Pandemic and beyond : phishing in a larger pond

Yang, Jennifer Hui; Teo, Yi-Ling

2020

Yang, J. H., & Teo Y.-L. (2020). Pandemic and beyond : phishing in a larger pond. (RSIS Commentaries, No. 121). RSIS Commentaries. Singapore: Nanyang Technological University.

https://hdl.handle.net/10356/143763

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 121 – 15 June 2020

Global Health Security:
COVID-19 & Its Impacts

Pandemic and Beyond: Phishing in a Larger Pond

By Jennifer Yang Hui and Teo Yi-Ling

SYNOPSIS

The greatly increased reliance on technology for work, education, business, and social interaction during the COVID-19 pandemic has opened up opportunities for cyber criminals. It is highly probable that post-COVID-19, this reliance will lead to a hyperconnected world.

COMMENTARY

ALMOST OVERNIGHT, the nature of organisational cyber security has changed as a consequence of the COVID-19 pandemic. These shifts have essentially mutated the nature of the digital threat surface. Where there were once relatively contained and static IT environments to be managed along standardised protocols and policies, it is no longer the case now.

People have been dispersed outside such environments – each to their own non-corporate networks; the systemic protections of which may or may not be consistent and robust as their corporate ones. A sudden surge in mass working over private, insecure connections thus gives attackers an easy entry.

An Uptick in Phishing Attacks

Unsurprisingly, alongside the worsening of the global pandemic, there has been a huge spike in phishing worldwide. "Phishing" is a cyber crime technique whereby users are duped into disclosing sensitive data such as personally identifiable information,

password and bank details. Phishing is responsible for as much as 94% of coronavirus-related cyber attacks.

In Singapore, an email supposedly sent by Prime Minister Lee Hsien Loong asked for "contributions and thoughts" from Singaporeans to address the spread of COVID-19. Scammers pretending to be Ministry of Health (MOH) employees and the contact tracing team asked people to collect documents from MOH, and obtained their personal information in the process. These are just some of the many examples of 'phishing' that Singapore encountered during the COVID-19 crisis.

The importance of addressing the challenges posed by phishing has been emphasised by the Cyber Security Agency of Singapore (CSA). Since the outbreak of the COVID-19 pandemic, malicious cyber attacks taking advantage of the coronavirus theme have increased. Even before the pandemic, phishing has been an ongoing cyber security issue in Singapore. Phishing was one of the methods deployed in the SingHealth cyberattack, the most serious data breach in Singapore's history.

As an attractive target for cyber attacks, as many as 16,100 phishing URLs with a Singapore link were detected in 2018. For individuals, phishing poses the threat of unauthorised purchases, the stealing of funds, or identity theft. On the organisational and governmental level, phishing is often used by advanced persistent threat (APT) actors to gain a foothold in their networks as a part of a larger attack.

The Human Factor: Social Engineering and Phishing

Human nature does not change; people are hardwired to react in certain ways. In terms of tackling this "phishing pandemic", it helps to understand some behavioural psychology around it. Cyber criminals are not focused on exploiting systemic or technological vulnerabilities – they seek to exploit vulnerabilities in human nature.

This aspect of the phishing threat is using the tactic of social engineering. Essentially, social engineering broadly describes the ways in which people are manipulated into carrying out certain behaviours. In the context of cyber security or information security, social engineering is about getting people to disclose sensitive information or be exposed to malware.

Social engineering appeals to the victims' emotions; the stronger the emotional response (positive or negative) induced in the recipient, the greater the probability is for the recipient to not think clearly and carefully. An example of an emotional response is fear.

Fundamentally, phishing taps into the fears people have to such a degree that they are unable to carefully discern the signs of scam e-mails. Such e-mails appear to be from legitimate organisations or authorities that possess personal or confidential information of the recipient (banks or government agencies, for example), or whose services provide quality of life to the recipient (for example, those provided by Amazon, Apple, or Netflix).

For example, scammers took advantage of some common keywords used in the COVID-19 pandemic and paired them with terms such as 'masks', 'loan', 'unemployment' and 'cure' to bait information seekers.

Tackling Phishing Post-COVID-19

This evolution of the attack surface is suddenly altering established cyber security practices. Alongside requiring employees to be more vigilant and proactive about their non-office cyber security risks, how else should organisations go about managing the cyber security of a very differently structured and less coherent attack surface?

Future responses should be two-fold. Firstly, organisations must actively support employees with resources and guidance. Remote working will persist, and such support as well as education about cyber risks is a long-term matter. Organisations must also think about redesigning security architectures: the environment around users could be tweaked to ameliorate the risk of phishing triggers reaching them.

Here, using a variety of tools such as secured exchange servers, host-based security tools and email scanners that actively scan attachments for viruses and block harmful emails can go some way in preventing phishing threat to organisations. Also, using artificial intelligence tools to track active phishing sources and differentiate between real and fake websites could help protect users against phishing attacks.

Secondly, there is the need to promote understanding of why we react in a certain way to phishing triggers, towards changing our behaviour to avoid falling victim. Ongoing public awareness campaigns and user awareness training on phishing must highlight such psychological biases, especially optimism bias (the belief that one is immune to falling prey to online scams), and provide applicable examples of how phishing can be avoided.

After all, the end of the COVID-19 pandemic will not mean the end of human vulnerability to cyber-enabled attacks. Hopefully, awareness of phishing is sharpened as one result. We should expect phishing tactics to become more sophisticated and cyber criminals more ingenious, enabled as well by technological advances.

Black swan events (unknown unknowns) could very well arise, any global crisis will have a cyber aspect, and protection plans must integrate cyber security. Cyber criminals see opportunity in every crisis, and cyber practitioners must anticipate such eventualities and endeavour to be one step ahead, or at least prepared to a point where they can respond appropriately.

Jennifer Yang Hui is an Associate Research Fellow and Teo Yi-Ling a Senior Fellow with the Centre of Excellence for National Security (CENS) and Future Issues and Technology (FIT) Cluster, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. This joint contribution by CENS/FIT is part of an RSIS Series.