How a Modern Business Could Respond to the Phishing Attack Challenges

MILICA D. ĐEKIĆ, Subotica

Professional paper

UDC: 343.533::004

004.738.5.056

DOI: 10.5937/tehnika1703455D

The majority of public and private enterprises as well as the entire society are getting dependable on cyber technologies. As it's known – cyber would deal with computers, internet and mobile devices being used through our everyday life's and work's activities. Many experts would agree that this new technological tendency would bring us many advantages as well as the real nightmares in sense of our safety and security. One of the well-known hacking attacks being applied in a business environment is a phishing. The phishing is a technique of sending mostly an e-mail with the link or attachment being included into that e-message. Sometimes it's possible to simply make a click on a malicious webpage searching the internet. This sort of incident got a great deal of attention from the Law Enforcement agencies worldwide for a reason it may cost an economy a lot. Through this article – we would try to discuss how this sort of hacker's campaign could be used in a practice as well as mention some security's challenges being present in this area of cyber defense.

Key words: information technology, cyber defense, phishing, hacking, business, economy, etc

1. INTRODUCTION

A modern business got extremely dependable on new technologies and such a situation would mean that an economy would get vulnerable to hacking attacks as well as cyber espionages. [1, 2, 3] The ultimate goal of today's business is to gain some sort of competitive advantage on a marketplace. Similarly – as in a military doctrine – our current commerce environment would seek brilliant strategists who would lead the business through all the challenges trying to avoid any sort of the obstacles being present on that path on. In order to cope with all the challenges being correlated with the modern business pool – you would need to deal as a competitive force.

That means you would need to adapt to any situation and never give up from your mission. Many people would say this is typical to a defense environment, but – believingly or not – today's business surrounding is highly competitive and as a natural selection would suggest – the strongest ones would keep going on.

As many experts, researchers and influencers would indicate – the time of bosses is behind us. Today we live the era of leadership where the best of us would pull on the rest of a crew and make a progress to all.

Some futurists would agree that the next phase in a human kind development would bring us an age of people being with the mission as something getting so important to good decision makers. The majority of Serbian marketplace would rely on small and midsize enterprises (SMEs) and we believe that similarly as in case of developed economies – we should deal with more strategic way of managing a business on. Everything being mention in this article could serve in making a better business condition to the rest of economy that should understand that today's world is full of competition and if you want to stay on a surface – you need to work both – smart and hard. Finally, we would take into a consideration that many businesses would somehow use cyber technologies in their everyday's operations. We would want to highlight that the majority of threats, risks and challenges coming from that sort of an environment could affect the entire business pool as well as economy. There is a wide spectrum of hacker's strategies that could get applied on some competitor's assets. Also, many hackers would operate on the black market and sell the confidential information to the real criminals or terrorists. One of the gravest threats coming from the

Author's address: Milica Đekić, Subotica, Vase Pelagića 39a

e-mail: milicadjekic82@gmail.com

Paper received: 25.04.2017.

Paper accepted: 10.05.2017.

hacker's environment to a business surrounding is a phishing campaign. It's a quite handy way of obtaining so significant details about some computer and a pretty convenient way of getting into the entire network. So, the weakest link in a chain in such a scenario would be your employee who would so unintentionally make a click on that skillfully prepared link being sent as a part of lovely e-mail. [4, 5] In addition, it's not a rare case at all that the entire computer's network would get infected with so hazardous malware if anyone of employees open up the attachments being the part of some carefully written e-mails. In any case, we intend to talk a bit more about those topics through this effort.

2. WHAT IS PHISHING?

The phishing is a technique of scamming the victim using carefully prepared e-mails that would lead

them to the malicious links or attachments. The point is to make someone leaves you his IP address and in return – you would insert him some malicious content.

Many phishing campaigns would be highly sophisticated and lead you to well-developed websites that would collect your IP details and allow the hackers using their tools to steal confidential information from you. [7] So, the purpose of a phishing attack is to obtain someone's IP information.

Once the bad guys get the IP address – they can take the entire spectrum of strategies in order to take advantage over someone's IT infrastructure.

In this case, we would give an example of quite common phishing tactic which aim would be to obtain an access to the healthcare IT asset. The first step of this campaign is illustrated in a Figure 1 as follows.

