Pós-Graduação em Ciência da Computação

FRANCISCO DE ASSIS FIALHO HENRIQUES

A influência da Engenharia Social no fator humano das organizações

Universidade Federal de Pernambuco
posgraduacao@cin.ufpe.br
www.cin.ufpe.br/posgraduacao

Recife
2016

FRANCISCO DE ASSIS FIALHO HENRIQUES

A influência da Engenharia Social no fator humano das organizações

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre Profissional em Ciência da Computação.

Orientador: Ruy José Guerra Barretto de Queiroz
Coorientador: Omar Andres Carmona Cortes

Recife
2016

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

H519i Henriques, Francisco de Assis Fialho
A influência da Engenharia Social no fator humano das organizações / Francisco de Assis Fialho Henriques. – 2017.
112 f.: il., fig.

Orientador: Ruy José Guerra Barretto Queiroz.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2017.
Inclui referências e apêndices.

1. Segurança da informação. 2. Engenharia social. I. Queiroz, Ruy José Guerra Barretto (orientador). II. Título.

005.8 CDD (23. ed.) UFPE- MEI 2017-127

Francisco de Assis Fialho Henriques

A influência da Engenharia Social no fator humano das organizações

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre Profissional em 06 de março de 2017.

Aprovado em: 06 / 03 / 2017

Prof. Hermano Perrelli de Moura
Centro de Informática/UFPE

Prof. Rodrigo Elia Assad
Universidade Federal Rural de Pernambuco

Prof. Ruy José Guerra Barretto de Queiroz
Centro de Informática / UFPE
(Orientador)

A meus pais , Vitoriano e Flaviana Henriques pelo apoio incondicional e que, com muito amor, sempre me ensinaram a trilhar pelos caminhos do bem.

A meu irmão Franz Henriques, pela parceria , pelos momentos alegres e principalmente por trazer ao mundo duas criaturinhas tão lindas : Pedro e Bianca.

A meu amor Ana Carolina Viana , por todo o amor , atenção e paciência de sempre.

Agradecimentos

Agradecimentos especiais a todos os amigos da Turma de Mestrado Profissional de Gestão em TI - uma grande família - em especial à Carol Picanço, Fernando Amorim, Jonas Ferreira e Robert Mercenas**.** Companheiros de lutas, alegrias e muitas risadas compartilhadas.

À Consultora e Instrutora de Segurança da Informação, Lilian Pricola, pelas dicas importantes e pelo seu tempo gasto com preciosas orientações durante várias etapas da pesquisa.

Ao professor e amigo Dr. Omar Andres Carmona Cortes, pela disponibilidade em ajudar na coorientação do trabalho.

Ao professor Dr. Ruy José Guerra Barreto de Queiroz, pelo apoio e liberdade dada para o desenvolvimento do mesmo.

A todos aqueles que disponibilizaram um pouco do seu tempo para responder ao questionário e possibilitarem a realização desse trabalho.

Agradecimentos aos professores do CIn-UFPE, que contribuiram com seus brilhantes ensinamentos;

A todos que direta ou indiretamente ajudaram de alguma forma.

“Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. ”

Sun Tzu

Resumo

A informação tornou-se um recurso essencial na sociedade contemporânea. As organizações estão investindo cada vez mais em tecnologia e equipamentos para fortalecer sua segurança e estão esquecendo as pessoas, o fator humano está ficando para trás. Com o crescimento das redes de computadores e o surgimento da tecnologia da informação, os ataques de Engenharia Social têm sido uma ameaça atual aos sistemas de informação em ambientes organizacionais. A fim de criar ações de contenção contra essa ameaça, é necessário entender o comportamento dos atacantes, ou seja, quais são as principais ações tomadas para alcançar os objetivos desejados. Não há nenhuma correção que você pode adquirir e aplicar às pessoas para ser livre destas formas de ataque. A solução para combater esse problema é o conhecimento. As pessoas devem entender como lidar com as formas de ataque e o que fazer para minimizar essa questão nas organizações. O presente estudo avaliou, através da aplicação de um questionário, o conhecimento dos entrevistados sobre Engenharia Social, à medida que percebem sua influência nas organizações e como estas abordam a questão da Segurança da Informação. O objetivo deste estudo é apresentar como as técnicas de Engenharia Social são aplicadas nas organizações respondendes e quanto estão preparados para enfrentar esta ameaça, sugerindo uma visão mais humana da Segurança da Informação.

Palavras-chave: Informação. Segurança da Informação. Privacidade. Engenharia Social. Vulnerabilidades.

