Mahajan & Aibara

Case study on Phishing E-mails and Cyber Fraud

Issue date: December 2020 | Issue no. 02

Read time: 6-7 mins

What is phishing?

Phishing is an attempt by an attacker to gather personal information from users. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent website that appears legitimate. The user may then be asked to provide personal information, such as account usernames and passwords, which if done, could expose them to getting compromised.

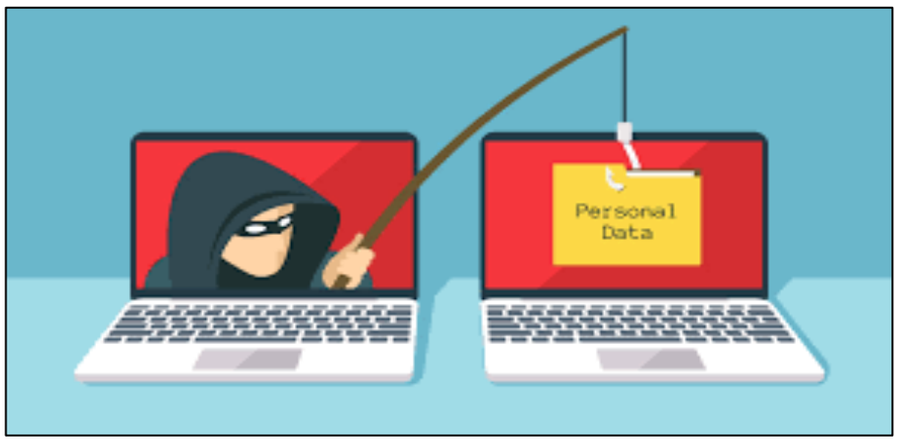
Preventive actions to avoid falling prey to phishing

1. The message is sent from a public email domain

- Many of us rarely, if ever, look at the email address that a message has come from.
- Your inbox displays a name, like 'IT Governance', and the subject line.
- When crooks create their bogus email addresses, they often have the choice to select the display name, which does not have to relate to the email address at all.

2. The domain name is misspelt

- Another clue that is available, is hidden in domain names. It provides a strong indication of phishing – but it unfortunately complicates our previous clue.
- The problem is that anyone can buy a domain name from a registrar. And although every domain name must be unique, there are several ways to create addresses that are sometimes not easy to distinguish from the one that is being spoofed. e.g. google.com can be spoofed as g00gle.com so if someone does not notice this spoof, it can either lead to serious data leakages, breach or other forms of compromise



3. It includes suspicious attachments or links

- Consider this one example, if you receive an email from Netflix, you would expect the link to direct you to an address that begins with 'netflix.com'.
- Unfortunately, many legitimate and scam emails hide the destination address in a button, so it is not immediately apparent where the link takes you.
- To ensure you do not fall for schemes like this one, you must train yourself to check where links go, before opening them.
- This can be done as follows: on a PC, hover your mouse over the link, and the destination address appears in a small bar along the bottom of the browser. On a mobile, hold down on the link and a pop-up will appear containing the link. This diligence helps mitigate the phishing risk considerably.

Case study

E-mail phishing/spoofing:

The client was a large, listed Indian multi-national with operations in India and several overseas locations. The company was aggressive on inorganic growth, and had made several acquisitions in the last seven years, ever since the founder's son had joined as the CEO.

