ISSN: 2237-826X
ARTIGO | PAPER

O impacto da Engenharia Social na Segurança da Informação: uma abordagem orientada à Gestão Corporativa

The Impact of Social Engineering on Information Security: an approach oriented to Corporate Management

João Paulo Aramuni [1] Luiz Cláudio Maia [2]

[1] *https://orcid.org/0000-0001-7538-5927* [2] *Universidade FUMEC, Faculdade de Ciências Econômicas, Administrativas e Contábeis, Belo Horizonte, Minas Gerais, Brasil.*

Autor para correspondência/*Mail to:* João Paulo Aramuni, joaopauloaramuni@gmail.com

Resumo

Este artigo apresenta uma abordagem sobre o impacto da chamada 'engenharia social' na segurança da informação corporativa. O período de convergência tecnológica da atual sociedade da informação tem forçado organizações a estarem mais dependentes da informação. Neste contexto, a engenharia social tende a crescer e constituir-se numa das principais ameaças aos sistemas de segurança das grandes corporações. Isso se justifica no fato de que o valor de mercado da organização pode ser drasticamente afetado se as informações utilizadas para tomada de decisão não tiverem sua integridade garantida. Este estudo contribui com o preenchimento de uma lacuna teórica na compreensão da relação entre engenharia social e segurança da informação. Na perspectiva aplicada, a pesquisa oferece contribuições para as organizações quanto à identificação de vulnerabilidades da informação e à compreensão das ações praticadas para obter e quebrar o valor da informação através de fatores humanos comportamentais.

Palavras-chave: Engenharia Social; Segurança da Informação; Tecnologia da Informação; Políticas de Segurança.

Abstract

This paper presents an approach to the impact of so-called 'social engineering' on corporate information security. The technological convergence period of the current information society has forced organizations to be more reliant on information. In this context, social engineering tends to grow and become a major threat to the security systems of large corporations. This is justified by the fact that the organization's market value can be drastically affected if the information used for decision making does not have its integrity guaranteed. This study contributes to filling a theoretical gap in understanding the relationship between social engineering and information security. In the applied perspective, the research offers contributions to the organizations regarding the identification of vulnerabilities of the information and the understanding of the actions practiced to obtain and break the value of the information through human behavioral factors.

Keywords: *Social Engineering; Information Security; Information Technology; Security Policies.*

INTRODUÇÃO

O termo engenharia social ficou mais conhecido em 1990, através de um famoso hacker Kevin Mitnick. Esse termo designa para práticas utilizadas a fim de se obter informações sigilosas ou importantes de empresas, pessoas e sistemas de informação, explorando a confiança das pessoas para enganá-las. Com a evolução do comércio eletrônico e sistemas rotineiros automatizados, a forma mais comum de ataque da engenharia social é online, e com isso aumentou a preocupação quanto à privacidade que, segundo o autor Bellavista (1991), refere-se ao direito que um indivíduo possui de controlar o uso que outros fazem das informações que digam respeito a ele.

À medida que a sociedade moderna se torna cada vez mais dependente da informação, a engenharia social tende a crescer e constituir-se numa das principais ameaças aos sistemas de segurança das (grandes) organizações (Silva Filho, 2004).

O nível de segurança desejado pode ser alcançado através de políticas de segurança da organização. Segundo Böger e Bodemüller (2007) elas formam um conjunto de regras que especificam como um sistema deve prover os seus serviços, limitar as operações dos usuários e determinar como as informações e os recursos devem ser administrados, protegidos e distribuídos no interior de um sistema específico.

De acordo com Mitnick (2001), uma empresa pode gastar fortunas com aquisição de tecnologias e serviços, mas a sua infraestrutura de rede pode ainda ser vulnerável a antigos métodos de manipulação. Isso é possível porque a engenharia social explora o elo mais fraco do sistema de segurança de informação, o ser humano (Eiras, 2004).

Entretanto, existem várias ferramentas para minimizar os problemas decorrentes pela engenharia social causados por vulnerabilidades, através de mecanismos de segurança como criptografia, assinatura digital, antivírus, controle de acesso (senhas, firewalls, sistemas biométricos e smartcards), políticas de segurança, dentre outros.