Abstract

Information has become an essential resource in contemporary society. Organizations are increasingly investing in technology and equipment to strengthen their security and are forgetting people, the human factor is falling behind. With the growth of computer networks and the Emergence of information technology, Social Engineering attacks have been a current threat to information systems in organizational environments. In order to create containment actions against this threat, it is necessary to understand the behavior of the attackers, i.e. what are the main actions taken to achieve the desired objectives.There is no correction that you can acquire and apply to people to be free from these forms of attack. The solution to combat this problem is knowledge. People should understand how to deal with the forms of attack and what to do to minimize this question in organizations. The present study evaluated, through the application of a survey, the knowledge of the interviewees about Social Engineering, as they perceive its influence in the organizations and how they address the issue of Information Security. The aim of this study is to present how the Social Engineering techniques are applied in responding organizations and how much they are prepared to face this threat suggesting a more human vision of Information Security.

.***Keywords:*** *Information. Information Security. Privacy. Social Engineering. Vulnerabilities.*

Lista de ilustrações

Lista de quadros

Lista de gráficos

Sumário

1 INTRODUÇÃO

A informação tem desempenhado um papel importante na sociedade contemporânea. Nesse contexto, surge a tecnologia da informação cujos impactos globais caracterizam nossa sociedade como uma sociedade da informação, tornando os sistemas informatizados de suma importância para seu funcionamento.

Assim, o crescimento dos sistemas informatizados gera um universo de conteúdos e ambientes sujeitos a ameaças que comprometem a estrutura da relação usuário-sistema-informação (MARCIANO; LIMA-MARQUES, 2006). Além disso, com o aumento e popularização das redes de computadores, há um crescente aumento do número de pessoas/usuários, consequentemente aumentando também a quantidade de vulnerabilidades nas organizações. E, sendo a informação um ativo importante na sociedade contemporânea, a mesma precisa ser protegida.

A Internet permitiu que as empresas ficassem conectadas, de forma que os intercâmbios e a produção de riqueza fossem favorecidas, ao mesmo tempo que novas vulnerabilidades pudessem ser exploradas por elementos mal intencionados. Com os sistemas de informações conectados à Internet, os fluxos de informações das empresas se vêem ameaçados por interceptação e/ou manipulação de terceiros.

Dentre as vulnerabilidades que podem ser exploradas está o ataque de engenharia social, que se tornou uma grande aceitação na comunidade de tecnologia como uma efetiva ferramenta social e psicológica para explorar os mecanismos de segurança de TI de uma organização alvo.

A engenharia social assume diversas formas e pode ser compreendida como a “arte de enganar”. Não é apenas utilizada em sistemas informatizados, é também usada para explorar falhas humanas nas organizações para obtenção de segredos industriais ou suspensão de serviços.Os ataques de engenharia social são ações que exploram a boa vontade das pessoas, colocando o atacante em uma posição privilegiada no fluxo de informação (MITNICK; SIMON, 2003).

A segurança é um processo e está em constante evolução. Os riscos que aceitamos, quer por escolha quer por necessidade, estão em constante mutação. Mas eles estão sempre lá. É preciso um trabalho de conscientização, de construção de políticas, treinamentos. Boas práticas de segurança usam tecnologia, mas estão focadas em torno de pessoas. Os bons sistemas de segurança são projetados para maximizar o valor que as pessoas podem oferecer e, ao mesmo tempo, minimizar as vulnerabilidades inerentes ao seu uso.

As pessoas são dinâmicas e melhor capazes de reagir a novas ameaças e

responder a novas situações do que a tecnologia (SCHNEIER, 2003).

Em virtude desse cenário, formula-se as seguintes questões de pesquisa: (1) Como os ataques de engenharia social se processam sobre as organizações e (2) O quanto estas organizações estão preparadas para enfrentar essa ameaça?

1.1 Justificativa

O conceito de engenharia social como ciência e seu uso como meio de persuasão de indivíduos ou organizações para cumprir um requerimento específico através da interação social (MOUTON et al., 2014), sustenta a idéia de que é relevante realizar a identificação da origem e do *modus operandi* dos engenheiros sociais, buscando analisar as falhas de segurança inseridas pelo fator humano nas organizações, demonstrar como os ataques de engenharia social se processam sobre as organizações e qual o nível de preparo para enfrentar essa ameaça. É importante avaliar qual a relação de conformidade existente entre os processos de segurança das empresas investigadas com boas práticas de mercado e técnicas de Segurança da Informação.

A existência de política e dos demais regulamentos de proteção da informação, é fundamental para definir as diretrizes e os direcionamentos que a organização deseja para os controles a serem implantados (FONTES, 2012).

Muitas empresas estão olhando para as normas internacionais de segurança, que abrangem muitas áreas de atuação como recursos humanos, TI e continuidade dos negócios. Mas uma fraqueza dessas normas é que seu aspecto de reconhecimento da engenharia social como ameaça é pobre, tratando apenas de uma cobertura mínima de conscientização do usuário e treinamentos, sem conseguir direcionar as pessoas para a total compreensão das ameaças de engenharia social (MANN, 2008).

