

Media Title : The Star  
Headline : Why phishing works so well  
Date : 18 August 2026  
Section : News  
Page : 14



PHISHING is a type of cybercrime in which perpetrators imitate reputable businesses to deceive individuals into disclosing personal information, including passwords, credit card numbers, and banking credentials.

A study published in the journal *Cybersecurity* reveals that phishing is among the most prevalent techniques employed by cybercriminals nowadays. Phishing attacks have grown from simple fraudulent e-mails to highly sophisticated schemes that involve phoney websites, SMS scams (smishing), and phone calls (vishing).

In Malaysia, phishing has become a serious concern, particularly through SMS scams and fraudulent banking messages. According to Bank Negara Malaysia, online financial scams have resulted in substantial losses among Malaysians, with phishing identified as a major contributor.

Phishing works because of the use of social engineering rather than just technology. Cybercriminals manipulate emotions such as fear, urgency, and trust to influence victims' decisions. For example, individuals may receive messages claiming their bank accounts have been compromised, prompting immediate action without verification. This

# Why phishing works so well



manipulation highlights that phishing is not only a technological issue but also a psychological one. Phishing also frequently targets vulnerable groups like the elderly and those with low digital literacy.

From an international and regional legal perspective, phishing poses major challenges due to gaps in existing regulations. In their *Research Horizon* paper, "Legal Accountability and Policy Gaps in Social Engineering-Based Phishing Cybercrimes" (June 2025), Purwadi et al highlights the

exploitation of psychological manipulation in social engineering-based phishing that current cybercrime laws often fail to address. While most legal frameworks focus on technical hacking, phishing relies on deception and human vulnerability, making it harder to prosecute.

Additionally, research in *Cybercrime: A New Challenge of Criminality in the Digital Age* (International Conference on Cybersecurity and Cybercrime) notes that, although phishing is classified under fraud and cyber-

crime offenses, enforcement is difficult due to its cross-border nature and the anonymity of perpetrators. Hence, addressing the threat of phishing requires a multi-level approach involving individuals, organisations, and governments.

First, public awareness must be strengthened. Research published by Fauzan Prasetyo Eka Putra and colleagues in the journal *Brilliance: Research of Artificial Intelligence* emphasises that user education is crucial, as informed individuals are better equipped to identify suspicious links and messages.

Second, organisations should enhance cybersecurity measures. According to research on phishing prevention strategies ("Phishing Attackers: Prevention and Response Strategies" in the *Journal of Artificial Intelligence General Science*), combining technological solutions – such as multi-factor authentication and advanced e-mail filtering – with user awareness is the most effective defence against phishing attacks.

Finally, governments must improve legal frameworks and

international cooperation. Since phishing often involves cross-border activities, stronger collaboration among countries is essential. Establishing mechanisms for information sharing and joint investigations can significantly improve efforts to combat cybercrime.

To reiterate, while legal frameworks and technological advancements provide some level of protection, they are not sufficient on their own, as they often fail to address the human element of security, which is crucial in preventing phishing attacks.

Combating phishing requires a combination of awareness, strong policies, and international cooperation. In a world where a single click can have serious consequences, understanding and preventing phishing is more important than ever.

**NUR DALILA WAHIDA  
MOHAMAD GHAZALI and  
DR MOHD ISTAJIB MOKHTAR**  
Department of Science and  
Technology Studies  
Faculty of Science  
Universiti Malaya