De acordo com Marciano e Marques (2006), a Tecnologia da Informação e Comunicação (TIC) é capaz de apresentar parte da solução a este problema, não sendo, contudo, capaz de resolvê-lo integralmente, ou até

mesmo contribuir em agravar o problema, em alguns casos. Com isso é possível afirmar que, não existem sistemas totalmente seguros, porém através da segurança da informação, há meios de reduzir esses riscos.

Assim, baseado em trabalhos de investigação já publicados no meio científico, o presente artigo se propõe a apresentar uma revisão bibliográfica acerca da relação entre a Engenharia Social e a Segurança da Informação, vínculo ainda pouco difundido apesar do avanço das Tecnologias da Informação e Comunicação (TIC's). O artigo busca contribuir também na identificação de vulnerabilidades de segurança da informação e à compreensão das ações praticadas para obter e quebrar o valor da informação através de fatores inerentemente humanos.

REVISÃO DA LITERATURA

A revisão da literatura apresenta, inicialmente, definições relacionadas à engenharia social, à segurança da informação e a relação entre ambas. Além disso, expõe a problemática relacionada a forma como a engenharia social é utilizada para extraviar informações sigilosas da organização. Por fim, são expostos alguns estudos correlatos relacionados ao tema pesquisado.

Engenharia Social

"Eu tinha tanto sucesso nessa linha de ataque que raramente tinha que lançar mão de um ataque técnico"
Kevin Mitnick, ex-hacker especialista em Engenharia Social

A engenharia social evita a criptografia, segurança de computador, segurança de rede e tudo o mais que for tecnológico. Ela vai diretamente para o elo mais fraco de qualquer sistema de segurança: O ser humano. Engenharia Social é o termo utilizado para definir a área que estuda as técnicas e práticas utilizadas para a obtenção de informações importantes ou sigilosas de uma organização, através das pessoas, funcionários e colaboradores de uma corporação ou de uma sociedade. Essas informações podem ser obtidas por ingenuidade ou confiança (Eiras, 2004).

Geralmente o engenheiro social é um tipo de pessoa agradável, educada, simpática e carismática. Mas, sobretudo criativa, flexível e dinâmica. Possuindo uma conversa bastante envolvente. Até, mesmo, pessoas sem conhecimento antecipado desta denominação, já cometeram algum ato de engenharia social involuntariamente (Peixoto, 2004).

De acordo com Coelho et al. (2013), para minimizar as perdas referentes aos ataques da engenharia social, deve-se: programar políticas de segurança nas organizações e sua ampla divulgação; promover a conscientização peculiar e continuada dos funcionários em relação às chantagens e intimidações por parte do engenheiro social; realizar a classificação e armazenamento da informação conforme o seu nível; executar a implementação e monitoramento dos mecanismos de segurança; não manusear informações corporativas fora da empresa e nem fornecer informações pessoais ou secretas; tomar cuidados especiais com o lixo eletrônico, assim como em qualquer outro meio, através de regras de descarte.

Para Hadnagy e Maxwell (2009), a engenharia social no contexto da segurança no uso de tecnologias de informação e comunicação se refere às ações praticadas para obter e quebrar o valor da informação. Também para obter dados importantes e sigiloso de organizações e/ou sistemas computacionais, por meio da exploração da confiança das pessoas.

Pode-se também definir engenharia social como a arte de manipular pessoas a fim de contornar dispositivos de segurança ou construir métodos e estratégias para ludibriar pessoas, utilizando informações cedidas por elas de maneira a ganhar a confiança delas para obter informações (Silva, 2008).

Para minimizar as perdas referentes aos ataques da engenharia social, Coelho et al. (2013) sugere:

a) Programar políticas de segurança nas organizações e sua ampla divulgação;

b) Promover a conscientização peculiar e continuada dos funcionários em relação às chantagens e intimidações por parte do engenheiro social;

c) Realizar a classificação e armazenamento da informação conforme o seu nível;

d) Executar a implementação e monitoramento dos mecanismos de segurança;

e) Não manusear informações corporativas fora da empresa e nem fornecer informações pessoais ou secretas;

f) Tomar cuidados especiais com o lixo eletrônico, assim como em qualquer outro meio, através de regras de descarte.