A Symantec Corporation (2016) cita em seu relatório anual que um conjunto de empresas multinacionais e agências do governo sofreram ataques diversificados e, em vários casos, as vítimas dentro de cada companhia eram pesquisadas para, em seguida, serem atacadas através de engenharia social personalizada para acessar as redes.

Esta pesquisa pretende colaborar com o conhecimento científico identificando métodos de ataque voltados ao fator humano, mostrando um outro cenário para aqueles responsáveis por cuidar da segurança de informações em seus ambientes organizacionais.

Existe uma grande oportunidade de chamar a atenção para engenharia social como verdadeira ameça, não apenas aos ataques voltados para sistemas informatizados. A referida pesquisa poderá também, fornecer material para a criação de métodos de diagnose de vulnerabilidades à engenharia social.

Serão propostas ações a serem seguidas de forma a mitigar essa ameaça nas corporações, no sentido de identificar métodos de ataque de engenharia social ligados a determinadas vulnerabilidades existentes na organização.

1.2 Objetivos e Escopo

1.2.1 Objetivo Geral

Determinar como os usuários de TI, gestores ou não, percebem a influência da engenharia social em suas organizações e qual o potencial de vulnerabilidade dessa influência.

1.2.2 Objetivos Específicos

1) Investigar aspectos relativos a fatores humanos em Segurança da Informação em ambientes corporativos;
2) Verificar o nível de impacto de ataques de engenharia social nos ambientes corporativos pesquisados e sua visão;
3) Identificar as técnicas utilizadas em ataques de engenharia social e métodos de defesa;
4) Analisar o conhecimento de empregados acerca de Segurança da Informação e ataques de engenharia social;
5) Identificar as vulnerabilidades do fator humano que são explorados por ações de engenharia social;
6) Sugerir ações para mitigar o risco de ataques de engenharia social às empresas.

1.2.3 Escopo

Foram investigados o nível de conhecimento de uma amostra de pessoas - usuários de sistemas de informação em diferentes áreas de trabalho - sobre a segurança de informação e o conhecimento específico sobre a engenharia social. A pesquisa deu-se através de questionário enviado a usuários de sistemas e gestores de TI não havendo qualquer tipo de ataque prático às empresas/pessoas avaliadas.

Aborda-se a engenharia social e seu conceito, bem como a Segurança da Informação e sua importância nos dias atuais para as pessoas e para as organizações

que sempre vão utilizar pessoas para controlar e manipular as informações que circulam em seu ambiente. Posteriormente serão observadas algumas características que as tornam vulneráveis à engenharia social e as principais características de um ataque.

Foi excluído do escopo da pesquisa os ataques de engenharia social às organizações ou pessoas entrevistadas, assim como o uso de qualquer ferramenta para execução de phishing ou outro tipo de coleta de dados.

Busca-se estabelecer os procedimentos que devem ser elencados em uma política de segurança e verifica-se se os mesmos contemplam métodos específicos para a contenção de ataques de engenharia social.

1.3 Metodologia

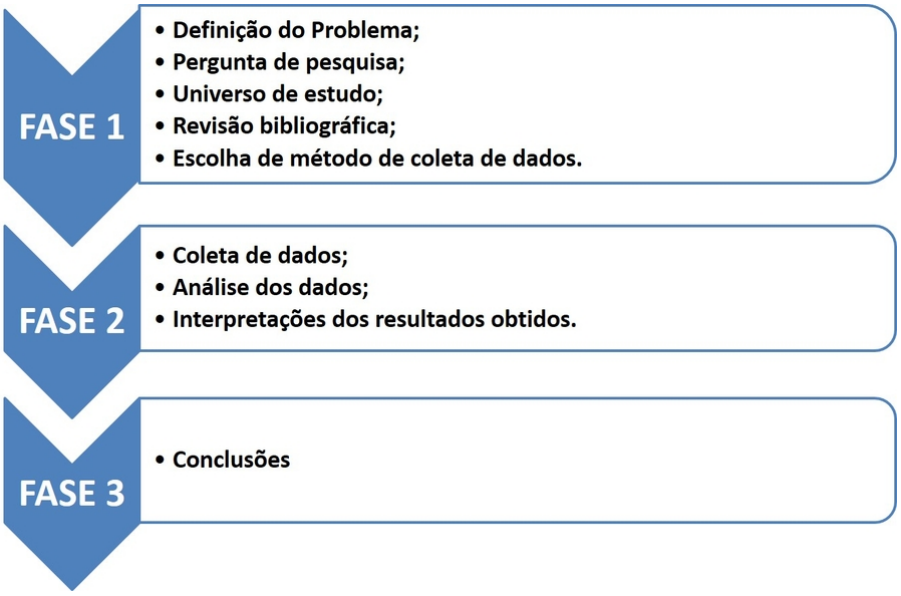
As pesquisas, do ponto de vista dos objetivos podem ser: exploratórias, descritivas e explicativas. O principal objetivo da pesquisa descritiva é “descrever as características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis. Envolve o uso de técnicas padronizadas de coleta de dados: questionário e observação sistemática. Assume, em geral, a forma de levantamento” (SILVA; MENEZES, 2005 apud GIL, 2008).