Figure 1 - The phishing e-mail attack

As it's illustrated in the Figure above, we would deal with the phishing e-mail campaign being directed to a healthcare sector. The reason why we would choose such a receiver is that the healthcare domain is quite profitable for the black market. For instance, the healthcare record is between 10 and 20 times more expensive than, say, the credit card number. That record would undoubtedly offer much more information and logically the hackers would seek more money for that. As you would see – in this example – we would use a lovely e-mail being sent from fake Wikipedia e-mail account that would seek from a target to make a click on the link that would offer him more details on how to publish his webpage with this prestigious website. So, the target would be CHC Zvezdara from Belgrade, Republic of Serbia that would not have its

Wikipedia page. The victim would be asked kindly to make a click on the following content <http://wikipedia.org/publish>. We would use such an obvious case not telling to people from the CHC Zvezdara that there is a back link behind such a selected text. Also, we would suggest that we would send such an e-mail from office@wiki-pedia.org e-mail address. It's important to know that this example is fully abstract and it illustrates how some of the attacks could work in a practice. At the moment of writing this article – we would not find that a domain www.wiki-pedia.org even exists, so we would use it as a case of opening up the website with the e-mail capabilities. In a Figure 2, we would demonstrate how back link appears in a practice and how it's possible to embed such a link into any selected text.

Figure 2 - How to edit the link?

In the Figure 2, it's shown how we could edit a link into any e-mail environment. In this case, we would illustrate how it's feasible in a Gmail surrounding, because we would not create a new website with its e-mail account for a reason it's not that suitable at all. We would only try to provide you with the necessary information on how the scammers would do so. In the previous illustration, we would see that the text to display would be <http://wikipedia.org/publish> and its web address would be <http://scam.xyz/scam>. That website could or could not exist for real – we would use it as a case study only in order to show how hackers could hide their web addresses and make you do a click onto their skillfully prepared trap. Finally, it's important to mention that this sort of technique could offer you a nice opportunity to obtain some confidential information and get into the entire IT system. The Serbian healthcare system would recently deal with the Integrated Healthcare Information System (IHIS) and just try to imagine how severe the consequences of smartly coordinated scammer's attacks could be.

3. THE IMPACTS OF PHISHING TO A BUSINESS

In the previous section, we would discuss how it's possible to scam anyone belonging to the healthcare sector. Further, we would talk how the similar scenarios could get applied in a business environment – especially in the area of SMEs. It's quite clear that the fraud with the Wikipedia's call for collaborators could work anywhere including a business. Many people would like to introduce something about their organizations or staffs to the rest of the world using the Wikipedia website as the place dealing with the reputable folks. So, such a trick could always offer the certain level of taken advantage to anyone being correlated with the hacker's community. Also, it's important to say that once you develop a website – you

would need to deal with the Content Management System (CMS) that would offer you a chance to see the IP addresses of computers calling your website.

In addition, it's interesting to suggest that you can create a website that would not necessarily appear within anyone's web browser. That would mean if you send an e-mail with the phishing link – someone may make a click on that sort of a trap, but he would not get anything in return. In such a case, many people would believe they deal with the broken link being corrupted on its way on through the e-mail communications. In developing economies such as Republic of Serbia, many SMEs would not get the IT Departments or at least a single IT Professional within their asset. Their employees being the weakest link in a chain would so confidently do many clicks anywhere and in such a way put the entire enterprise at the risk to become an easy target to malicious actors.

Finally, we would try to analyze how a Serbian business sector could become a possible target to many hackers' organizations. For instance, we would notice a certain lack of safety and security procedures with the Serbian business. In other words, the hackers would so easily obtain the confidential information from those organizations, sell them on the black market and feasibly cause the collapse of the entire enterprise within some brief period of time. If anyone being the part of this region or some global organization would conduct the series of hacking attack to the Serbian SMEs – that could be catastrophic to the entire country. With more than 60% of the Serbian GDP coming from the SMEs – it's so obvious that we would call that sort of asset being the critical one. [16, 17] In addition, no one should underestimate the role of a business sector to the Serbian economy and people should know that such a sector is from strategic importance to our nation. Also, if anyone would try to

threaten the healthcare system – the response should get similar – fast and effective.

