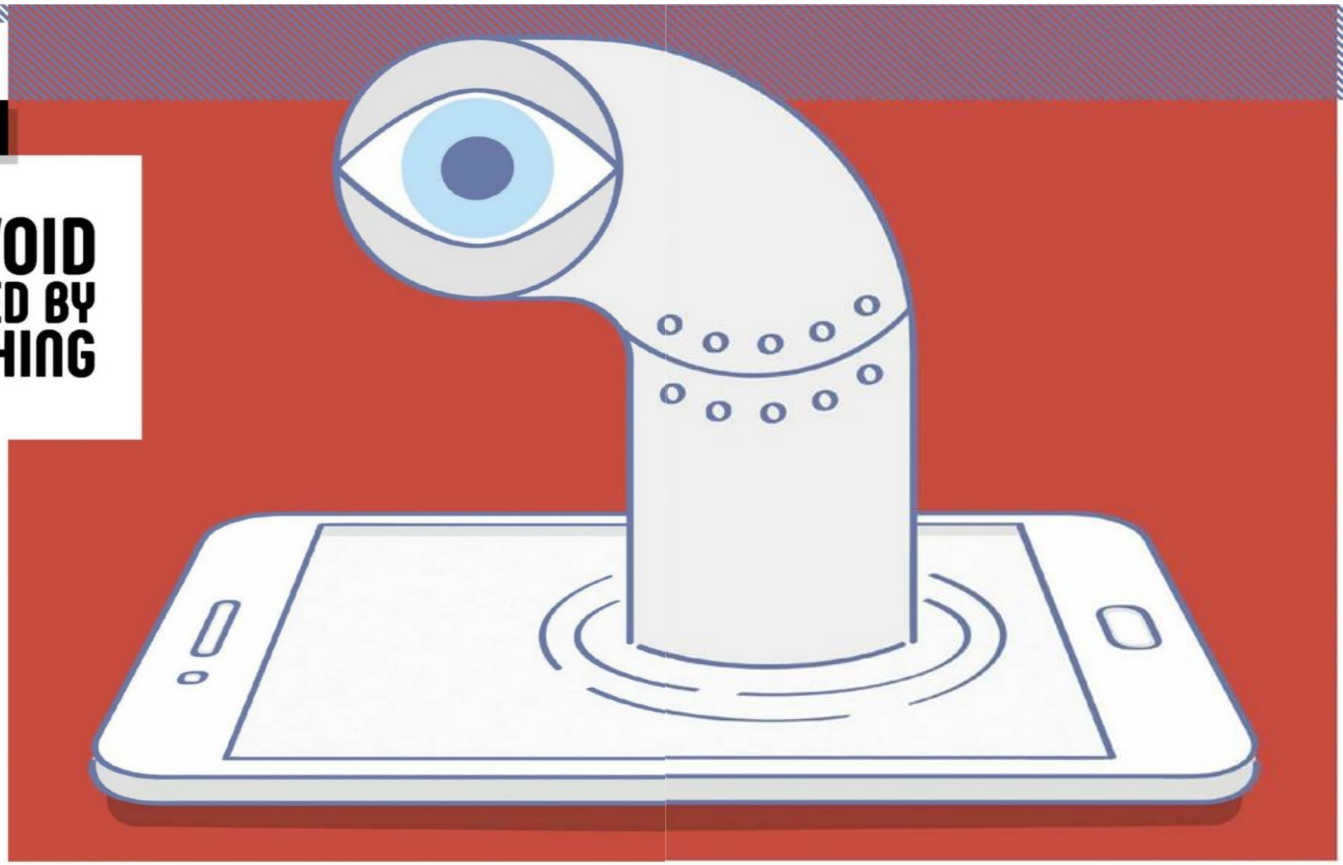
PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: How to avoid getting hooked by mobile phishing
Publication/Portal: SME Magazine
Date: 1 July 2019

Language: English
Section: N/A
Page: 46

BY BRIAN GLEESON

HOW TO AVOID GETTING HOOKED BY MOBILE PHISHING



The first recorded use of the term 'phishing' was in 1996, in the earliest days of the Web. So why is this 20+ year-old method of online fraud still with us? For one very simple reason: it works very effectively. It's one of the most reliable methods a hacker can use to steal access to personal or business digital accounts. The FBI has estimated that the total losses from business email compromise alone – a highly targeted variant of phishing – have exceeded US$12 billion globally.

Phishing has become an industrialized process. It's estimated that around one in every 2,000 emails is a phishing email, and over a million fake websites are created every month to try and trick users into giving away personal information. A recent study showed that 25% of phishing emails bypass Microsoft Office 365 security. For criminals, it's a numbers game: they just need to distribute enough emails and links to fake sites, and wait for people to fall into their traps. And as more and more transactions are conducted via mobile devices, mobile users are being increasingly targeted – with increasing success.