O trabalho desenvolvido pode ser visto como descritivo, pois tem como objetivo analisar como as pessoas nas organizações são afetadas pelos ataques de engenharia social e como os mesmos afetam a segurança de informações das pessoas e organizações. Com propósito claramente definido,o processo de pesquisa foi precedido por um levantamento bibliográfico de dados coletados por questionário.

A pesquisa científica pode englobar um universo muito grande de elementos, o que pode tornar impossível obter a totalidade de elementos. Deste modo, utiliza-se amostras, uma parcela do universo selecionado (GIL, 2008).

A pesquisa se formou a partir de levantamento bibliográfico sobre Segurança da Informação e ataques de engenharia social; estudo em relatórios e artigos publicados em jornais e revistas especializadas (fontes secundárias) e questionário aplicado com usuários de várias empresas e segmentos de mercado e empresas de sistemas de tecnologia. A figura 1 mostra o fluxo da pesquisa que é composta de 3 fases:

Figura 1 – Fluxo da pesquisa



Fonte: Autor

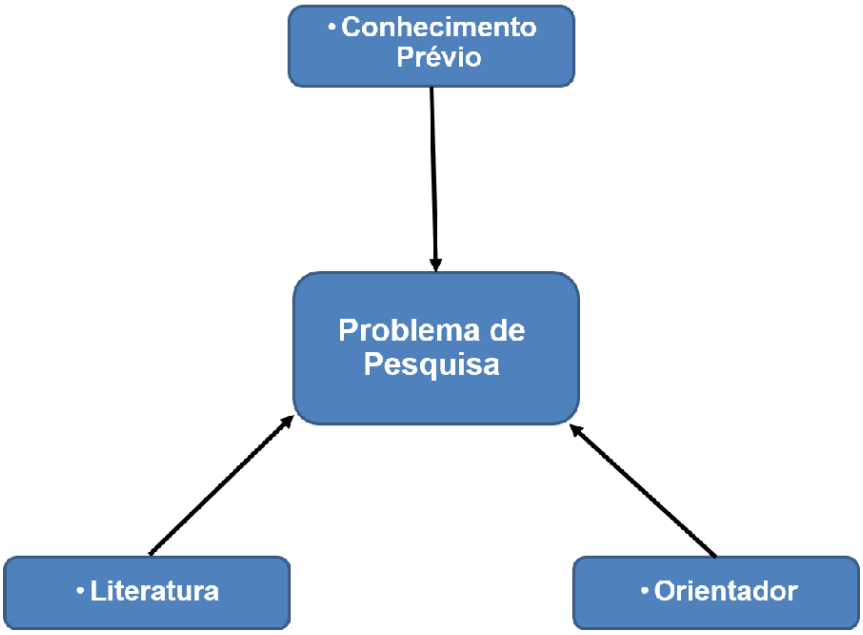
Fase 1: definição do problema/pergunta de pesquisa, universo de estudo, revisão bibliográfica e escolha do método de coleta de dados;

O problema normalmente é definido em forma de pergunta, pois, refletindo uma curiosidade compartilhada pela comunidade científica o pesquisador deve escrevê-lo de forma que o trabalho seja entendido por todos. Os leitores devem interessar-se pelos resultados obtidos e procedimentos metodológicos adotados na pesquisa caso possuam a mesma curiosidade. Através da revisão bibliográfica e da análise de outros trabalhos, ao notar uma pergunta sem resposta, o autor captura uma oportunidade de pesquisa. (ALVES, 2015)

A origem do problema de pesquisa é demonstrado na Figura 2. A partir de um conhecimento prévio sobre o assunto a ser estudado, foram levantadas questões cujas respostas foram encontradas na revisão bibliográfica. Através de uma leitura mais detalhada de autores que realizaram estudos sobre o mesmo tema, foram observadas lacunas que os próprios autores declaram como oportunidades para trabalhos futuros.

Após identificados potenciais problemas, foi escolhida juntamente com o orientador, uma questão de interesse escrita na forma de problema de pesquisa.

