Understanding Phishing and Protecting the 8th Layer

Anthony M. Ralston

East Carolina University

November 28, 2016

Abstract

This paper will focus on understanding the risk associated with phishing attacks on companies and how we can measure growth through phish benchmarking. The paper will define and look at the different angles that phishes can exploit users and how we can measure their effectiveness. The paper will look at the traditional measurements matrix based on clicks and credential harvesting. Moreover, this paper will look at cultural, quality of phish, work environment, and other factors to establish a larger picture of the risk to a company from phishing attacks. It is hoped that this paper will serve as a closer consideration what it takes to measure and protect users from phishing attacks.

Keywords: Phishing, Social Engineering, Malware, Credential Harvesting, Clicks

Understanding Phishing and Protecting the 8th Layer

In the modern world, there are many risks and more so on the cyber front. There are hacktivists that target our favorite sites with DDoS attacks, malware of all shapes and kind, internal and external malicious actors, and various forms of phishing. Phishing comes in many flavors, from general spammed phishing attacks to focused spear-phishing. So, what is phishing? It is the act of sending emails that look legitimate trying to trick targets into doing something that ether gives information to the attacker, infects an asset or both (Hadnagy & Fincher, 2015). This threat vector involves both technical and social engineering in a blinded mess that tends to be very effective. Spear-phishing is a focused phish, where the attackers research information about the target and tailor the phish to be effective against them (Sjowerman, 2015). This attack comes from many different sources hacktivists, someone looking to make a quick buck, criminal organizations, and even state funded organizations. There are many examples of successful phishing campaigns and in fact almost eighty percent of all malware attacks come from phishing emails and other attempts (DBIR, 2015). Much of that malware is used to establish connections to assets or exfiltrate data or obtain user credentials.

Who is targeted?

If you have an email address you have most likely received a phishing email and it is also likely that you have clicked on a link that they provided or opened an attachment (Hadnagy & Fincher, 2015). This is such a prolific issue that the Nigeria Country Risk Report – Q1 2017 (2016) said “the biggest threat in Nigeria is associated with phishing”. Attackers target any organization or person that they can get money from or information that might lead to money (Hadnagy & Fincher, 2015). That means any company no matter if they are large or small are a

potential target for phishing campaigns. The juicier the target the more energy and time the attacker will most likely invest into the phish. Hacktivists on the other hand tend to be motivated by social, religious, or political reasons. This makes their targets harder for security professionals to identify and protect. With the advent of social media attackers have an extremely large pool of data to gather information about their targets from. Phishing exploits the weakest part of a corporation's attack surface, the human component. The destruction this vector can cause is very clear when considering cases like that of Ubiquiti Networks Inc. who lost over $46.7 million in phishing campaign (Brecht, 2016). This campaign tricked authorized users into transferring funds to attackers. This is only one example of the destructive power attackers have if they successfully exploit legitimate users. While there have been many attempts to curb the use of the phishing attack vector none have been overly successful.

Phishing messages are delivered by any means that is available to the attacker however, bulk emailing also known as spam is the most well-known means (James, 2005). This normally means that the attacker will use a domain name that looks like what the target would most likely expect to see. They are also going to obfuscate URLs and email addresses whenever possible. This increases the likelihood that the victim will trust the source. With the advent of social media that has become another method of phish delivery, however this has been focused more on attacking social or political targets.

How do we protect against it?

How can companies protect against something that exploits their personnel? Adding an intrusion prevention system (IPS) to an equipment string and configuring it to detect and stop malware or shell connections to the outside might help to an extent. However, there are ways around it. How do we prevent encrypted traffic, like SMTP, SSL, or TLS? Companies add email

security filters to help mitigate the risk. This might catch some of the traffic, but will still miss well-crafted phish attacks. To truly defend against phishing campaigns, companies need to raise awareness of the threats and have knowledge of what areas they are especially susceptible to attack. One way to do this is to conduct in house or third party phishing campaigns to assess weak points in the company's defense. This does not take the place of technical controls that corporations employ, but helps to address the social engineering component of a phish. Identification of the high-risk areas and clear metrics of a baseline, growth, or deficiencies can help administrators to tune IPS, firewalls, and other filters to support those areas. With the volatility of this risk vector it and will never be a "set and forget" solution. However, it can be manageable with the proper planning and support. This plan requires active security team members to regularly schedule phishing campaigns to test the state of the environment. Also, it required incident response planning. This planning will have actions that need to occur to secure the environment after an event has occurred. The testing of these plans is just as important as having them. Without validation, plans are of no use.

