ACADEMIA | Letters

Utilising BIMI-VMC as a Cybersecurity Tool for Brand Protection

Ifeanyi Emmanuel Okonkwo, Nnamdi Azikiwe University, Awka, Nigeria;
University of Cape Town, SA
Blessing Udo, University of Uyo, Nigeria

Introduction

Emerging technologies have disrupted traditional patterns of human interaction and business activities as transaction cycles in today's business world are almost completely digitized. With a digital economy comes the need to ensure an impeccable brand reputation amidst the inundating challenges of cybercrimes, phishing, and malware. Email communication which is an important business tool for communication has become a vulnerability exploited by hackers for cyberattacks and has necessitated the need for businesses to establish a security in their emails, with built-in protections to help automatically filter out potentially malicious messages. Have you noticed certain brand logos next to emails in your inbox? Are you wondering what this new identifier signifies? The need for an additional layer of email authentication that can enhance brand recognition and trust for a business has necessitated an innovation – Brand Indicators for Message Identification (BIMI). BIMI is intended to make it easier for email recipients to easily identify authentic emails through brand identification. This article seeks to give an analysis of what BIMI entails, how it can be combined with validated trademark certification for email authentication and its benefits to businesses and government.

Academia Letters, January 2022

Corresponding Author: Ifeanyi Emmanuel Okonkwo, okonkwo.ie@gmail.com
Citation: Okonkwo, I.E., Udo, B. (2022). Utilising BIMI-VMC as a Cybersecurity Tool for Brand Protection. *Academia Letters*, Article 4690. https://doi.org/10.20935/AL4690.

BIMI-VMC

Brand Indicators for Message Identification or BIMI is an emerging email specification that enables the use of brand-controlled logos within emails using an authenticated domain name, while confirming trademark validation through Validated Mark Certificates (VMCs). In place of the Company's initials, the logo of the organisation is displayed alongside emails from the brand in the recipient's email client as an avatar. BIMI serves as an additional layer of email authentication for recipients to instantaneously verify the authenticity of a sender before opening or engaging such an email. (Jeremy Speres, 2021).

Previously, mailbox providers had developed their separate methods for representing logos in mailboxes, but it required each provider to maintain its own repository of logos. It also required that brand owners had to liaise individually with every mailbox provider to get verified and had to meet each provider's specifications. The process of brand owners verifying with the mailbox provider was tedious and complex, hence BIMI was introduced to serve as a standardised form for email authentication. Without a standardized means of discovering and publishing each brand's preferred logo, each mailbox provider or email interface (MUA) interested in displaying logos is required to create a unique system for logo management and display. This results in complex, hard to maintain, proprietary systems that frequently leave brands frustrated with the logos associated with their emails. BIMI helps standardize logo display for participating organizations. (BIMI, 2019) Through the mark verifying authorities (MVAs) examination for a Validated Mark Certificate is also made to ascertain - the legitimacy of a logo; that the applicant has rights to the trademark logo; and that the trademark logo is associated with the domain name in question.

Thus, BIMI gives verified brand owners control over how their brand is represented in messaging services. For participating mailbox providers like Yahoo or Gmail that means BIMI adopters will have the logo they choose displayed in their recipients' inboxes. The United States, United Kingdom, Canada, Australia and Germany have already adopted BIMI. Multinational companies including Yahoo and Google-GMAIL, et al, have adopted BIMI.

Cybersecurity Concerns

83% of global infosec respondents experienced phishing attacks in 2018 and the number keeps increasing (PurpleSec, 2021). Kaspersky, global cybersecurity and digital privacy company, reports that leading countries in Africa, including Nigeria and South Africa, have experienced eight million malware attacks in 2020 and 102 million detections of potentially unwanted programs, and that fake notifications from email services are one of the most common spammer

Corresponding Author: Ifeanyi Emmanuel Okonkwo, okonkwo.ie@gmail.com
Citation: Okonkwo, I.E., Udo, B. (2022). Utilising BIMI-VMC as a Cybersecurity Tool for Brand Protection. *Academia Letters*, Article 4690. https://doi.org/10.20935/AL4690.

trucks used by hackers to harvest usernames and passwords (personal data) of unsuspecting recipients (Kerpersky 2020). These cybersecurity concerns are global and technology and communication continues to undergo disruption, the cybercrime activities continue to adapt and strife.

The Weakness of Trademark Laws in Cyberspace

With the digital economy comes the need to create an online presence and domain names on the Internet in a manner similar to a physical address, where a proprietor may sell its brand products and services. Trademark protection in the digital space becomes not only essential but inevitable.

