MARSH

September 2015

ADVISER

VISHING FOR TROUBLE

RISK ALERT: COMPANIES URGED TO REVIEW COUNTER-FRAUD MEASURES AFTER UK COMPANY SUFFERS GBP1 MILLION FRAUD.

A recent *Telegraph* article[1] concerning a company that was defrauded of GBP1 million by a bogus caller claiming to be from the company's bank highlights the need for organisations and their employees to be vigilant and to be aware of social engineering-based frauds.

While many may be aware of phone hacking after the recent *News of the World* revelations or have watched movies featuring computer hacking such as *War Games* (1983), *Sneakers* (1992), *Swordfish* (2001), and *The Girl With the Dragon Tattoo* (2009), very few may know that many hacks or cyber-related fraud starts with social engineering — or, as author Christopher Hadnagy terms it, "human hacking".

Fraud requires information, which has never been more abundant in an age where data and communication touches every part of our personal and business lives. Illicit access to information is the catalyst of the majority of frauds, and the "confidence trickster" has come of age, using many subtle techniques — and increasingly complex and audacious schemes — to target individuals and the data and systems they control.

The "traditional" techniques that have been frequently used fall into two basic categories:

- **Phishing**: A broad-based email deception soliciting information either directly or by persuading the recipient to validate information by clicking a link which then installs software such as keystroke loggers to capture items such as usernames and passwords.
- **Pharming**: A more sophisticated form of phishing which can potentially cause a virus (or Trojan horse) to be installed on the user's computer simply by opening an email. These Trojans are capable of redirecting the browser to the pharmer's fake version of the genuine website the user is trying to access. Confidential information is then captured as the unsuspecting individual enters access information into the counterfeit site.

VISHING

The fraud reported in the *Telegraph*, however, is one of many examples of a newer technique — **vishing**.

Vishing typically targets a specific individual who may have already been identified and researched by the fraudsters using social media data or purchased background information. In many situations, vishing will involve telephone communication. By employing this most trusted form of personal communication, fraudsters typically rely on basic psychology to gain trust.

VISHING MASTER CLASS

Simple statements that trigger strong emotions such as fear when directed against a person in authority have increased credibility and will often result in the victim being more easily persuaded to comply with the fraudsters requests. Add to this additional subliminal supporting information and the potential for a successful fraudulent interaction increases dramatically.

The case reported in the *Telegraph* is an excellent example of these techniques:

- Fear: The caller advised the staff member that "there was a virus on the firm's internet banking facility and that their money needed to be transferred to a holding account while the bank fixed the problem".
- Subliminal supporting validation: The fraudster's telephone number was displayed and had been manipulated to replicate the bank's fraud team telephone number displayed on its website.

Whether it involves their personal or business lives, individuals need to develop a heightened awareness of the lengths to which a fraudster will go to extract potentially valuable — and damaging — information. The game has changed and often the approaches being made are highly credible, believable, and, importantly, well researched.

The old adage "if something is too good to be true it probably isn't" has been a watchword for investment scams and yet people still succumb to them. Unfortunately the modern fraudster who employs vishing and similar techniques targets us as individuals as much as the assets and information we control.

FOUR STEPS TO REDUCE RISK

Companies and individuals need more education, awareness, and resources to improve the likelihood of being able to spot, avoid, and ultimately defeat a determined fraudster. In the meantime, some basic risk awareness training and protocols can significantly reduce your exposure to this type of fraud:

1. Talk with your bank representatives and ask them to issue specific guidance on what they will and will not ask for in communications with you.
2. Create simple protocols on payment or information requests to prevent a single person being able to fulfil a request from start to finish.
3. Maintain trusted telephone number and email directories for key suppliers. If in doubt, insist on calling another known person to validate the situation.
4. Be vigilant, be safe, and never feel pressured into immediate action.

FOR MORE INFORMATION, PLEASE CONTACT:

DEAN WHITE
Managing Director & Head of Product Governance, FINPRO
+44 20 7357 2205
dean.white@marsh.com

[1] "Business scammed into handing over £1million to bogus caller" http://www.telegraph.co.uk/news/uknews/crime/11878125/Business-scammed-into-handing-over-1million-to-bogus-caller.html, accessed 23 September 2015.

GRAPHICS NO. 15-1023