A Engenharia Social é uma técnica antiga e muito popular, que poderia ser traduzida, grosso modo, como "enganar pessoas". A ideia é que o engenheiro social, como são conhecidos aqueles que praticam essa arte, possa manipular pessoas para que elas revelem informações importantes ou, então, para que elas façam algo que facilite o seu trabalho.

Além disso, a Engenharia Social também pode ser encarada como uma maneira de tirar proveito em benefício próprio, por meio de truques psicológicos, ao manipular a tendência que as pessoas possuem de confiar umas nas outras.

Existem diversos motivos para alguém estudar e usar esses truques: espionagem industrial, obter informações confidenciais para cometer alguma fraude, roubo de identidade, interromper redes e serviços ou, simplesmente, por pura diversão, apenas para provar que nenhum sistema é seguro o suficiente.

Segurança da Informação

Segurança da informação, conforme Beal (2005), é o processo de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade. Sêmola (2003) define segurança da informação como "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade." A ISO/IEC 17799:2005, em sua seção introdutória, define segurança da informação como "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio". Assim, podemos definir segurança da informação como a área do conhecimento que visa à proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade a fim de garantir a continuidade do negócio e minimizar os riscos.

A integridade da informação tem como objetivo garantir a exatidão da informação, assegurando que pessoas não autorizadas possam modificá-la, adicioná-la ou removê-la, seja de forma intencional ou acidental; A disponibilidade garante que os autorizados a acessarem a informação possam fazê-lo sempre que necessário; A confidencialidade da informação é a garantia de que somente pessoas autorizadas terão acesso a ela, protegendo-a de acordo com o grau de sigilo do se conteúdo;

Sêmola (2003) acrescenta a estes três objetivos os de: Legalidade - garantia de que a informação foi produzida em conformidade com a lei; Autenticidade - garantia de que num processo de comunicação os remetentes sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação.

A fim de garantir um nível de proteção adequado para seus ativos de informação, as organizações e seus principais gestores precisam ter uma visão clara das informações que estão tentando salvaguardar, de que ameaças e por que razão, antes de poder passar a seleção de soluções específicas de segurança (Beal, 2005). Grande parte dos dados importantes ao negócio da empresa está armazenada em computadores, por isso as organizações dependem da confiabilidade de seus sistemas baseados em TI; se a confiança nesses dados for destruída, o impacto pode ser comparável à própria destruição do sistema.

Dessa forma, as organizações precisam adotar controles de segurança – medidas de proteção que abranjam uma grande diversidade de iniciativas – que sejam capazes de proteger adequadamente dados, informações e conhecimentos, escolhidos, levando-se em conta os riscos reais a que estão sujeitos esses ativos (Beal, 2005).

A segurança da informação considera os seguintes elementos, como principais pilares, para orientar a análise, o planejamento e a implementação de tal, a chamada tríade CIA, de acordo com Siewert (2008):

a) Confidencialidade: significa garantir o segredo das informações, liberando acesso somente às pessoas autorizadas; a perda deste atributo ocorre quando pessoas não autorizadas obtêm acesso às informações confidenciais;

b) Integridade: significa garantir que a informação não foi alterada indevidamente, ou seja, devem-se manter as características originais impostas pelo proprietário da informação, mantendo o seu ciclo de vida (nascimento, manutenção e destruição);

c) Disponibilidade: significa garantir a disponibilidade da informação, sempre que necessário às pessoas autorizadas.

Segundo Böger e Bodemüller (2007) os principais mecanismos de segurança são divididos em:

a) Controles administrativos: que são as políticas de segurança;

b) Controles físicos: que são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura, garantindo a existência da informação, que a suporta. Como portas, paredes, trancas, blindagem, guardas;

c) Controles lógicos: que são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico. Exemplos disto são os mecanismos de criptografias, assinatura digital, mecanismos de certificação, controle de acesso, entre outros.

Para colocar em prática tais mecanismos de segurança, deve-se considerar, principalmente, os riscos associados à carência deles à segurança, os benefícios esperados e os custos da implantação dos mesmos.

