# J2 Software and SlashNext address growing threats of email compromise and phishing



J2 Software, in collaboration with the cybersecurity firm SlashNext, recently conducted a comprehensive webinar detailing the escalating threat posed by business email compromise (BEC) and advanced phishing attacks. This virtual event highlighted the transformative role of AI-driven solutions in enhancing cybersecurity, aimed at providing proactive measures against rapidly evolving cyber threats.

With cyber attacks reportedly occurring every 11 seconds, industry experts anticipate that cybercrime could surpass $10 trillion annually by 2025. Email remains a pivotal vector for these attacks, with research indicating that between 85% to 93% of successful breaches initiate via this medium. Often, perpetrators manipulate victims into utilizing alternative communication channels such as mobile messaging or web applications, effectively circumventing traditional email security protocols.

Small and medium-sized enterprises (SMEs) have emerged as key targets for cybercriminals, predominantly due to their perceived vulnerability. John McLoughlin, the CEO of J2 Software, underscored the necessity for heightened visibility in safeguarding essential components of digital operations, such as users, email, data, devices, and internet infrastructure. He reiterated the need for comprehensive protection, stating, "You can't protect what you can't see."

The phenomenon of generative AI and large language models (LLMs) has notably changed the landscape of phishing attacks, with cybercriminals now leveraging advanced tools like ChatGPT to craft targeted and sophisticated email scams. McLoughlin presented a striking case of deepfake technology employed in a scam, where a fraudster successfully impersonated a chief financial officer during a video call, resulting in a $25 million loss for a multinational firm. “The employee, believing he was interacting with genuine colleagues, was tricked into transferring the substantial sum,” he explained. This incident exemplifies the potential for AI to be misused in social engineering offences, where attackers replicate trusted figures during virtual engagements.

In response to these emerging threats, J2 Software and SlashNext are enhancing their service offerings. Their comprehensive cybersecurity suite leverages cutting-edge features aimed at thwarting modern threats. Key offerings include zero-hour protection that detects and neutralises BEC and social engineering attacks in real time, alongside malicious content filtering to block phishing links and malware.

Their security technology extends to mobile devices, recognising the rise of phishing attempts through SMS, commonly referred to as smishing. The SlashNext mobile application is designed to filter harmful messages directly on users’ devices, thus ensuring layers of privacy and security without contacting external systems. The recent Twilio breach, where attackers exploited the company's single sign-on system through SMS, underlined the critical necessity for robust mobile security measures.

Moreover, SlashNext’s browser extension utilizes on-device machine learning to conduct dynamic analyses of web pages, providing immediate protection against phishing attempts, particularly those involving URL redirection and credentials theft.

Within the framework of these technical advancements, the importance of user education was emphasised during the webinar. Cultivating a security-centric culture in organisations, where employees feel empowered to report suspicious activities without fear of reprisal, emerges as vital in strengthening overall defence mechanisms. Behavioural training is essential to fortifying organisational resilience.

To assist organisations in assessing their vulnerability to email and phishing threats, J2 Software offers a complimentary cloud email risk assessment, powered by SlashNext. Additionally, seamless integration options are available for organisations looking to enhance their existing security frameworks.

The collaborative efforts between J2 Software and SlashNext exemplify the application of AI in combatting the sophisticated tactics employed by cybercriminals today. With cyber threats becoming increasingly complex, businesses are urged to adopt innovative and adaptable security measures to protect their digital assets and personnel effectively.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.itweb.co.za/article/j2-software-slashnext-highlight-ais-role-in-combating-bec-and-advanced-phishing-attacks/mQwkoM6Y42a73r9A> - Corroborates the collaboration between J2 Software and SlashNext, the escalating threat of BEC and advanced phishing attacks, and the role of AI in cybersecurity.
* <https://www.itweb.co.za/article/j2-software-slashnext-highlight-ais-role-in-combating-bec-and-advanced-phishing-attacks/mQwkoM6Y42a73r9A> - Supports the statistic that cyber attacks occur every 11 seconds and the projection that cybercrime could surpass $10 trillion annually by 2025.
* <https://www.itweb.co.za/article/j2-software-slashnext-highlight-ais-role-in-combating-bec-and-advanced-phishing-attacks/mQwkoM6Y42a73r9A> - Confirms that email is a primary vector for cyber attacks and that 85%-93% of successful breaches initiate via email.
* <https://www.itweb.co.za/article/j2-software-slashnext-highlight-ais-role-in-combating-bec-and-advanced-phishing-attacks/mQwkoM6Y42a73r9A> - Highlights the vulnerability of small and medium-sized enterprises (SMEs) to cyber attacks.
* <https://www.itweb.co.za/article/j2-software-slashnext-highlight-ais-role-in-combating-bec-and-advanced-phishing-attacks/mQwkoM6Y42a73r9A> - Quotes John McLoughlin, CEO of J2 Software, on the necessity for visibility in cybersecurity, 'You can’t protect what you can’t see.'
* <https://www.itweb.co.za/article/j2-software-slashnext-highlight-ais-role-in-combating-bec-and-advanced-phishing-attacks/mQwkoM6Y42a73r9A> - Details the misuse of generative AI and large language models (LLMs) in phishing attacks, including the case of deepfake technology used in a scam.
* <https://slashnext.com/recorded-webinar-weaponizing-gen-ai-how-chat-gpt-and-ai-bots-transform-bec-and-advanced-phishing-attacks/> - Supports the use of ChatGPT and AI bots in creating sophisticated BEC and advanced phishing threats.
* <https://www.itweb.co.za/article/j2-software-slashnext-highlight-ais-role-in-combating-bec-and-advanced-phishing-attacks/mQwkoM6Y42a73r9A> - Describes the comprehensive cybersecurity suite offered by J2 Software and SlashNext, including zero-hour protection and malicious content filtering.
* <https://www.itweb.co.za/article/j2-software-slashnext-highlight-ais-role-in-combating-bec-and-advanced-phishing-attacks/mQwkoM6Y42a73r9A> - Explains the importance of mobile security measures, including the SlashNext mobile application and the recent Twilio breach.
* <https://www.itweb.co.za/article/j2-software-slashnext-highlight-ais-role-in-combating-bec-and-advanced-phishing-attacks/mQwkoM6Y42a73r9A> - Details the use of SlashNext’s browser extension for dynamic web page analysis and protection against phishing attempts.