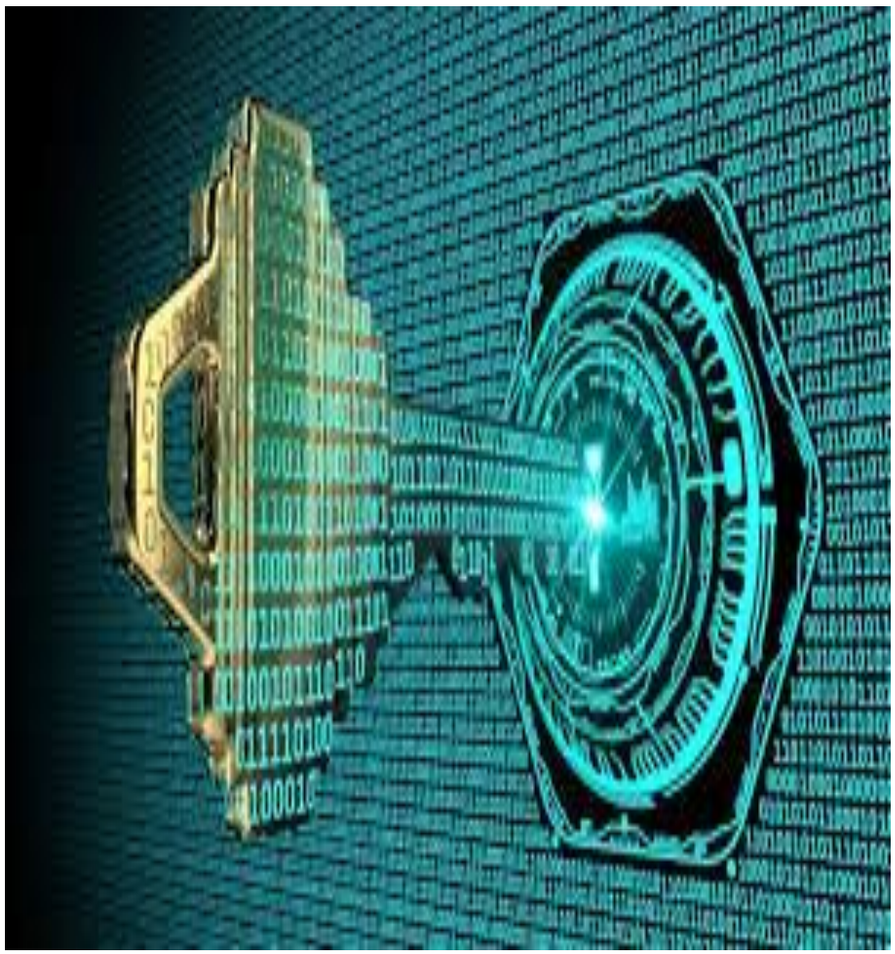
The CEO had recently been on a business trip to South Africa, for a potential acquisition. The CFO, who was with the company for a few years and knew the CEO's hands-on style, got an e-mail from him, early on a Monday morning, marked "Urgent". The e-mail asked him to contact an international law firm, in Johannesburg, and talk to the Partner handling the transaction for the company.

The CEO had copied in the law firm partner in his e-mail, and had instructed the CFO to transfer a sum of USD 15 million, as an advance payment towards the transaction. The target was well known, privately held, profitable, business. The CEO stated that he had closed the deal over dinner on Sunday night.

The CFO quickly got to office and called the law firm Partner on his mobile number provided by the CEO in his e-mail. When he spoke with the law firm Partner, he asked him a few basic details of the transaction, and after satisfying himself, asked the law firm Partner to e-mail him the firm's bank account details. The law firm partner sent him the bank account details by e-mail, within a few minutes of his call.

The CFO promptly sent instructions over to their bank to transfer the USD 15 million. Once that was done, he called the law firm partner to notify him. He also e-mailed the CEO and the law firm partner, the transfer details, in response to the CEO's e-mail.

The CEO was scheduled to take a flight back to India that very morning, so just to be sure, once the CEO landed in India late that evening, the CFO called up the CEO to understand what more needed to be done, in terms of raising funds to pay for the rest of the acquisition.



When he spoke with the CEO, the CFO was shocked with the CEO's response. The CEO did not know what the CFO was talking about and it seemed that he had neither sent an e-mail to the CFO to talk to any law firm partner about the transaction, nor had he asked him to transfer funds to any law firm's bank account for any advance payment to the acquisition target. As a matter of fact, the CEO said, that while there were a few interesting deals, none of them had reached a level of closure.

The investigation: The team was hired by the Board, to unravel the fraud. Through their work, spread over one and a half months, they were able to decipher how this fraud was carried out.

