Phishing: Um estudo sobre Engenharia Social

Lucidia A. Silveira, Maurício Realan A., Érico Amaral

Engenharia de Computação – Universidade Federal do Pampa (UNIPAMPA)
Avenida Maria Anunciação Gomes de Godoy, n°1650 – Bagé – RS – Brasil

lucidiasilvera@gmail.com, mauriciorealan@gmail.com,
ericoamaral@unipampa.edu.br

Abstract. *Often, the main vulnerabilities of a computer system are not in their conception, but in its users. A unprepared individual to identify malicious actions can provide relevant informations, that can weaken their system. Based on this problem, this research sought to identify the effectiveness of a social engineering technique known as phishing, aiming to expose the importance of recognizing this type of method and the user awareness about many activities that can raise the level of risk of their systems.*

Resumo. *Muitas vezes, as principais vulnerabilidades de um sistema computacional não estão em sua concepção, mas sim em seus usuários. Um individuo despreparado para identificar ações maliciosas, pode disponibilizar informações relevantes, as quais possibilitam fragilizar seu sistema. Com base neste problema, esta pesquisa buscou identificar a efetividade de uma técnica de engenharia social conhecida como phishing, com o objetivo de expor a importância de reconhecer este tipo de método e, da consciência do usuário sobre as diversas atividades que possam elevar o nível de risco de seus sistemas.*

1. Introdução

Muitos *crackers* não seguem o estereótipo de alguém tímido e com pouca habilidade social, como é do imaginário popular. São pessoas carismáticas, que conseguem convencer outras pessoas a fazer o que eles necessitam, mesmo que isso não seja a intenção da vítima à princípio. Esses *crackers são* chamados de Engenheiros Sociais (ES), que segundo Mitnick (2004) são indivíduos com a capacidade de manipular a confiança de outra pessoa, a fim de obter acesso à suas informações privadas.

De acordo com Cavalcanti (2011) muitas vezes o ponto mais frágil de um sistema é o "fator humano", seja por inocência, por vontade de socializar ou pela provocação de sentimentos (como pena, compaixão ou curiosidade) o usuário acaba se colocando em risco, divulgando informações que podem ajudar o ES a aplicar seu golpe.

Para o diretor técnico da Symantec Security Response, apenas cerca de 3% dos *malwares* são lançados com o objetivo de explorar uma falha técnica, os outros 97% estão tentando enganar um usuário através de algum tipo de esquema, que leva a uma exposição indevida de informações pessoais, afirma Lord (2016).

O objetivo deste artigo é conscientizar o usuário menos informado sobre as questões de segurança na internet, sobre as técnicas de Engenharia Social e seus perigos, utilizando o *phishing* como objeto de estudo principal, mostrando assim, a recorrência destes ataques e também algumas medidas de prevenção que podem ser adotadas pelo usuário. Para apresentar este estudo o presente artigo possui a seguinte estrutura: a contextualização do tema, na primeira seção; na seção 2 é apresentado um breve referencial sobre Engenharia Social*;* na seção 3 é descrita a metodologia

adotada e na seção 4 um levantamento sobre informações relevantes de *phishing* e como se prevenir desse tipo de golpe; por fim, as conclusões parciais são apontadas na seção 5.

2. Engenharia Social

Para Nakamura (2007) a engenharia social, no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais. Este é um termo que descreve um tipo psicotécnico de intrusão que depende fortemente de interação humana e envolve enganar outras pessoas para quebrar procedimentos de segurança.

Os ES se utilizam de diversas técnicas de ataque para ludibriar as suas vitimas e assim alcançar os seus objetivos. (DE CASTRO, 2013) aponta em seu estudo as seguintes técnicas, comumente utilizadas pelos Engenheiros Sociais: *(i)* análise do lixo, pois o lixo é uma das fontes mais ricas de informações para os engenheiros sociais; *(ii)* internet e redes sociais, visto que nas redes sociais é possível encontrar informações pertinentes pessoais e profissionais; *(iii)* contato telefônico, sabendo que os ES utilizam diferentes abordagens, via telefone, para coletar informações relevantes; *(iv) baiting*, processo baseado no comprometimento de mídias removíveis, com *exploits* específicos para o roubo de informações.