4. HOW WE CAN PREVENT SOME PHISHING CAMPAIGNS

As we would indicate through this article – the weakest link in your cybersecurity chain is your employee. We would mention before that even the experienced staffs could get the victims of skillfully prepared hacker's operations. So, the question here would be how we could prevent anything of that even happens. The answer to this question is quite straightforward – you should invest into education and training or any sort of awareness rising campaigns within your organization. Indeed, those sorts of education and training should teach the employees to think twice before they decide to make a click or open an attachment coming from some unknown sender. As we've suggested through the case of the Wikipedia scamming – sometimes it's so hard to recognize that the link being included into some e-mail could be the malicious one. In those cases – you would need a strong eye to details in order to estimate if the e-mail is authentic or phishing. Many experts would suggest that it's always the best to avoid any action on if you are not confident about what you are supposed to do in the certain case. For example, if you notice anything being suspicious – you should report that to your IT Department or at least your IT Security Professional. Those guys should deal with some security procedures and policies that would protect your asset from any sort of harm. Also, they should get a sufficient level of the skills and expertise that would support them to resolve such a situation. So commonly, the IT Security people would get in touch with the Police Departments that would also get involved in a case. Sometimes it's possible that a discovered case is only the piece in something big happening on the national, regional or international stage. In other words, no organization should be slack and miss an opportunity to leverage its human resources capacities making them actively participate into any sort of cyber defense campaign. The next chapter would demonstrate why phishing could get assumed as a challenge to a modern safety and security as well as discuss some measures of prevention and incident response.

5. WHY PHISHING IS A CHALLENGE TO OUR SAFETY AND SECURITY

The main reason why phishing could get considered as a challenge to today's safety and security is that the computer and network breaches being the consequence of those operations could affect the critical infrastructure. As it's well known – the critical infrastructure is vitally important to any nation's life

and business. Try to imagine what would happen with the entire electricity network of our country if the phishing attack to some of the power plants would be successful. [4, 5] That scenario would cause the catastrophic impacts to the entire country and we would probably need some time to recover that electricity network.

On the other hand, the example being made with the healthcare sector is also the illustrative one. There are many similar cases we would mention in order to demonstrate that the phishing is the challenge – not only to our country, but rather to the states worldwide. Finally, we would mention that such a challenge should get handled carefully and skillfully and we would always try to respond to that. The education and training are good measures of prevention, but we should also attempt to think about the incident response strategies being from strategic importance to any organization.

6. DISCUSSIONS

In this modern time – many organizations would be the targets of phishing campaigns leading to any sort of cyber breach. It's not easy at all to develop and adopt the best practice – once you have in mind that modern threats are getting more and more sophisticated. As we would illustrate through this effort – everyone including the private and public sector could get the victims of a cybercrime. If we take into account that such a sort of criminality could cost the global economy several hundred billion dollars per a year – it's obvious that the good defense strategy is more than welcome. Finally, is so significant to add that today's technological progress would always make us follow the tendency and cope with the only permanent thing in this world and that is a change. In addition, we would highlight that one of the biggest applications of this challenge could be in a corporate security being so closely correlated with the threats to a business itself.

7. CONCLUSION

The purpose of this effort is to engage the expert's network of Republic of Serbia and the rest of the researcher's community to deal harder and smarter with these topics. We've found this field as quite exciting to investigate and we would suggest to everyone to take part in that. In conclusion, it appears that the phishing is a never ending threat, so it's highly recommended to think about some new approaches and insights to that area.

REFERENCES

- [1] Ablon L, Libicki M. C, Golay A, *Markets for Cybercrime Tools and Stolen Data*, Sponsored by

