Over Phishing: Practical Steps for Resisting Phishing Attacks and Immediate Action to Be Taken By a Phishing Victim

December 2017

You may have seen that there have been a number of news stories of late regarding the increased frequency of phishing attacks in recent months, including on the front page of the SCMP last week. These scams are not only directed at individuals, but are becoming increasingly sophisticated and targeted at companies, including large multinationals.

Our recent experience of acting for clients in relation to such matters has shown that these frauds are sophisticated. The fraudsters will usually create an email domain name very similar to, but not quite the same as, the victim's email domain – perhaps by adding a hyphen between company names, adding (or deleting) the word 'group' or in one example of which we are aware where the victim company name began with a 'w', replacing the 'w' in the domain name with 'vv'.

The fraudsters do their research: they will know how the company's emails are designed and structured (footers, headers, email names etc.), the roles of senior officers of the company and also who within the victim organisation to target. Much of the information the fraudsters obtain may be public information, but the fraudsters may have previously installed spyware within the victim company's systems and so can track the company's payment systems and protocols as well as its response (if any) to the potential fraud. We have also seen fraudsters using the same bank account to carry out a number of fraudulent transactions against different victims, generally withdrawing the fraudulently obtained money the same day it is received. It is essential for a company which suspects it has been the victim of such a scam to react quickly: recent experience has shown us that the fraudster's accounts can be frozen before the money is withdrawn.

Common elements of these scams include:

- The phishing email purportedly coming from a senior individual in the target organisation – for example, we have seen emails purporting to be from the CEOs and Financial Directors of clients.

- The phishing email being sent to a more junior administrative member of staff who may not know or have met the senior management member who has purportedly sent the email.

- The fraudster often claims in the email to have spoken to other senior individuals in the target organisation who the fraudster alleges have authorised/corroborated the payment request.

- The requested payment may be in respect of a purported invoice in favour of a company providing services to the target organisation. That company will often have only been incorporated shortly before the attack and will have no substantial online or physical presence – for example, its registered address may be that of an entity which provides company secretarial services.

- The fraudster's email will often stress the urgency of the request for payment, suggesting that paperwork will follow and asking the target employee to transfer the money as soon as possible.

- The email user and domain names will be very close to – but not quite the same as – the genuine email addresses of the target company.

- The sender will send follow-up correspondence, asking whether the payment has been made and asking the employee of the target organisation to confirm when payment has been made. These emails will be frequent and short.

- The sum requested may be relatively large, but not so large that it necessarily arouses suspicion or falls outside the target employee's delegated authority.

- If the sum does fall outside the targeted employee's deleted authority or there are insufficient funds in the target account, the fraudsters may suggest a lower amount.

If a company thinks it has been the victim of such an attack, set out below are steps it may take to protect itself and try to prevent any further dissipation of monies paid to a fraudster's account:

- Verify with the person the fraudsters have impersonated whether or not that person did in fact instruct the payment.

- Immediately report the matter to the police in both the jurisdiction from which the payment originated as well as in the jurisdiction where the fraudster's bank account is located. If the fraudster's bank account is in Hong Kong, the company can inform the Hong Kong Police on crimeinformation@police.gov.hk. However, the Hong Kong Police may not take further investigative steps unless and until the company provides it with a crime number from the jurisdiction where the payment originated.

- Ask the originating bank where the company's bank account is held to inform the fraudster's bank of the fraudulent transfer ASAP, by SWIFT message if the payment has been generated by SWIFT.

- Gather as much information as you possibly can in relation to the payment, such as emails between the fraudster and anyone in the company.

- Verify whether the company has had any prior correspondence/dealings with the company/individual to whom the fraudsters have requested payment be made.

- Immediately inform in-house counsel and instruct external counsel in the jurisdiction to which the payment has been transferred. External counsel may be able to assist in contacting the recipient bank locally to put it on notice of the suspicious transaction (in part with the aim of triggering any local AML reporting requirements) and, more importantly, to take steps to obtain an injunction from the local courts to freeze the assets of the fraudster and order the recipient bank to provide information to the company in relation to the fraudster's bank accounts. External counsel will also be able to take steps to research the fraudster and attempt to obtain further information. External counsel will also be able to advise whether any regulators need to be informed and – if the fraud is particularly significant and the victim company is listed or part of a listed group – in relation to any disclosure obligations that may arise.

These attacks are becoming increasingly sophisticated and are executed quickly. It is rare that funds will remain in the fraudster's recipient bank account for more than 24 hours. It is therefore important to train all staff, particularly those in accounts roles, to recognise and how to react to suspicious emails, remain vigilant and act swiftly once suspicions arise.

To the extent you have any further questions or suspect any such phishing activity, please do not hesitate to contact me or your usual Slaughter and May contact.

Mark Hughes
T +852 2901 7204
E mark.hughes@slaughterandmay.com