Figura 2 – Origem do problema de pesquisa



Fonte: Alves, 2015 (Adaptado pelo autor)

O método científico “é uma premissa sobre como o conhecimento é construído”. Além disso, o método hipotético-dedutivo sugere que, a partir de um conhecimento previamente construído e de uma lacuna observada, o pesquisador pode propor novas teorias, em formato de hipóteses ou proposições (DRESCH; LACERDA; ANTUNES JÚNIOR, 2015).

O desenvolvimento deste trabalho utiliza-se de pesquisa conduzida pela abordagem do tipo *survey*, e de acordo com Dresch, Lacerda e Antunes Júnior (2015) tem como objetivo “desenvolver conhecimento em uma área específica”. Segundo os autores, a investigação é conduzida por meio da coleta de dados e/ou informações, para avaliar o comportamento das pessoas e/ou ambientes em que se encontram.

Buscou-se realizar uma análise quantitativa a partir de dados coletados de pessoas, usuários de sistemas de informação de instituições empresariais e governamentais. Os dados disponibilizados no trabalho são resultado de questionário enviado a gestores de TI e usuários de empresas de diversos ramos de atuação no mercado.

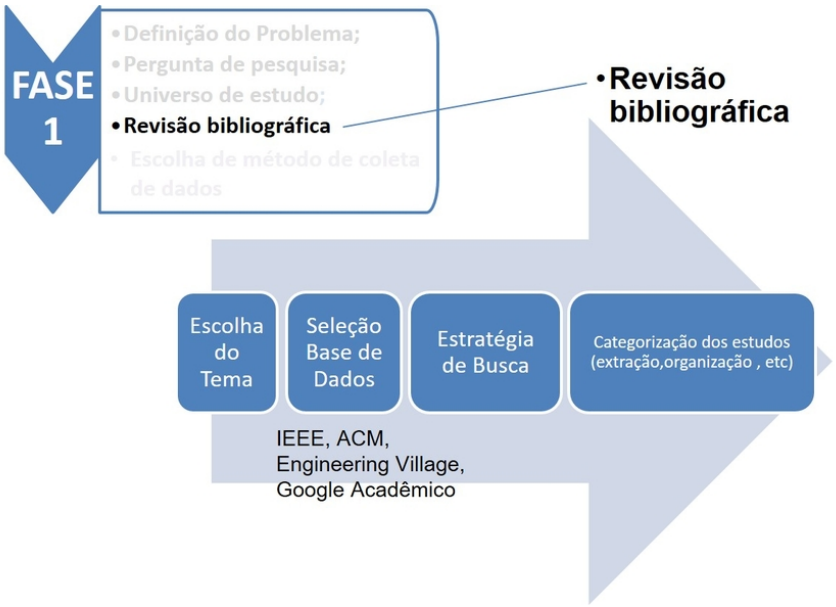
Conclusões foram obtidas a partir da população estudada. O tema engenharia social foi explorado através de um levantamento bibliográfico no contexto corporativo e buscou levantar através de usuários do meio empresarial, quais são as influências sofridas pelas empresas através de seu elemento humano.

De acordo com Cervo e Bervian (2002)a referência bibliográfica “busca conhecer e analisar as contribuições culturais ou científicas existentes sobre um determinado assunto, tema ou problema.” Procura explicar um problema a partir de referências

teóricas publicadas em documentos.

Diversas fontes bibliográficas foram utilizadas, detalhando aspectos técnicos do problema e justificando a análise do problema frente às ameaças constantes sobre as instituições. A figura 3 detalha o processo de revisão bibliográfica:

Figura 3 – Fluxo de Revisão Bibliográfica



Fonte: Autor

Os recursos e estratégias para busca e seleção de estudos foram definidos e selecionados com base em:

• Fontes de busca: base de dados eletrônicas indexadas (IEEE, ACM, Engineering Village, Google Acadêmico) e anais de conferências relacionadas ao assunto;

• Idioma: preferencialmente a língua inglesa, por ser considerado o idioma mais aceito internacionalmente para artigos científicos na área de pesquisa.Artigos relevantes na língua portuguesa, publicados em eventos nacionais relacionados à área de pesquisa, também foram considerados;

• Palavras-chave: engenharia social, gestão da segurança, information security, privacidade, privacy, riscos, risk, security frameworks, security management, Segurança da Informação, social engineering, vulnerabilidades, vulnerability.