Fator Humano na Segurança da Informação

Segundo Santos (2011), a principal ameaça para qualquer segurança é o próprio ser humano, pois todo processo de segurança se inicia e termina no usuário do sistema. Assim, para se proteger dos oportunismos da engenharia social, a sociedade da informação deve criar uma cultura que incentive um comportamento humano consciente no domínio das informações, a fim de evitar riscos de perdas, pessoais ou corporativas.

Para Kevin Mitnick:

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis. (Mitnick, 2003, p. 3).

Silva Filho (2004) mostra os traços comportamentais, que tornam o ser humano susceptível a ataques:

a) Persuasão – Compreende quase uma arte a capacidade de induzir pessoas, onde se busca obter respostas específicas. Isto é possível porque as pessoas têm características comportamentais que as tornam vulneráveis à manipulação;

b) Vontade de ser útil – O ser humano, comumente, procura agir com cortesia, bem como ajudar outros quando necessário;

c) Busca por novas amizades – O ser humano costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável e aberto a dar informações;

d) Propagação de responsabilidade – Trata-se da situação na qual o ser humano considera que ele não é o único responsável por um conjunto de atividades.

O fator humano é apenas um dos diversos tipos de vulnerabilidades existentes na área de segurança da informação. Para Peixoto (2006), os principais tipos de vulnerabilidades existentes podem ser do tipo: Físicas; Naturais; Hardware; Software; Mídias; Comunicação e Humanas.

A camada humana é formada por todos os recursos humanos presentes na organização, principalmente os que possuem acesso aos recursos de TI, seja para manutenção ou uso. São aspectos importantes desta camada: a percepção do risco pelas pessoas: como elas lidam com os incidentes de segurança que ocorrem; são usuários instruídos ou ignorantes no uso da TI; o perigo dos intrusos maliciosos ou ingênuos; e a engenharia social (Adachi, 1993).

Das três camadas de segurança existentes: física, lógica e humana, a camada humana é a mais difícil de se avaliar os riscos e gerenciar a segurança, pois envolve o fator humano, com características psicológicas, socioculturais e emocionais, que variam de forma individual (Schneier, 2001).

Para reduzir os riscos relacionados à erros humanos ou atos criminosos por parte dos usuários internos, é aconselhável que a organização estabeleça políticas de informação, controles e procedimentos enfocando a área de pessoal. As atividades dos funcionários devem ser controladas por meio de procedimentos de operação e supervisão, e políticas adequadas de seleção, treinamento, avaliação de desempenho, segregação de funções e interrupção de contratos de trabalho.

A gestão da segurança da informação envolve mais do que gerenciar os recursos de tecnologia – hardware e software – envolve pessoas e processos, porém algumas empresas negligenciam este fator. A política de segurança e a conscientização dos usuários são algumas das formas de se controlar a segurança relacionada ao fator humano.

METODOLOGIA

Considerando o objetivo proposto para este estudo, que visa identificar as estratégias de uso da engenharia social para quebrar a segurança da informação, através de fatores humanos comportamentais, a pesquisa classifica-se, quanto aos objetivos, como **exploratória**. Segundo Gil (2008), a pesquisa exploratória envolve a proporcionar maior familiaridade com o problema (explicitá-lo). Pode envolver levantamento bibliográfico e entrevistas com pessoas experientes no problema pesquisado.

Em relação à abordagem do problema, a pesquisa caracteriza-se como **qualitativa**. De acordo com Oliveira (2000), o método qualitativo "sempre" foi considerado como método exploratório e auxiliar na pesquisa científica. No entanto, o autor destaca que o novo paradigma da ciência coloca o método qualitativo dentro de outra base de concepção teórica na mensuração, atribuindo-lhe valor fundamental no desenvolvimento e consolidação da ciência em diferentes áreas.

Quanto aos procedimentos técnicos, a pesquisa caracteriza-se como **bibliográfica**. Para Gil (2008), a pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos.

ANÁLISE E DISCUSSÃO DOS RESULTADOS

A literatura sobre engenharia social e segurança da informação ajudou a alcançar os objetivos deste estudo, através da metodologia de pesquisa utilizada, gerando os resultados que serão apresentados a seguir.