3. Metodologia

Tendo em vista o objetivo geral desse estudo, que visa apresentar uma análise sobre a engenharia social utilização a técnica de *phishing* como modelo principal de estudo, foi adotada a seguinte estrutura metodológica: em um primeiro momento foi realizada a definição do objetivo da pesquisa. Posteriormente, partiu-se para o levantamento de um referêncial teórico para servir como base ao todo da pesquisa**.** No momento seguinte, foi definida a técnica de *phishing* como objeto de análise específica, pois a mesma é amplamente utilizada pelos engenheiros sociais e também por ser a que mais chega perto de usar apenas o computador, sem precisar de contato pessoal. Depois se definiu a importância de indicar como um usuário pode tentar se prevenir deste golpe.

4. Técnica de *Phishing*

Além das técnicas descritas na seção 2, destaca-se o método de *phishing*, um dos principais recursos de um ES. O *Phishing* é uma forma de golpe em que um atacante tenta, de forma fraudulenta, adquirir informações de uma vítima personificando uma entidade em que esta confia, (JAGATIC *et al.* 2007). Os engenheiros sociais utilizam sites fraudulentos e *e-mails* falsos para roubar dados pessoais do alvo. Os criminosos buscam obter estas informações de diferentes formas como: *links* falsos, *defacement*, *keyloggers* entre outros.

4.1. Recorrência dos Ataques de *Phishing*

Durante o primeiro trimestre de 2015, os produtos da Kaspersky Lab registraram mais de 50 milhões (50.077.057) de detecções pelo sistema *antiphishing*, o que revela um aumento de um milhão em comparação ao último trimestre de 2014, de acordo com o Relatório de *Spam* e *Phishing* (KAPERSKY, 2016). Geograficamente, o Brasil continua a ser o líder no volume de usuários atacados, embora tenha diminuído 2,74% no primeiro trimestre, os brasileiros continuam sendo as vítimas preferidas dos *phishers* e representam 18,28% dos ataques no índice mundial, seguido da Índia (17.73%) e China (14,92%).

Quanto a atividade, a categoria "Portais Internacionais da Internet" ocupa o primeiro lugar com 25,66% dos ataques dirigidos, os bancos com 18,98% estão em segundo lugar, seguidos de Lojas Online (9,68%), que aumentou 2,78% em número de ataques. No pódio das plataformas,

sobre as quais são coletados dados para ataques do tipo de Engenharia Social, encontram-se o Facebook com 10,97%, o Google (8,11%) e por ultimo o Yahoo! com 5,21%, segundo relatório emitido pelo Kaspersky (2015).

4.2. Técnicas Antiphishing

É sempre preciso ter cuidado ao fornecer informações pessoais através da Internet. Felizmente, as empresas começaram a adotar estratégias *antiphishing* a fim de reduzir a ocorrência deste tipo de incidente, contudo estas ações não protegem completamente seus usuários. Desta forma, é necessário que os indivíduos assumam atitudes contra o *phishing,* como segue: proteção de *e-mail*, evitar a transmissão de informações pessoais pela rede (salvos casos utilizando *sites* seguros); tomar cuidado com esquemas de *phishing* via telefone; cuidado com *downloads,* e; atenção na utilização de *links* (JOSHUA, 2008*).*

Outras ações preventivas estão relacionadas ao controle do acesso a *pop-ups,* manutenção dos sistemas atualizados, adoção de *firewall*, filtros de *spam*, anti-vírus e s*oftware* anti-*spyware*. Por fim, deve ser sempre feita uma verificação das contas online e extratos bancários regularmente para garantir que não hajam transações não autorizadas realizadas. A figura 01 ilustra a metodologia para prevenção e defesa contra o *phishing*.

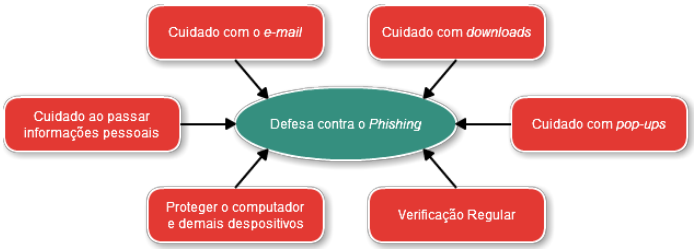

Figura 01. Técnicas para prevenção de *phishing*.