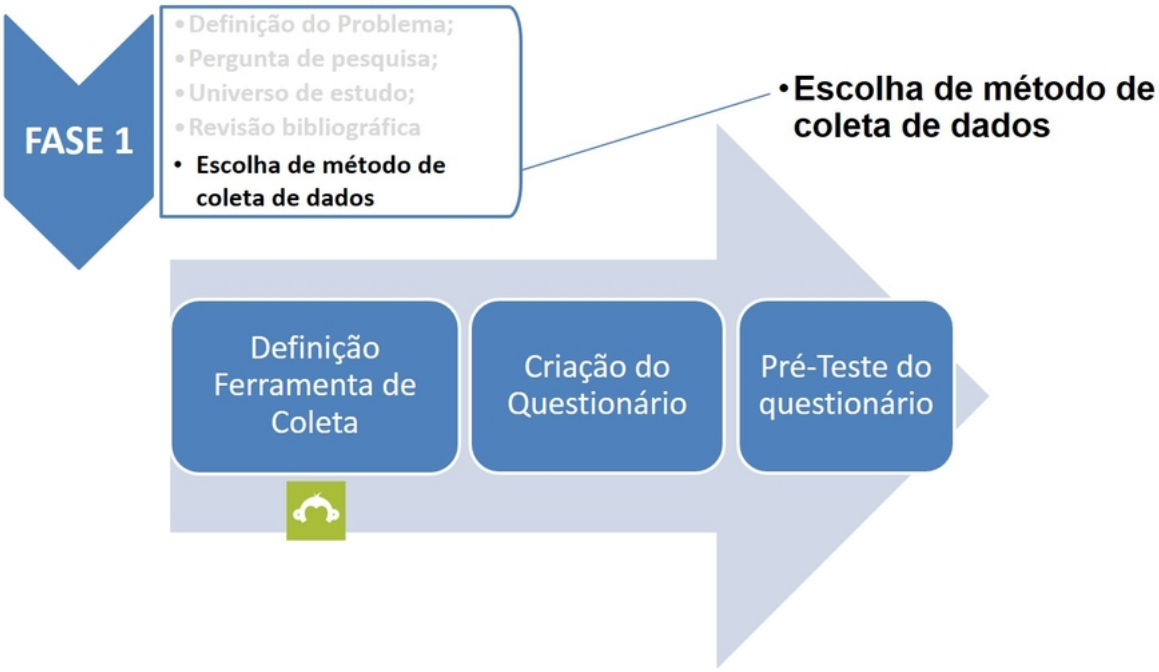
Uma string de busca foi formada pela combinação das palavras-chave identificadas e submetidas às máquinas de busca relacionadas. Os trabalhos recuperados das bases foram inicialmente armazenados em um software de organização de referências bibliográficas, em seguida realizada a leitura dos resumos dos trabalhos armazenados.

Os resultados serão apresentados sob discussão a partir dos dados coletados nas entrevistas,respostas a questionários, bases teóricas e confronto com as teorias existentes.

Buscou-se, em consequência da pesquisa, identificar de forma mais ampla os riscos dos ataques de engenharia social nas operações das empresas, incentivar o conhecimento de conceitos de segurança de informação por parte dos usuários e obter maior participação dos responsáveis pelo manuseio de informações e ativos críticos, auxiliando na redução dos problemas de segurança na organização.

Ainda na primeira fase, a escolha do método de coleta de dados é definido conforme Figura 4.

Figura 4 – Escolha de método de coleta de dados



Fonte: Autor

Para operacionalização da pesquisa foi utilizado o site www.surveymonkey.com, onde foi disponibilizado o formulário de pesquisa no endereço **https://pt.surveymonkey.com/r/5YH8JYH.**

O endereço foi divulgado de duas formas. Inicialmente foi criado um link de divulgação do endereço de pesquisa, o qual foi distribuido para 10 profissionais especialistas e professores da área de Segurança da Informação para que pudessem fazer a validação do questionário. Especialistas em Segurança da Informação e alguns respondentes foram escolhidos aleatoriamente para darem sugestões e avaliarem

se o questionário se propõe a avaliar a influência da engenharia social no universo investigado.

1.4 Estrutura do Trabalho

A pesquisa divide-se em cinco capítulos: Capítulo 1, trata-se a contextualização da pesquisa focada na engenharia social como fator de influência sobre as pessoas das organizações. O capítulo possui as seções de Introdução, Justificativa, Objetivos e Escopo, Metodologia e a Estrutura Geral do Trabalho. Neste capítulo, apresenta-se a metodologia definida, a questões principais da pesquisa são levantadas de forma a orientar o trabalho investigativo.

No Capítulo 2 apresenta-se a fundamentação teórica da pesquisa, onde são abordados os conceitos de Informação e Conhecimento, o contexto histórico da Segurança da Informação com seus princípios e ameaças e a engenharia social, seus conceitos, sua influência nas empresas e o que fazer para mitigar esse problema.

O Capítulo 3 trata sobre a coleta de dados. Neste capítulo são apresentados os procedimentos feitos para a criação do questionário de pesquisa e sua divulgação.

O Capítulo 4 apresenta os resultados e discussão. Este capítulo trata sobre os resultados da coleta de dados através do questionário. É a apresentação e discussão dos resultados da pesquisa através de gráficos, detalhando os resultados obtidos.