Relação entre engenharia social e segurança da informação

Levando-se em conta o significado de cada uma das palavras, conforme pesquisa realizada por Peixoto (2004), o termo Engenharia Social não parece ter a conotação maléfica que carrega consigo:

a) Engenharia: Arte de aplicar conhecimentos científicos, empíricos e certas habilitações específicas à criação de estruturas, dispositivos e processos que se utilizam para converter recursos naturais em formas adequadas ao atendimento das necessidades humanas;

b) Social: Da sociedade, ou relativo a ela. Sociável. Que interessa à sociedade.

Porém, a engenharia social não é baseada em ciência natural, mas sim nas ciências humanas e sociais, tais como a filosofia, psicologia, economia, próximas com teorias básicas dos seres humanos e a sociedade (Departament of social engineering Tokyo Institute of Technology, 2006).

Assim, a junção das duas palavras anteriormente definidas traz um significado bem diferente da ideia de harmonia e equilíbrio que expressam quando utilizadas separadamente: Engenharia Social: designa a arte de manipular pessoas a fim de contornar dispositivos de segurança. É baseada na utilização da força de persuasão e na exploração da ingenuidade dos utilizadores de um sistema (*Engenharia Social*, 2009).

A melhor maneira de se proteger das técnicas de engenharia social é utilizar o bom senso para não divulgar informações que poderiam prejudicar a segurança dos dados da organização. Assim, independentemente do tipo de informação pedida, é aconselhável informar-se sobre a identidade do agente mal-intencionado pedindo informações precisas (nome e sobrenome, empresa e número de telefone). Se possível, checar também as informações fornecidas e avaliar a importância das informações pedidas para a obtenção dos efeitos prometidos. Neste contexto, a formação e a sensibilização dos usuários para os problemas de segurança revelam-se altamente necessárias.

Impacto do fator humano na segurança da informação

Após realizada a revisão sistemática de literatura, pode-se perceber que a maioria dos incidentes envolvendo a segurança da informação está diretamente ligada ao fator humano, pois este está totalmente relacionado com a segurança da informação.

Além disso, é notável que questões técnicas são menos impactantes do que questões comportamentais humanas.

Neto e Silveira (2007), realizaram uma pesquisa de campo sobre gestão da segurança da informação em empresas de pequeno e médio porte e constataram que a camada humana é a que carece de maior atenção por parte das empresas, pois foi a que apresentou o menor índice de controles implantados. Os dados confirmam que as empresas investem principalmente em controles tecnológicos para diminuir o risco de incidentes de segurança da informação, porém esquecem que o fator humano é uns dos grandes responsáveis por falhas na segurança.

A segurança da informação está mais relacionada com os processos e as pessoas do que com a própria tecnologia. Dessa forma, não há vantagem em investir pesado em tecnologia e deixar de lado o fator humano.

CONSIDERAÇÕES FINAIS

Este trabalho buscou, além dos objetivos propostos, oferecer sua contribuição acadêmica, a partir de uma perspectiva mais abrangente, integradora, em busca da melhoria na compreensão das questões que envolvem o uso da engenharia social para comprometer a segurança da informação. O trabalho atingiu os objetivos estabelecidos, que eram colaborar como um instrumento de conscientização a respeito do tema proposto, mostrando que as pessoas podem ser manipuladas e terem suas informações extraviadas de maneira simples.

O presente artigo procurou abordar a engenharia social de maneira a esclarecer sua relação com a segurança da informação e exaltar a importância dos ativos de informação para as organizações e a necessidade de protegê-los.

Como apontado no decorrer deste estudo, não há literatura extensa sobre a relação explícita entre engenharia social e segurança da informação. São oportunidades para avanços aos quais os pesquisadores e profissionais podem se dedicar.

Como sugestão para trabalhos futuros, pode-se apontar a necessidade de metodologias, ferramentas ou práticas de segurança da informação voltadas exclusivamente à engenharia social e ao fator humano nas organizações.

REFERÊNCIAS

Adachi, T. (1993). *Gestão de Segurança em Internet Banking* (Mestrado). Fundação Getúlio Vargas – Administração. Orientador: Eduardo Henrique Diniz, São Paulo: FGV.

