Phishing Attacks – Protecting Employees and Organisations from Data Privacy Breaches and Unintended Fund Transfers

Samuel Sharpe & Sinyee Ong
16 June 2020

Introduction

The pandemic has created opportunities for unscrupulous individuals to attack organisations through 'phishing'. Leveraging on the pandemic-related concerns of employees, hackers lure employees with deceptive communications that would open up a pandora's box of negative repercussions. In a recent case, hackers used artificial intelligence to mimic the voice of a CEO to convince an employee to transfer funds to a bank account controlled by the hackers.

In this briefing note, we will highlight some of the common repercussions of falling prey to phishing attacks and provide suggestions to assist organisations to cope with consequences of falling prey to such attacks.

Phishing in a Pandemic

Phishing is a cyber-attack where hackers masquerade as a trustworthy entity to trick a victim, usually by e-mail (but increasingly by other electronic and even voice communications), into providing information or money to the hacker, either by clicking on a malicious link or, in more extreme cases, actively transferring information or money to the hacker.

The COVID-19 pandemic provides a fertile environment for phishing attacks for the following reasons:

- Most people (employees included) are interested to find out more about the pandemic. Hackers prey on this curiosity by sending e-mails from seemingly authoritative sources (i.e., the World Health Organisation or other governmental agencies) purporting to provide updates or guidelines on protection methods or vaccines to curious employees.

- There has been a great deal of disruption to supply chains and changes to usual methods of doing business. In the midst of a pandemic, employees may not find it unusual for sellers to change their bank details or buyers to change their delivery addresses. Hackers make targeted phishing e-mails or calls (known as 'spear phishing') to the relevant employees pretending to be the legitimate payee or recipient of goods and trick employees into diverting legitimate payments to the hacker.

- There are many more corporate communications through e-mails or other forms of communications (i.e., on work-from-home policies or requirements to resume work-

at-office) sent by individuals in management or central services, all of whom may not be personally known to employees. Hackers can disguise themselves as these key individuals and send similar communications to unsuspecting employees (who may not be able to differentiate such malicious communications from legitimate ones).

Employees who unwittingly fall prey to such attacks can facilitate malware being installed on the company system, which increases the risk of the system being infiltrated and data being lost. In other cases, employees may be tricked into sending funds directly to hackers.

Consequences of Falling Prey to Phishing Attacks – Data Protection Considerations

Phishing attacks do not only put commercial information and organisational functions at risk, personal data of the organisation's clientele, employees and counterparties are also put at risk.

Leakages in personal data may lead to serious legal and regulatory ramifications for the victim of a phishing attack. Most jurisdictions now have data protection legislation that may impose penalties on organisations who allow data breaches to occur and require organisations to compensate victims of data breaches.

- In the European Union, the General Data Protection Regulation ("**GDPR**") requires organisations to implement appropriate technical and organisational measures to ensure that data is handled securely. Infringement of GDPR provisions may cost an organisation up to € 20 million worth of fines or up to 4 % of an organisation's total global turnover of the preceding fiscal year (whichever is higher). Furthermore, in the case of any breach in data security, organisations have 72 hours to inform the relevant data protection authority and can be liable to compensate persons who have suffered damage due to the data breach.

- In Singapore, the Personal Data Protection Act requires organisations to implement reasonable security arrangements to prevent unauthorised access or disclosure of personal data. Failure to do so can lead to a criminal conviction and fines for organisations. Otherwise, individuals who have suffered damage or loss as a result of any leakage in data may pursue civil proceedings against the organisation responsible for the data breach.

Consequences of Falling Prey to Phishing Attacks – Recovering Money

It is not uncommon for victims of phishing attacks to unwittingly send funds to hackers.

If this happens, there are steps that the organisation can take to recover its funds, provided it acts quickly. The following steps should be considered:

- Inform all banks concerned (i.e., the sending bank, the recipient bank and any intermediary banks) of the suspected fraudulent transfer. All reputable banks have strict anti-money laundering procedures. When informed that funds in their possession may have been fraudulently transferred, the bank should freeze the funds immediately. Once the funds are frozen in the account, the organisation should work with the relevant bank to recover the money.

- If funds have left the recipient bank account, immediate steps should be taken to trace the destination of the funds. Organisations should seek legal assistance in the destination country to obtain court orders: (a) requiring the recipient bank to disclose all onward transfers of funds from the recipient account (known as a Norwich Pharmacal order in many common law jurisdictions); and (b) preventing the recipient organisation or individual from dealing with the funds (known as freezing injunctions or Mareva injunctions).

- Lodge police reports in the countries where the money was transferred from and to. Organisations should also keep the police updated if additional information comes to light.

How We Can Help

At Sharpe & Jagger LLC, we regularly assist clients with comprehensive training programmes and materials to enable organisations to comply with data protection requirements. We also assist clients with tracing and recovering unintended fund transfers. Feel free to contact any of our lawyers to find out how we may be of assistance.

Samuel Sharpe

samuel.sharpe@sjlaw.com.sg
65 6694 7283 | 65 9786 7409

Sinyee Ong

sinyee.ong@sjlaw.com.sg
65 6694 7281 | 65 9148 5059