O Capítulo 5 apresenta as considerações e trabalhos futuros demonstrando as conclusões finais, limitações e propostas para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Segundo Prodanov e Freitas (2013), a revisão da literatura demonstra que o pesquisador está atualizado nas últimas discussões no campo de conhecimento em investigação.

O referencial teórico que norteia a pesquisa abordando os conceitos de Segurança da Informação, as melhores práticas ditadas pelos frameworks de Segurança da Informação, além de conceitos de engenharia social e suas diversas manifestações ao longo do tempo e técnicas usadas nesse tipo de ataque às organizações.

A revisão de literatura/pesquisa bibliográfica contribuirá para: obter informações sobre a situação atual do tema ou problema pesquisado; conhecer publicações existentes sobre o tema e os aspectos que já foram abordados; verificar as opiniões similares e diferentes a respeito do tema ou de aspectos relacionados ao tema ou ao problema de pesquisa (SILVA; MENEZES, 2005).

2.1 Segurança da Informação

2.1.1 Informação e Conhecimento

Michaelis (2016) registra as seguintes definições e origem do termo informação:

> 1 Ato ou efeito de informar(-se).
> 2 Conjunto de conhecimentos acumulados sobre certo tema por meio de pesquisa ou instrução.
> 3 Explicação ou esclarecimento de um conhecimento, produto ou juízo; comunicação.

Em todas essas definições o termo informação está relacionado ao conhecimento e à comunicação. Com um papel definido na sociedade contemporânea, a informação desempenha um papel central como ativo e o surgimento da tecnologia da informação e seus impactos globais caracterizam nossa sociedade como uma sociedade da informação.

A informação é um ativo como qualquer outro ativo importante para o negócio, tem um valor para a organização e consequentemente necessita ser adequadamente protegida (ABNT, 2013).

A Segurança da Informação protege a informação de vários tipos de ameaças para garantir a continuidade do negócio.

As organizações precisam entender o conceito de que, conhecimento e informação devem ser levados a todos os ambientes da organização. A informação agrega

valor aos bens, quanto maior a informação agregada à produção de um bem, mais ele será valorizado (DIAS, 2014).

Os processos de trabalho são realizados por pessoas que atuam junto à TI em um espaço organizacional. Esse ciclo se inicia com a criação da informação que sempre é produzida pelas pessoas ou pelos computadores por meio do processamento. Essa informação criada passa por uma série de fases que inicia com o registro da informação, que fornece um caráter de permanência à mesma, seguida pela coleta por pessoas que usarão essa informação em um momento posterior(FERNANDES, 2013).

Para que isso aconteça, a informação precisa ser organizada de forma que possa ser feita sua classificação, localização e posteriormente haja a recuperação dessa informação.

Uma vez organizada e armazenada, onde pode passar muito tempo, a informação pode ser publicada ou descartada. Sendo ela necessária e mantida no ambiente organizacional, ela passa por um processo chamado distribuição, que visa tornar a informação passível de busca por um usuário que, após buscar essa informação, faz o acesso a ela, usando-a e fechando assim o ciclo com a criação de novas informações baseadas em informações muitas vezes já existentes.

ABNT (2013) nos ensina que:

> A informação tem um ciclo de vida natural, desde a sua criação e origem, armazenagem, processamento, uso e transmissão, até a sua eventual destruição ou obsolecência. O valor e os riscos aos ativos podem variar durante o tempo de vida da informação (por exemplo, revelação não autorizada ou roubo de balanços financeiros de uma companhia, é muito menos importante depois que elas são formalmente publicadas), porém a Segurança da Informação permanece importante em algumas etapas de todos os estágios.

A relação entre esses conceitos é apresentada na Figura 5:

Figura 5 – O Ciclo da Informação

Fonte: (Fernandes, 2013)

Castells (1999) diz:

> A tecnologia da informação tornou-se ferramenta indispensável para a implantação efetiva dos processos de reestruturação socioeconômica. De especial importância, foi seu papel ao possibilitar a formação de redes como modo dinâmico e auto-expansível de organização da atividade humana. Essa lógica preponderante de redes transforma todos os domínios da vida social e econômica.

Vivemos em uma sociedade informacional. Deixamos o trabalho informal, o trabalho mecânico e partimos para uma sociedade onde o conhecimento e a informação são aplicados para a geração de bens, de valores. Para designar que a nova sociedade não mais se caracteriza pelo modo de produção industrial, várias nomenclaturas foram atribuídas a essa nova sociedade.

Dantas (1996) nos ensina que:

> A Sociedade da Informação caracteriza uma etapa alcançada pelo desenvolvimento capitalista contemporâneo, no qual as atividades humanas determinantes para a vida econômica e social organizam-se em torno da produção, processamento e disseminação da informação através das tecnologias eletrônicas.