Psychology of a phish

The goal of the attacker is to get the target to perform an action based on the email. A successful attacker will take the psychology of decision-making into account. According to SparkNotes 101 Psychology "Decision-making involves weighing alternatives and choosing between them" (2005) and the attacker wants to influence the target into choosing to open and perform the function of the phish. There are many ways that an attacker can accomplish this. One method is to take advantage of representativeness heuristic. This is where the attacker makes the phish look like something that the target would assume was trusted by the way that it is presented (SparkNotes 101 Psychology, 2005). The same way that if someone drove a big truck,

wore cowboy clothes, and talked with a country accent most people who saw him would assume that I was from the country when in fact he could be from New York City. If as an attacker I can make you assume that it is legitimate traffic based on the look and feel of the message, targets will be more likely not look to validate the message any further.

Cognitive bias is another advantage that an attacker has over a target. This is because people tend to view things based on their pass experiences and beliefs (Hadnagy & Fincher, 2015). This occurs in all levels of life from picking the food that we eat to what neighborhood we want to live in. If an attacker can tap into this bias, then he increases the likelihood that the phish will be successful. Also, people tend to be overconfident in their beliefs and decision making ability, leading to a lack of evaluation of their decision-making (SparkNotes 101 Psychology, 2005).

The target can also be exploited using emotional triggers. Increasing or decreasing the pleasantness or sensuality of a phish will affect the judgement and decision-making abilities of possible targets (George & Dane, 2016). If an attacker sends a phish to a company saying that there will be negative changes to their 401k the likelihood of this being successful is higher than if something that does not incite an emotional response. In an organizational context, using emotions of targets could have complex and potentially far reaching results, if the phish is engineered successfully (George & Dane, 2016).

Cultural influence of a phish

To phish is to use social engineering to influence or manipulate someone into acting or behaving how we want them to (Hadnagy & Fincher, 2015). Methods of manipulating behavior changes between targets. Different cultures and peoples have differences among social norms and how they are educated. Western people tend to be more concerned and less likely to click on

a basic phishing emails than middle-eastern people (Al-Hamar, Dawson, & Al-Hamar, 2011). There also seems to be a trend where older people fall victim to basic phishing emails more than their younger counterparts (Rocha Flores, Holm, Nohlberg, & Ekstedt, 2015). These factors should be considered and attackers do consider them. Company culture is another aspect that can be exploited. If an attacker identifies how a corporation communicates to one another he can use that information to tailor the phish and become more successful in his activities.

Cultural context is a very important aspect when looking for weaknesses. If a phish email is sent to a Midwestern company impersonating a surf board company, might not have the same effect as it would in California. However, the same company might be very susceptible to religious phishing scams. Sending a phishing email to an Asian based company impersonating the executive leadership team might be very successful, where in America it might not be as successful. It is important for security professionals to research what is succeeding within the areas where you are responsible for protecting and adjusting your strategy appropriately.

Protection

Educating users is key to preventing or limiting the effects of a phishing attack. Lessons need to be tailored to strengthen the weak points identified within the organization. However, critical and analytical thinking should be a common theme across all areas. To think critically the user must move beyond the face value of a message and dig deeper (Hadnagy & Fincher, 2015). They need to know where the message is coming from, look if this message meets the patterns expected from that source, is it reasonable, and does this message employ an emotional response. Setting an expectation that critical thinking should be employed in all aspects of communications will help to mitigate many social engineering assaults. However, Attackers can and will still find

weak points within this method. The primary means of overcoming someone that is critically thinking about decisions is to get them emotionally involved in the choice.

