PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: Phishing attacks rising since pandemic struck
Publication/Portal: The Malaysian Reserve
Date: 2 September 2021

Language: English
Section: News
Page: 6

Phishing attacks rising since pandemic struck

by LYDIA NATHAN

THE pandemic has seen 65% Malaysians reporting an increase in phishing emails directed at employees, proving it an effective cyberattack method despite being around for almost three decades.

Sophos' Phishing Insights 2021 was conducted on 5,400 information technology (IT) professionals around the globe to provide the latest insights with a real-life case study.

Sophos principal research scientist Chester Wisniewski said phishing has been successful because of its ability to continuously evolve and diversify, tailoring attacks to topical issues or concerns, such as the pandemic and playing on human emotions and trust.

"Organisations want to see phishing attacks as a relatively low-level threat but that underestimates their power. Phishing is often the first step in a complex, multi-stage attack.

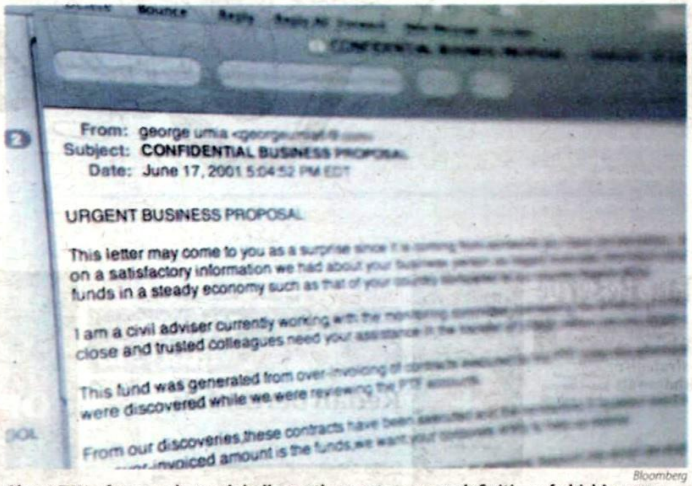
"According to Sophos Rapid Response, attackers frequently use phishing emails to trick users into installing malware or sharing credentials that provide access to the corporate network.

"The team has seen first-hand how a seemingly innocuous email can ultimately lead to a multi-million-dollar ransomware attack. Cryptojacking, data — and even financial — theft are all potential outcomes after a phishing attack has opened a door for adversaries," Wisniewski said in a statement.

Seventy percent of the survey's respondents reported an increase in attacks on organisations since the pandemic began, with all sectors being affected.

"The central government experienced the highest increase at 77% followed by business and professional services at 76% and healthcare at 73%," the report said.

Sophos Labs Research showed that cyber criminals were quick to take advantage of opportunities due to the impact of the pandemic.



Bloomberg

About 76% of respondents globally say the most common definition of phishing was emails that falsely claim to be from a legitimate organisation, combined with a threat or request for information

According to the survey, IT professionals across Malaysia have not been able to agree on the exact definition of phishing.

The survey said 76% of respondents globally said the most common definition of phishing was emails that falsely claim to be from a legitimate organisation, combined with a threat or request for information.

"Sixty percent consider Business Email Compromise attacks to be phishing, and more than half (55%) think threadjacking, which is when attackers insert themselves into a legitimate email thread, as part of an attack is phishing," the survey stated.

Additionally, the survey revealed 90% of organisations globally have implemented a cyber awareness programme to address phishing concerns.

"Despite 97% of organisations running cyber security programmes to address this concern, in light of the survey results, phishing awareness and education programmes need to consider the wide range of perceived phishing definitions and include training for non-technical employees that explain the different facets of phishing and email attacks in general," it said.