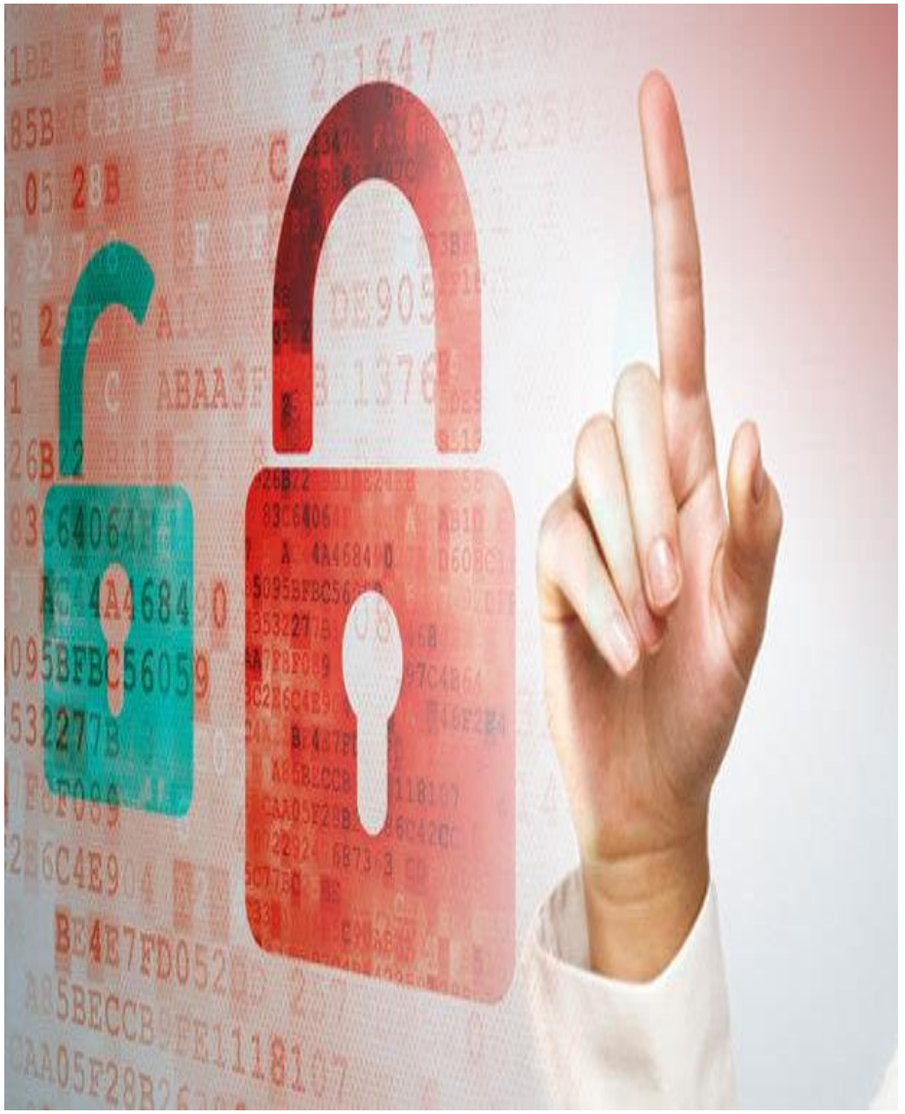
The e-mail address used by the CEO, was a spoof of the CEO's original official e-mail address, which was created using a domain name similar to the company's domain name, and which was easy to overlook.

The law firm Partner's e-mail address, which was used to communicate with the CFO, was also a spoof e-mail address created. The law firm Partner, who the CFO had spoken with, was also one of the fraudsters, as his phone number was spoofed using freeware available, and was not a registered mobile number with the telecom company in Johannesburg.

The CFO seemed to have done his diligence before he had done the transfer of USD 15 million, and seemed to be as much a victim of the fraud, as the company that had lost USD 15 million.

During the investigation, the CEO expressed that he knew the CFO to be a very careful professional and was quite surprised that he had not spoken with him even once, before completing the transfer of USD 15 million.

Though the CEO was scheduled to fly out that morning, he said that his flight had got delayed, and that he was stranded at Johannesburg for over three hours, during which time the money had been transferred.



The CFO had not called the CEO even once to try and talk to him, before transferring the USD 15 million to the law firm. During our interview with him, the CFO's stand was that he believed the CEO was in his flight back to India then, so he did not call him, since he knew that the CEO's phone would not be accessible. He repeatedly said that he had acted diligently and in good faith.

Based on the investigation team's recommendation, the CEO authorised a limited review of the CFO's computer disk, to determine if he was being completely honest.

Further investigation through use of computer forensics and analysis of the CFO's e-mail metadata, revealed, that the CFO had masterminded the entire fraud scheme and had used his associates in London and his sisters based in Nairobi and London, to perpetrate the fraud.

Further evidence through social media and company registry records in the UK and India also revealed that the funds embezzled from the company, were transferred to the CFO's company, which he had set up with his immediate family members; his two sons and his wife, in India.

The elaborate fraud scheme, which was designed to look like a phishing attack, was indeed a phishing attack, but where the CFO was the mastermind.

Thanks to use of technology, profiling, social searches and looking beyond the ordinary, the investigation team was able to unearth the fraud and recover the entire sum of money the company had lost to the fraud. The CFO was duly dismissed from services with the company. Given his years of service with the company however, and to avoid reputational damage, the Board decided not to press charges against him.

For any enquiries please contact :
mnaknowledge@mahajanaibara.com
Our Offices:
Mumbai | Pune | Delhi | Bengaluru