FTI CONSULTING

SPEAR PHISHING

Carefully Targeted, Extremely Damaging and Fast Increasing

It's a depressingly familiar experience – a message pops into the recipient's inbox demanding that they log-in to their bank account, office systems or email provider urgently. Badly written, often featuring a generic salutation ("Dear Valued Customer") and frequently purporting to be from a bank or other organisation that the recipient is not even a customer of, most of these messages are instantly deleted.

But what about the message that seems more authentic and relevant to the recipient? It might not feel right, but would a fraudster go really take the trouble to get so many details right – referring to their bank, their employer, their location and perhaps even a colleague?

The practice of sending fraudulent emails that, unlike most phishing activity, contain precise and usually factually correct details is known as "spear phishing." Just as a real-life spear fisher targets a particular fish, the electronic variety goes for specific individuals, creating fraudulent emails that look more genuine and convincing than the general phishing variety.

According to the National Cyber Security Centre, which is part of GCHQ, "One of the main differences between a targeted attack and mass generic campaigns, is that a targeted attack may have a specific goal within your organisation. This could be about transferring money, or getting access to an administrator account," it says. "For example, someone after money might target your finance team by mimicking your normal invoice process."

In March last year, Spanish police arrested a gang of fraudsters that were sending spear phishing emails to bank employees resulting in the theft of around €1billion from 100 financial institutions. "The criminals would send out to bank employees spear phishing emails with a malicious attachment impersonating legitimate companies," said Europol. The carefully targeted messages appeared to come from international financial institutions or ATM manufacturers. In some cases, the attached malware caused specific ATMs to spew out cash at certain times when gang members would be waiting.

Recently the US Air Force targeted its own personnel in Europe with a spear phishing campaign, describing these attacks as a "persistent threat" to its network integrity. "Even one user

falling for a spear-phishing attempt creates an opening for our adversaries," said Colonel Anthony Thomas, head of Air Force Cyber Operations. "Part of mission resiliency is ensuring our airmen have the proficiency to recognise and thwart adversary actions."

To mimic the kind of credible, targeted emails that victims of spear phishing attacks receive the Air Force sent the messages that purportedly came from the Airman and Family Readiness Center and a legal office. These included requests to input information into a hyperlinked document.

"Whaling" is spear phishing which, as the name suggests, targets larger prey. These are frequently members of the C-suite and the emails they receive will be particularly well personalised. In 2016 a senior executive at a global manufacturing company received an email that she believed to be from the company's new CEO requesting that a payment of $3million be made to a Chinese vendor.

She approved the payment – only to find just hours later that the message had not come from the CEO and was probably the work of Chinese hackers. However, by this stage it was too late – the money had gone. The company had fallen victim to a Business Email Compromise (BEC), something that is often associated with whaling.

Because the returns are greater with spear phishing and whaling, fraudsters are willing to devote more time and energy to crafting these emails. They might trawl through Facebook pages, company websites and LinkedIn accounts to find details relating to a victim's work and private life that they can include to make their messages look more authentic – and therefore more likely to prompt a response.

Although most organisations provide detailed guidance to their staff about the risks of phishing and most people these days can recognise one of these emails when they see one, too few organisations are yet focussed on training staff on spear phishing. Employees at all levels should be made aware that fraudulent emails are becoming ever more authentic.

Senior managers should be aware that they're more likely than more junior staff to be targeted by spear phishers or whalers. Frequently time-poor and under pressure to respond quickly to messages, members of the C-suite and the management level just below them can easily find themselves opening an apparently legitimate email on their smartphone, perhaps, as they're on the move that can have devastating consequences for their organisation.

Rather than attempt to train staff to be alert for both regular and spear phishing separately, organisations should talk to them about factors such as classic influence techniques – these include messages with themes of urgency, threat and authority. These themes are common to both spear and ordinary phishing emails.

As spear phishing becomes sophisticated and widespread it's essential that organisations take a multi-layered approach to protecting themselves. This means buying in expertise in staff training, cyber security and monitoring from an external source that specialises in this growing risk.

Muthmainur Rahman
Senior Managing Director
+971 (0) 4 437 2131
muthmainur.rahman@fticonsulting.com

FTI CONSULTING™

EXPERTS WITH IMPACT

About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.

0677-03/19