Para não cair nas armadilhas de ataques de *phishing* além do internauta precisar estar muito atento e prevenido contra o golpe é possível ainda utilizar ferramentas *antiphishing* gratuitas ou pagas e filtrar boa parte dessas ameaças. Alguns exemplos de aplicativos com esta finalidade são PhishGuard para o Firefox ou Internet Explorer e WOT para Google Chrome. Além disso, quase todos os antivírus no mercado são capazes de barrar este tipo de fraude. Contudo, é necessário apontar que essas técnicas de prevenção podem não ser o suficiente para barrar ataques mais elaborados e de mais alto nível de periculosidade, como golpes de *spearphishing* (ataque de *phishing* altamente localizado, exige uma etapa de minuciosa pesquisa por parte dos atacantes, além de muita paciência).

5. Conclusões Parciais

A Engenharia Social é uma das principais técnicas, utilizadas por atacantes, no intuito de obter o acesso não autorizado a sistemas computacionais, pois empresas e usuários geralmente dedicam grande parte de seus esforços, na área de segurança, em ações de cunho técnico, ignorando atividades de formação de pessoal, sobre questões básicas e métodos de ataque como *phishing*.

Como resultado parcial deste estudo destaca-se, então, o levantamento da importância de se conhecer os aspectos que compoem a engenharia social, especialmente o *phishing*. Conhecer este tipo de golpe é muito relevante considerando que qualquer um é um possível alvo. Saber como

se precaver destes ataques é o primeiro passo que pode ser adotado para tentar manter suas informações pessoais em segurança.

Um objetivo futuro é determinar um modelo de testes de experimentação que deve constituir-se na construção de *e-mails* fictícios enviados à endereços eletrônicos de alguns usuários, para assim realizar uma medição do número de vítimas da técnica de *phishing* aplicada e também o seu perfil. E, também, a proposição e construção de uma aplicação que realize uma espécie de pré-visualização de uma página para qual o usuário foi direcionado e não permita nenhuma ação à página até que o usuário permita, isso para tentar evitar sites indesejados e fraudulentos.

Referências

Banks, Alex. *"Brazil Digital Future in Focus 2015"*. ComScore, 2015. Disponível em: <http://blog.aotopo.com.br/wp-content/uploads/2015/02/Futuro-Digital-do-Brasil-em-Foco-2015-ComScore.pdf>. Acessado em: 11 de julho de 2016.

Cavalcanti Jr, R. L. *"Engenharia social nas redes sociais"*. Monografia (especialização), Universidade Estadual de Maringá, 2011.

CGI: *"Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2014"*. Coordenação executiva e editorial Alexandre F. Barbosa. Comitê Gestor da Internet no Brasil, São Paulo, 2015. Disponível em: <http://cetic.br/media/docs/publicacoes/2/TIC_Kids_2014_livro_eletronico.pdf>. Acessado em: 11 de julho de 2016.

De Castro, Gustavo. *"Engenharia Social: as técnicas de ataques mais utilizadas"*. 2013. Disponível em: <https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/>. Acessado em: 09 de julho de 2016.

Jagatic, Tom N., *et al*. "*Social phishing"*. Communications of the ACM 50.10, 2007: 94-100.

Joshua, identity theft killer. *"Are You Phishing For Trouble? These 8 Ways To Prevent "Phishing Scams". Will Keep You From Getting Wet "*. 2008. Disponível em: <http://www.identitytheftkiller.com/prevent-phishing-scams.php>. Acessado em:26 de julho de 2016.

Kaspersky Lab: *"Ataques de phishing fazem maior número de vítimas no Brasil"*. São Paulo, 2 de julho de 2015. Disponível em: <http://brazil.kaspersky.com/sobre-a-kaspersky/centro-de-imprensa/comunicados-de-imprensa/2015/Ataques-de-phishing-fazem-maior-numero-de-vitimas-no-Brasil>. Acessado em: 25 de julho de 2016.

Lord, Nate. "Social Engineering Attacks: Common Techniques & How to Prevent an Attack". Digital Gurdian, 2016. Disponível em: <https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack>. Acessado em: 11 de julho de 2016.

Mitnick, Kevin. *"A Arte de Enganar"*. 2004, Pearson. 1ª Edição.

Nakamura, Emilio Tissato. "Paulo Licio de Geus." Novatec. *"Segurança em redes cooperativas"*. Editora Novatec, 2007.

NORTON: *"7 essential tips to beat phishing scams"*. 2016. Disponível em: <http://us.norton.com/7-tips-to-protect-against-phishing/article>. Acessado em: 24 de julho de 2016.