Beal, A. (2005). *Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações.* Atlas.

Bellavista, A. (1991, 9). Quale legge sulle banche datti? *Rivista Critica del Diritto Privato*, *9*(3).

Böger, D. S., & Bodemüller Junior, R. (2007). *Segurança da Informação.* Recuperado em 18 out. 2018, de https://goo.gl/rXjaui

C., H., & Maxwell, E. (2009). *Social Engineering Defined.* Social engineering framework. Recuperado em 15 out. 2018, de https://goo.gl/swbGAf

Coelho, F., Rasma, E., & Morales, G. (2013). Engenharia Social: Uma Ameaça à Sociedade da Informação. *Revista Perspectivas Online*. Recuperado em 15 out. 2018, de https://goo.gl/74kwCq

Departament of social engineering Tokyo Institute of Technology. (2006). *WHAT is Social Engineering.* Recuperado em 15 out. 2018, de https://goo.gl/JZHVq7

Eiras, M. C. (2004). *Engenharia Social e Estelionato Eletrônico* (Monografia (Conclusão de Curso – lato sensu)). IBPINET – The internet school e Uni-Rio, Graduação em Segurança da Informação na Internet, São Paulo: FGV.

Engenharia Social. (2009). Recuperado em 18 out. 2018, de http://pt.kioskea.net/contents/attaques/ingenieriesociale.php3

Gil, A. C. (2008). *Como elaborar projetos de pesquisa.* Atlas.

Marciano, J. L., & Marques, M. L. (2006). O Enfoque Social da Segurança da Informação. *Revista Ciência da Informação*, *35*(3), 89-98.

Mitnick, K. (2001). *My first RSA Conference.* Recuperado em 6 out. 2018, de http://www.securityfocus.com/news/199

Mitnick, K. (2003). *A arte de enganar. Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação.* Pearson Education.

Netto, A., & Silveira, M. (2007). Gestão da Segurança da Informação: Fatores que influenciam sua adoção em pequenas e médias empresas. *Revista de Gestão da Tecnologia e Sistemas de Informação*, *4*(3), 375-397. doi: 10.1590/S1807-17752007000300007

Oliveira, C. d. S. (2000). *Metodologia científica, planejamento e técnicas de pesquisa: uma visão holística do conhecimento humano.* LTR.

Peixoto, M. C. P. (2004). *Gestão da segurança da informação no contexto da vulnerabilidade técnica e humana inserida nas organizações* (Monografia (Conclusão de Curso)). Centro Universitário do Triângulo, Pró-Reitoria de Ensino de Graduação de Ciência da Computação, Uberlândia.

Peixoto, M. C. P. (2006). *Engenharia Social e Segurança da Informação na Gestão Corporativa.* Brasport.

Santos, L. A. F. d. (2011). *Segurança da informação.* Recuperado em 15 out. 2018, de http://www.slideshare.net/luiz_arthur/seguranca-da-informao-introduo

Schneier, B. (2001). *Segurança.com: segredos e mentiras sobre a proteção na vida digital.* Campus.

Siewert, V. C. (2008). *A Constante Evolução da Segurança da Informação.* Recuperado em 13 out. 2018, de http://artigocientifico.uol.com.br/uploads/artc_1202929819_49.pdf

Silva, E. M. d. (2008). *Cuidado com a engenharia social: Saiba dos cuidados necessários para não cair nas armadilhas dos engenheiros sociais.*

Silva Filho, A. M. (2004, 12). Entendendo e Evitando a Engenharia Social: Protegendo Sistemas e Informações. *Revista Espaço Acadêmico*, *4*(43), 375-397. Recuperado em 15 out. 2018, de http://www.espacoacademico.com.br/043/43amsf.htm

Sêmola, M. (2003). *Gestão da Segurança da Informação: uma visão executiva.* Campus.

Como citar este artigo (APA):
Aramuni, J. P. & Maia, L. C. (2018). O impacto da Engenharia Social na Segurança da Informação: uma abordagem orientada à Gestão Corporativa. *AtoZ: novas práticas em informação e conhecimento, 7*(1), 31 – 37. Recuperado de: http://dx.doi.org/10.5380/atoz.v7i1.64640