Another quick win is to teach personnel not to just click on hyperlinks. They should read what the URL is and if they do not recognize it then they should think critically about it (Hadnagy & Fincher, 2015). Clicking the link because it is what they are used to doing is one of the first things that a security team should teach their users not to do. Informed users are less likely to follow impersonated links.

There will be a time when a user clicks on a malicious URL. When this occurs, their training should take over and they should know to call the security team and report it immediately. The company should have a standard operating procedure for handling these types of events. Even if the user went a step further and put in their credentials there should be a procedure to handle this event and this should be well known and practiced. When an event occurs, it is important for personnel to remain calm and isolate the effects of the event where ever possible.

Educating personnel on how to read URLs is also another important aspect of protecting your information from malicious actors (Hadnagy & Fincher, 2015). Test your users, to see if they understand the difference between HTTP, HTTPS, and FTP. Showing them how to read URLs will not stop all threats, but it will address many of the low hanging fruit and help them identify phishing emails more efficiently. In addition, there should be a push to educate users in reading email addressing (Hadnagy & Fincher, 2015). You should identify to them what email addresses they should expect to see from the IT team or any other mass emailing source that the company might be using.

Evaluating Risk

Evaluating user's susceptibility of falling victim to social engineering is very challenging. There is not a one size fits all or a magic program that can be installed to tell you this, no matter what the salesmen say. This is a constant evolving landscape where mountains turn into molehills and molehills into mountains overnight. Technical controls are a part of the overall evaluation process, but does not provide much support for an attack designed to exploit personnel. There are many programs, company sponsored, and third party phishing campaigns that can be employed, but without understanding the results it just becomes another check in the box that does not properly show the risk to the company or where the education of the users should be focused. If there was some magical device or system, phishing campaigns would not be as successful as they are today. Much of evaluating risk is based on consistency of a baseline and continued testing to determine improvement of different types of social engineering attacks. This can be done by applying customized metrics to understand internal phishing results. Future testing, education, and technical controls should be placed with this information in mind.

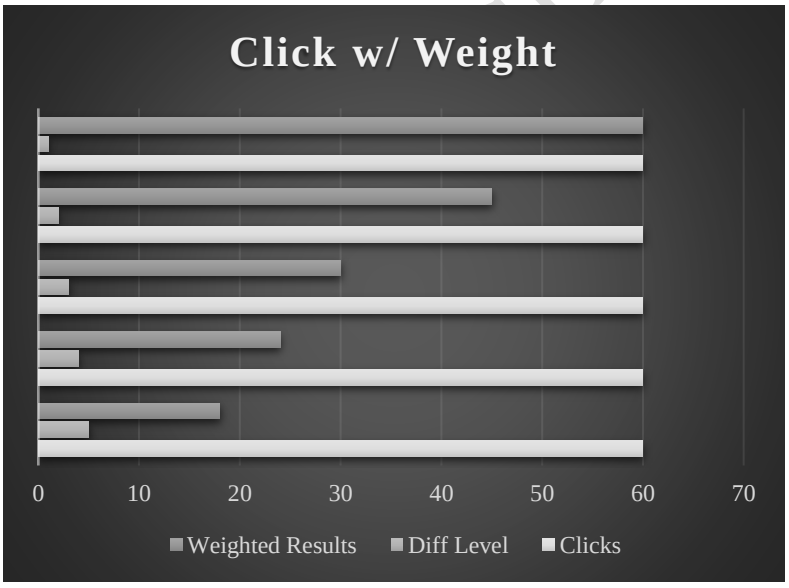
Conducting internal phishing

A phishing strategy is key for collecting information on how the personnel within an environment is doing with social engineering risks. This however can be a challenge to measure growth and where the risk is. Categorization and population baselines help to show growth or the lack there of (Hadnagy & Fincher, 2015). A generic and basic phish would be a good baselining point. This will help to see if basic understanding of phishing risks is understood from the user population. However, if an advanced phish increases click rate or credential harvesting, that is not necessarily an indication of the population becoming less aware of security risks. Instead it means that the risk has not been fully baselined. Categorical analysis of phishing results would

be beneficial within environments to better identify weaknesses within training plans. Prior planning on what difficulty to start testing from is also key in developing a phishing plan and weather to inform users of the phishing activities (Hadnagy & Fincher, 2015). Starting a phishing campaign without informing the personnel will give the clearest view of the current risks. Telling them will give the security personnel the change to educate then validate users with scheduled and randomized testing (Hadnagy & Fincher, 2015).