There are several reasons for the rise in mobile phishing attacks. First, the ergonomics and smaller screen size of mobiles makes it harder for users to inspect an emailed URL that they are asked to click on – and easier for scammers to attract unwitting visitors to their fake sites. Second, mobile devices are typically used to connect to multiple email accounts, enabling hackers to target both business and personal accounts. And finally, smartphones can also be targeted by phishing texts, and by malicious apps too, giving the attacker a range of methods to try and get victims hooked. Let's take a closer look at each of these three main phishing vectors.

SPEAR PHISHING BY EMAIL Email phishing attempts can target both consumers and enterprise mobile users. Spear phishing attacks on consumers usually involve stolen databases of consumer names, phone numbers and accounts to create very targeted and convincing messages. For example, hackers will use a stolen database of credentials from a major breach – such as the recent breaches at Equifax or Yahoo!– to send mobile users targeted messages using that brand's name or personal information about the recipient.

Attacks against enterprise users involve building a profile of individuals from corporate websites and LinkedIn, Facebook and Twitter profiles, and then creating targeted emails that purport to be from a senior executive, requesting an urgent payment or service and directing the target to make a legitimate-looking but fraudulent transaction. Alternatively, these attacks can appear to originate from the enterprise IT team, directing users to URLs to collect passwords and VPN credentials.

SMS PHISHING So-called 'smishing' – SMS, text and iMessage phishing – is an increasingly common vector for delivering malicious URLs to mobile device users. Again, there are several varieties, from large-scale attacks resembling spam email attacks that incorporate ruses such as password resets or account security updates, through to far more targeted and personalized attacks.

APP PHISHING Mobile apps have become a hugely fruitful channel for the distribution of phishing links. After all, most mobile devices have a huge number of apps installed, and with over 3.8 million apps available to Android users on Google Play, over 2 million apps on the Apple App Store, and over 1.5 million apps on other third-party stores, there are plenty of opportunities for hackers to introduce malicious content.

Yet again, there are multiple varieties to be aware of. Encrypted communication phishing takes advantage of the encrypted nature of WhatsApp, Telegram and Signal to send convincing messages claiming to be from customer support or a known online service, which cannot be flagged by the enterprise because they are encrypted.

Fake social media phishing uses apps like Twitter, with attackers setting up fake accounts purporting to be genuine customer support services. And of course, there are entirely fake apps, and even fake third-party app stores. The latter often use the technique of distributing a configuration profile that is installed on a device by visiting a web page. Once such a profile is installed on the mobile device, the user can then access the third-party app stores and download apps to the device. These apps are not subjected to any verification or security review, and can be used to deliver phishing URLs, malicious content, and even to install malicious apps on the user's device.

NEXT-GENERATION PROTECTION AGAINST BEING PHISHED To protect individuals and organizations against phishing attacks, a four-stage approach is needed.

1) The first line of defense is robust, server-based anti-phishing protection. This must incorporate anti-spam filtering, phishing detection, BEC phishing detection and spear phishing detection.
2) Second, device-based URL protection is a must, given that the vast majority of phishing attacks direct a victim to a URL that provides convincing content to trick the user into disclosing credentials or installing malicious apps. URL protection which spans not just an enterprise email account but also personal email accounts, SMS/text/iMessage and the content that apps download is crucial.
3) The third stage is device-based security profiling, in order to detect whether devices have been purposely or inadvertently made vulnerable to targeted attacks or traffic interception. This needs to examine operating system versions and patch levels, installed configuration profiles and certificates, and scan for malicious apps.
4) Finally – and this element is often neglected – user education is essential. The nature of phishing attacks requires unwitting or uneducated users at the device side – and even the most sophisticated technical education can be undone in a second by a careless user. And as mobile phishing attacks get more sophisticated, mobilizing sophisticated social engineering techniques to trick even savvy individuals, user education has never been more important.

Workforces need to be educated to be suspicious of any email that is unknown, to avoid opening any attachment that is now known or requested, to not provide any personal information over email or text, and to exercise extreme caution when they receive unexpected payment notifications via email, or requests from social media contacts they don't recognize. They also need to be able to identify potentially fake websites, and know to immediately close their browser if a URL directs to a completely different website. With this combination of best-practice security technologies and user education, organizations will be in a good position to ensure that their employees will not easily fall for the bait offered by mobile phishers.

BRIAN GLEESON IS HEAD OF MOBILE SECURITY PRODUCT MARKETING AT CHECK POINT SOFTWARE.