Just as a trademark identifies a product as belonging to a specific company and recognizes the company's ownership of the brand, domain names also serve this purpose. However, there is no synergy between domain name registrars and trademark registries to ensure that existing trademarks are not registered and used as domain names and vice versa. Trademark laws are wired as remedial measures when an infringement has occurred, as against preventive measures. This is the lacuna of the Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994 (TRIPS) which has been adopted and domesticated by member-states.

Domains on the internet are regulated by the Internet Corporation for Assigned Names and Numbers (ICANN). All regional Registrars are subject to the overriding regulations of the ICANN. Disputes arising from domain and trade mark related breaches, are administered by administrative panels approved by ICANN and these panels are bound by the provisions of the Uniform Domain Name Dispute Resolution Policy and the UDRP Rules of Procedure. One of such recognised panels is the World Intellectual Property Organisation. While this is an effective way to handle domain name disputes, having a synergized medium to ensure that existing trademarks are not registered and used as domain names, would be a more proactive regulatory pattern.

Benefits of Deploying BIMI-VMC

The deployment of BIMI by organisations and businesses would serve as a preventive measure for brand exploitation, and adoption of BIMI is accompanied with certain advantages. First, phishers would find it difficult to effectively use the brand name or logo for their illegal-email commercial activities as the technology would raise flags to email recipients.

Secondly, recipients are more likely to trust the source of the emails that carry the validation marks, thus, ensuring brand trust over the activities of the true proprietor. Moreso, email

Corresponding Author: Ifeanyi Emmanuel Okonkwo, okonkwo.ie@gmail.com
Citation: Okonkwo, I.E., Udo, B. (2022). Utilising BIMI-VMC as a Cybersecurity Tool for Brand Protection. *Academia Letters*, Article 4690. https://doi.org/10.20935/AL4690.

open rates and engagement will increase.

Finally, the global adoption of BIMI-VMC will lead to a synergy between the trademark-regulatory bodies and the internet-domain regulators, thus, offering a platform to improve the lacuna in the present domain registration and dispute system.

Conclusion

The digital economy has fostered seamless transactions and communication patterns, which in the same vein has also led to an increase in social engineering cyber-attacks leading to a distrust of emails. This aligns with the well-known reality that humans are the weakest link in cybersecurity systems, as scammers are always devising intelligible means of tricking email recipients.This has necessitated organisations and email marketers to seek new strategies to ensure email authentication and brand recognition. Regardless of email exploitation by cyber attackers, brand owners now have the opportunity to include an additional layer of email authentication that can increase brand trust and prevent brand spoofing, while enhancing and protecting the goodwill in their trademarks and logos - BIMI-VMC is that opportunity.

Corresponding Author: Ifeanyi Emmanuel Okonkwo, okonkwo.ie@gmail.com
Citation: Okonkwo, I.E., Udo, B. (2022). Utilising BIMI-VMC as a Cybersecurity Tool for Brand Protection. *Academia Letters*, Article 4690. https://doi.org/10.20935/AL4690.

References

Jeremy Speres, 'Everything you need to know about BIMI and validated mark certificates, how they increase brand trust, and which companies have adopted them' WTR (2021) available at https://www.worldtrademarkreview.com/brand-management/everything-you-need-know-about-bimi-and-validated-mark-certificates-how-they-heighten-brand-trust-and-how-companies-have-adopted-them accessed 1 October 2021.

BIMI Group 'All about BIMI' (2019) available at https://bimigroup.org/all-about-bimi/ accessed 17 October 2021.

PurpleSec 'Cybersecurity trends in 2021' (2021) available at https://purplesec.us/resources/cyber-security-statistics/ accessed 22 December 2021.

Kaspersky Newsroom - https://kaspersky.africa-newsroom.com/press/south-africa-kenya-and-nigeria-saw-millions-of-cyber-attacks-in-2020-and-the-year-is-not-over-yet?lang=en accessed on 22 December 2021.

Kaspersky Daily 'Online fraud: 5 most common spammer tricks' available at https://www.kaspersky.co.za/blog/phishing-spam-hooks/21617/ accessed on 20 December 2021.

Corresponding Author: Ifeanyi Emmanuel Okonkwo, okonkwo.ie@gmail.com
Citation: Okonkwo, I.E., Udo, B. (2022). Utilising BIMI-VMC as a Cybersecurity Tool for Brand Protection. *Academia Letters*, Article 4690. https://doi.org/10.20935/AL4690.