- Juniper Networks, Web source: http://www.rand.org/content/dam/rand/pubs/research_reports/R600/RR610/RAND_RR610.pdf, 2014.
- [2] Beaver K, Davis P. T, *Hacking Wireless Networks for Dummies*, Wiley Publishing, Web source: https://cdn.preterhuman.net/texts/underground/hacking/Hacking_Wireless_Networks_For_Dummies_2005.pdf, 2005.
- [3] Bergman M. K, *The Deep Web: Surfacing Hidden Value*, White paper, Web source: http://jornalggn.com.br/sites/default/files/documentos/2011_bergman_7_cafarella_informationretrieval_presentation1_2.pdf, 2000.
- [4] Charney S, *Rethinking the Cyber Threat: A Framework and Path Forward*, Microsoft, 2009
- [5] Chaliand G. and Blin A, *The History of Terrorism*, University of California Press, Web source: https://wikileaks.org/gifiles/attach/177/177597_History%20of%20Ter.pdf, 2007.
- [6] CRS Report for Congress, *Critical Infrastructure and Key Assets: Definition and Identification*, Web source: <https://www.fas.org/srg/crs/RL32631.pdf>, 2004.
- [7] James P, Jenson M. And Tinsley H, *Understanding the Threat: What Data Tell Us about U.S. Foreign Fighters*, START, Web source: <https://www.start.umd.edu/publication/understanding-threat-whatdata-tell-us-about-us-foreign-fighters>, 2015,
- [8] Mester G, *Intelligent Mobil Robot Control in Unknown Environments*, Intelligent Engineering Systems and Computational Cybernetics, Part I Intelligent Robotics, Library of Congress, Springer, 2009
- [9] *RFID Security*, The Government of the Hong Kong Special Administrative Region, Web source: <http://www.infosec.gov.hk/english/technical/files/rfid.pdf>, 2008.
- [10] Payne S. P, *A Guide to Security Metrics*, SANS Institute, Web source: <https://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55>, 2007,
- [11] Puhe M, Edelmann M, Reichenbach M, *Integrated urban e-ticketing for public transport and touristic sites*, Final report, Science and Technology Options Assessment, Web source: [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513551/IPOL-JOIN_ET\(2014\)513551_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513551/IPOL-JOIN_ET(2014)513551_EN.pdf), 2014,
- [12] Ponemon Institute LLC, *2015 Cost of Data Breach Study: Global Analysis*, Ponemon Institute Research Report, Web source: <https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF>, 2015,
- [13] Symantec, *Internet Security Threat Report*, Web source: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>, 2016.
- [14] S. Weine and B. H. Ellis, *Lessons Learned from Mental Health and Education: Identifying Best Practices for Addressing Violent Extremism*, START, Web source: https://www.start.umd.edu/pubs/START_LessonsLearnedfromMentalHealthAndEducation_FullReport_Oct2015.pdf, 2015,
- [15] Weine S. and Ellis B. H, *Supporting A Multidisciplinary Approach to Addressing Violent Extremism*, START, Web source: https://www.start.umd.edu/pubs/START_LessonsLearnedfromMentalHealthAndEducation_MentalHealthSummary_Oct2015.pdf, 2015.
- [16] Đekić M. D, *Cyber procedure za poslovno okruženje u Srbiji*, Tehnika, vol. 71, br. 3, str. 471-474, 2016.
- [17] Đekić M. D, *Kako sačuvati kontinuitet u poslovanju uprkos cyber incidentima*, Tehnika, vol. 70, br. 2, str. 346-349, 2015.

REZIME

KAKO SAVREMENO POSLOVANJE MOŽE DA ODGOVORI IZAZOVIMA PHISHING NAPADA

Većina javnih i privatnih preduzeća, kao i čitavo društvo su postali zavisni od cyber tehnologija. Kao što je poznato – cyber se odnosi na računare, internet i mobilne uređaje koji se koriste kroz naše svakodnevne životne i poslovne aktivnosti. Mnogi stručnjaci se slažu da ova nova tehnološka tendencija donosi mnoge pogodnosti, ali i realne noćne more u smislu naše sigurnosti i bezbednosti. Jedan od dobro poznatih hakerskih napada koji se primenjuje u poslovnom okruženju je phishing. To je tehnika slanja – uglavnom – e-mail poruka sa linkom ili zakačkom. Ponekad je moguće jednostavno kliknuti na malicioznu web stranicu pretražujući internet. Ta vrsta incidenta je dobila ogromnu pažnju od strane policijskih službi širom sveta iz razloga što košta ekonomiju mnogo. Kroz ovaj članak – mi ćemo pokušati da prodiskutujemo kako ovaj vid hakerskih kampanja može da se iskoristi u praksi, kao i da spomenemo neke bezbedonosne izazove koji su prisutni u ovoj grani visokotehnološke bezbednosti.

Ključne reči: informacione tehnologije, visokotehnološka bezbednost, phishing, hakovanje, poslovanje, ekonomija, itd.