PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: Thwart phishing attacks
Publication/Portal: The Star
Date: 10 August 2020

Language: English
Section: Star Two
Page: 2

Thwart phishing attacks

Did you receive a strange email? It's best to check that you're not the target of a phishing attack.

By PHILIPP SCHULTE

FAKE bills, falsified invoices, strange correspondence from the bank: Who hasn't had a suspicious email land in their Inbox? In most cases, it's a phishing attack – an attempt to trick people into sharing personal or sensitive data in order to steal from them.

Most phishing attempts occur over email, text or social media messages, though they can also happen over the phone or through the mail, says financial expert Ralf Scherfling from a consumer centre in western Germany.

Often times, criminals will obtain a large dataset, and then try out their scams on all the email addresses included.

There are also more targeted phishing scams, where the perpetrators use data they already have to launch a more credible attack – for example, an email that looks like it's from your banking consultant.

For the most part, however, phishing attempts are pretty timeless.

"For example, it may be about the introduction of a new security technology or a discrepancy in a customer's account," according to Scherfling.

The email will probably ask the recipient to click on a link and enter data, or open a file attachment that may contain malware.

Melanie Volkamer, a professor at Germany's Karlsruhe Institute of Technology, and her research group have together come up with guidelines for how to tell whether an email is a phishing attempt.

The first thing to look for is plausibility: Does the message seem to match the person who's allegedly sending it? Does it ask for sensitive information? Is the salutation wrong or incorrect?

"The more such questions you can answer with 'yes', the more likely it is that you're dealing with a fraudulent message," says Volkamer.

The structure of the message also gives hints as to its intent.

"After the salutation and the reason given for why the email was sent to you, there's a need for action, many times with a close deadline attached to increase the time pressure," says Scherfling. The recipient is pressured to click a link or open an attachment.

Even when the email's contents and sender seem plausible, you should still closely inspect the links attached, says Volkamer.

If you move your mouse over the link without clicking, you should be able to see where it will take you – is the address connected to the alleged sender?

"Especially if the domain consists of numbers, an IP (Internet Protocol) address, it is most likely a dangerous web address," according to Volkamer.

Another rule for staying safe is to look at the email attachments. Formats like .exe, .bat or .cmd are especially dangerous, though Microsoft Office formats like .docx, .xlsx or .pptx, which may contain macros, should also be approached with the utmost caution.

"You should only open such an attachment if you expected that exact one from the sender," advises Volkamer.

If you're unsure, it's best to first double-check with the sender – preferably with a phone call.

If you've uncovered a phishing email, just delete it, says Scherfling. You can also warn others over social media.

Anyone who's fallen for the trap should change their passwords and security questions – and they should definitely not delete the message, which is now evidence.

You should inform the respective service provider and file a criminal complaint about the phishing attempt against you that was successful. – dpa