also face the financial and reputational repercussions of brand exploitation and can be less equipped to handle the issue.

Brands don't realise the extent of the problem

In the *State of Email Security* report, nearly half of respondents (47%) saw an increase in the volume of spoofed emails that misused their organisation's brand during the past year, and 38% saw an increase in spoofed web domains. Others may not be paying close attention to the problem. After all, while brand impersonation 'in real life' is tangible - counterfeit goods, trademarks and copyrights are obvious to brand marketers - brand impersonation online is invisible until you proactively look for it.

There's a clear gap in brand safety

Despite the rapidly increasing virulence of brand impersonation attacks and the growing list of potential consequences, many small and midsize companies remain oblivious to the danger threatening their brands. At the same time, some

consumers remain unaware of the threat and are unsure what checks they should be carrying out to determine email and website legitimacy.

Brand monitoring/protection services are a must

Services that provide monitoring to identify brand impersonation, including third-party brand protection technologies and the Domain-based Message Authentication, Reporting and Conformance (DMARC) email protocol, are a must for online brand safety. They shed light on the severity of the issue and can help brands mitigate the problem more rapidly.

The bottom line? Brand impersonation is a scary thought – but businesses that put the right measures in place and increase collaboration between marketing and cybersecurity professionals can weather the storm. The time to act is now.

ABOUT THE AUTHOR

Duane Nicol is a cybersecurity expert at Mimecast.