Understanding phish measurements

How we measure the results of a phish will determine how we identify the health of our security program. If there are inconsistencies within the measurements, then we will have an inaccurate view of the risk that we are facing. While it is important to track things like clicks and credentials harvested there should also be identification of how difficult it is to identify the email as a phish. This will create a weighted system that will better identify the real risk to the environment. The difficulty of the phish does not mean how complex, but more so of how focused and tailored it is for the target (Hadnagy & Fincher, 2015). With increased difficulty, the weighted click rate goes down. This way phishing results with a difficulty of five can be compared to results of a difficulty of one. This creates consistency within reviewing results of phishing campaigns.



There should also be weights to the different metrics. User clicking on a website that was designed to obtain credentials is not the same as the user putting their credentials into the website. Malware infection is also a higher risk than that of a click. These factors should be put into prospective when assessing the state of risk within an environment. Without clearly understanding the context around the measurements it is impossible to identify the true risk of phishing attacks within your environment. How this information is identified and quantified is not as important as it is to be consistent with the methodology. An inconsistent approach of tracking the information will lead to incorrect results.

Conclusion

In today's world, there are many dangers and phishing is one of the most dangerous in the cyber arena, because it attacks the most volatile and unpredictable resource within any infrastructure, people. Understanding the risk, psychology, and vulnerably around phishing is the first step in developing a strong and consistent security plan to help mitigate some of the risk. Given the constant changing of the security landscape it is highly unlikely that we will ever eliminate these risks. However, we can hopefully, limit the impact of these phishing campaigns that cost corporations, governments, and civilians so much. Education is the key to minimizing the effects of this plague.

References

*Al-Hamar, M., Dawson, R., & Al-Hamar, J. (2011). The need for education on phishing: A survey comparison of the UK and qatar. *Campus - Wide Information Systems, 28*(5), 308-319. doi:http://dx.doi.org.jproxy.lib.ecu.edu/10.1108/10650741111181580

Brecht, D. (2016, January 18). Spear Phishing: Real Life Examples. Retrieved November 28, 2016, from http://resources.infosecinstitute.com/spear-phishing-real-life-examples/

*Collette, R., & Gentile, M. (2006). IT RISK MANAGEMENT: Countering the increasing threat of Phishing/Pharming attacks. *Computer Economics Report, 28*(2), 8-12. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/214228052?accountid=10639

*George, J. M., & Dane, E. (2016). Affect, emotion, and decision making. *Organizational Behavior and Human Decision Processes, 136*, 47. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1821758662?accountid=10639

Hadnagy, C., & Fincher, M. (2015). Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails (1). Somerset, US: Wiley. Retrieved from http://www.ebrary.com

James, L. (2005). Phishing Exposed (1). Rockland, US: Syngress. Retrieved from http://www.ebrary.com

**Nigeria country risk report - Q1 2017.* (2016). (). London: Business Monitor International. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1841853890?accountid=10639

Rocha Flores, W., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information and Computer Security, 23*(2), 178-199. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1786145806?accountid=10639

*Sjouwerman, S. (2015). Confronting 'spear phishing' etc. *Privacy Journal, 41*(7), 3-4. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1691260002?accountid=10639

SparkNotes 101 psychology. (2005). New York, NY: Spark Educational Pub.

Verizon Enterprise Solutions. (2015, April 17). *Verizon 2015 Data Breach Investigations Report – Q&A*. Retrieved from http://news.verizonenterprise.com/2015/04/2015-data-breach-report-info/