nccgroup

Aug 28, 2020 18:14 BST

Psychology of the Phish: Leveraging the Seven Principles of Influence

By Sourya Biswas, Principal Security Consultant, NCC Group

If you have an email address (who doesn't?), you have received phishing emails. Derived from the word "fishing", as in "fishing for information", phishing emails are an unfortunate fact of modern, connected life. From exotic princes offering millions of dollars in emails full of wrong spellings and bad grammar, to sophisticated, targeted emails that spoof sender addresses and replicate official templates, phishing emails span a wide maturity spectrum.

Why is phishing popular?

The popularity of phishing is driven not only by its success, but its success relative to its cost. Due to mass emailing tools (legitimate) and mailing lists (both legitimate and illegitimate), it's quite inexpensive to carry out a phishing campaign. In other words, the return on investment (ROI) for the cybercriminal is quite high. That is why, the average user receives more than 16 phishing emails a month.

Here's an illustrative example of the economics of email fraud. Back in 2008, researchers from the University of California, Berkeley and UC, San Diego (UCSD) infiltrated the Storm botnet network used by cybercriminals. They ran fake spam campaigns to measure the efficacy of email fraud and could make only 28 sales over 26 days even after sending 350 million emails. Seems a very poor return of investment, right. Not so much if you run the numbers. Even with an abysmal response rate of 0.00001%, this represents a $7000 per day revenue. Note that this is an example of simple spam trying to get recipients to buy non-existent or faulty products; with sophisticated phishing campaigns leading to identity theft or fraudulent payments or data held to ransom, the returns are significantly higher.

If we consider the two parameters used to evaluate a cybercriminal – motivation and capability – both can be considered high for phishing. With respect to "motivation", or what an attacker seeks to achieve, this can range from something simple like getting recipients to disclose personal or financial information, or something more sinister like getting them to download malware to provide a backdoor for ransomware attacks or data breaches. Also, if "capability", or ability of attacker to carry out an attack is concerned, it doesn't take much to carry out phishing campaigns.

Here are some interesting statistics that illustrate the magnitude of the problem:

- In 2019, Business Email Compromise, a subset of phishing attacks, caused more than $1.7 billion losses (Source: FBI Internet Crime Report)
- In 2018, phishing accounted for 32% of data breaches and 78% of cyber espionage activity (Source: Verizon Data Breach Investigations Report)
- In 2017, 76% of organizations were targeted by phishing emails (Source: Wombat Security's State of the Phish Report)
- In 2017, around 1.4 million new phishing sites were created each month (Source: Webroot Quarterly Threat Trends Report)

How is phishing performed?

There are different ways in which phishing emails seek to compromise their targets. The simplest mechanism is prompting direct action outside of the email platform, such as sending directions purportedly from the CEO asking

for a payment to be made. Others include directing recipients to click a link that downloads malware or directs them to an external site that mimics a genuine web page for credential harvesting.

Phishing is an example of social engineering, that is, it leverages normal social behavior to get people to do something that can harm them or their environment. In other words, it allows the attacker to exert influence on the victim. As with anything that seeks to influence behavior, a psychological view may be of interest.

The psychology of phishing

While not a psychologist, I've been intrigued at the psychological elements at play here, a line of thought that took me to my MBA days learning about the principles of influence. These six principles, later expanded to seven, were expounded by Arizona State University professor Robert B. Cialdini in his book "Influence: The Psychology of Persuasion".

Here are the seven principles of influence and how I believe they translate to phishing:

1) Reciprocation – This is simply "give and take", a version of "you scratch my back, I scratch yours." An email promising to give access to confidential information if a certain attachment is downloaded or a link is clicked is a classic example of this principle being leveraged in phishing.

2) Scarcity – People want what is difficult to get. Phishing emails that stress that a certain benefit is accessible only if action is taken within a short period of time ("download this attachment to continue having access to your email") is an example of this principle at play.

3) Authority – People defer to authority. That's why many phishing emails seek to impersonate senior executives / Human Resources / Information Technology / Finance. An email from the CEO (supposedly) asking the Finance department to immediately wire $300,000 to an account unknown to the department is an example scenario that has occurred many times in the past.

4) Consistency – You must have heard the expression "creature of habit". In some way, all of us are creatures of habit in that we like to go about our lives in set ways. Phishing emails that look like official communications exploit this fact, hoping the recipient overlooks the unusual request that is included in such an email. An email with the Amazon logo saying a shipment is held up and asking the recipient to confirm their home address may not raise red flags even if no shipment is expected; that's the power of a recognized brand.

5) Consensus – We have all seen the power of the crowd, from frenzied fans at a rock concert or the mad mobs in riots. People have a tendency to follow other people. A phishing email that mentions something like "544 of 800

employees have updated their software, click this link to download" seeks to exploit this fact.

6) Liking – This is an extremely obvious principle of influence, and something that we use daily. If people like you, they will say "yes". Conversely, if people want to be liked, they will also say "yes". This is exploited by phishers when they target eager-to-please new employees. An email from HR (supposedly) asking a new employee for their SSN to update in payroll is one such common ruse.

7) Unity – This was not in the original list but was added later by Cialdini. The idea is that the more we identify ourselves with others, the more we are influenced by them. A phishing email supposedly sent by someone who shares the same interests as the recipient, information that can easily be sourced through social media, has a high chance of success. For example, if a person loves dogs, an email from another dog-lover (supposedly) with an attachment of cute dog pictures (supposedly) has a high chance of being opened.

How not to fall prey to phishing

While there are many technical controls to combat phishing like Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC), IP blacklisting, spam filtering, etc., some will always get through. This is a function of the sheer volume of phishing emails as well as the increasing sophistication of the attackers. In that scenario, end users are the last line of defense.

The best way to train users about the dangers of phishing is to make them aware of the tactics used by attackers and by conducting repeated simulations that make use of the aforementioned principles of influence. For example, an organization's security team sends mock phishing emails at irregular intervals, that leverage one or more of the seven principles, trying to get employees to take the bait. Those that do are provided information on why they should have been more careful, including a brief summary of Dr. Cialdini's work. This should be supplemented with a section on the psychology behind phishing, accompanied by examples, during annual security awareness training refreshers.

As the saying goes, "I hear, I know. I see, I remember. I do, I understand." Nothing creates understanding like actually falling victim to phishing; phishing simulations are the next best thing. Supplement that with formal training, and your employees will be much better equipped to handle these criminal amateur psychologists that modern phishers are increasingly developing into.

Author: Sourya Biswas

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750