Tofler e Tofler (1994) em Guerra e Anti-Guerra, impõe um novo comportamento:

> Essa nova civilização traz consigo novos estilos de famílias;modos de trabalhar, amar e viver diferentes.

Uma nova estrutura social dominante surgiu, ao fim dos anos 60, com três processos independentes: a revolução da tecnologia da informação, a crise econômica do capitalismo e estatismo com suas posteriores reestruturações e o ápice de movimentos sociais e culturais como libertarismo, direitos humanos, feminismo e ambientalismo.(CASTELLS, 1999)

Meira ()(2013) nos diz que a noção de sociedade da informação foi estabelecida por Fritz Machlup em 1962; as economias associadas a educação, pesquisa e desenvolvimento representavam 29% da economia americana em 1959.

A revolução da tecnologia da informação acentuará seu potencial transformativo. O século XXI será marcado pela conclusão da Infovia global, pela telecomunicação móvel e pela capacidade da informática, descentralizando e difundindo o poder da informação. Para a produção de ferramentas e objetos, usamos aparatos para tratar o ciclo de vida da informação e, dentre tantas opções que podem ser a solução de um problema, os mais simples serão preferidos aos mais complexos, desde que exerçam o mesmo papel.

Fernandes e Borges (2012) nos diz que “as pessoas buscam informações junto às outras visando à tomada de decisões”. Podem ser decisões simples ou complexas, de curto prazo, ou de longo prazo, de pequeno impacto ou de grande impacto.

Segundo Drucker (2011 apud MEIRA,)(2013) “o modelo para as tecnologias contemporâneas e seu uso e impacto na sociedade é organizado ao redor da informação.”

Capacidade técnica e tecnológica ganharam valorização para o desempenho de várias atividades, dando muita força a serviços e ao trabalho de valor agregado.

A informação por si mesma não garante sucesso, é necessário que seja lapidada e transformada em conhecimento, e que, ao ser compartilhado alcance maior vantagem competitiva e inovação.

Após o surgimento do termo “Era da informação”, determinado por Castells (1999), a Segurança da Informação surgiu como um termo mais visível. A informação tornou-se um bem fundamental para as organizações e suas estratégias.

No instante em que os setores tradicionais das indústrias, intensivos em mão-de-obra e maquinaria migram para setores representados pelo grande uso de TICs as práticas de gestão de conhecimento devem ser verificadas.

Chiavenato (2005) nos diz que a palavra conhecimento,pode significar informação, conscientização, saber, cognição, sapiência, percepção, ciência, experiência, qualificação, discernimento, competência, habilidade, prática.

“O conhecimento é um conjunto de informações, não o acúmulo delas, mas um agrupamento articulado, “significa compreender todas as dimensões da realidade, captando e expressando essa totalidade de forma cada vez mais ampla e integral” ”. (ANGELONI, 2003 apud SCHRÖEDER; ANTUNES; OLIVEIRA, 2011)

O conhecimento passa a ter um valor agregado nas habilidades de diversas funções. É a substituição da mão-de-obra desqualificada, de produção mecânica e seriada, para o reconhecimento das singularidades no processo de trabalho. A competência por habilidades passa a acentuar e sofisticar o mercado de trabalho.

> “Confere uma idéia ou noção sobre algo aliado à experiência de vida e ao discernimento sobre a vasta gama de dados, informações ou conhecimentos gerados constantemente no ambiente.”(SCHRÖEDER; ANTUNES; OLIVEIRA, 2011)

O fenômeno informação necessita de duas coisas fundamentais: organização e gestão dessa informação e a comunicação e uso dessa informação.Pensar como gerir e organizar essa informação com qualidade.Quem necessita dela? A informação está íntegra? Quem pode acessá-la? As questões relacionadas à Segurança da Informação devem ser pensadas quanto à sua integridade, seu acesso e sua disponibilidade.

Mandarino Júnior (2010) nos ensina que os valores sociais e econômicos foram alterados sem a percepção dessas mudanças a médio ou a longo prazo. A necessidade de garantir que esta quantidade de informações, que se faz presente no cotidiano das pessoas, esteja segura é muito grande.

Os fluxos de informação e comunicação precisam ser garantidos, implicando assim na necessidade de Segurança da Informação. Quando falamos em segurança, seja no mundo real ou no mundo virtual, observamos uma evolução constante de ataques e formas de proteção. Novos ataques promovem novas formas de proteção que por sua vez faz com que surjam novas formas de ataque, criando um ciclo.

2.1.2 Contexto Histórico

Segurança da Informação é um termo relativamente novo, como o campo e programas de graduação associados são relativamente recentes, muitos daqueles que trabalham em segurança da informação tem antecedentes ou conhecimentos em campos diferentes.

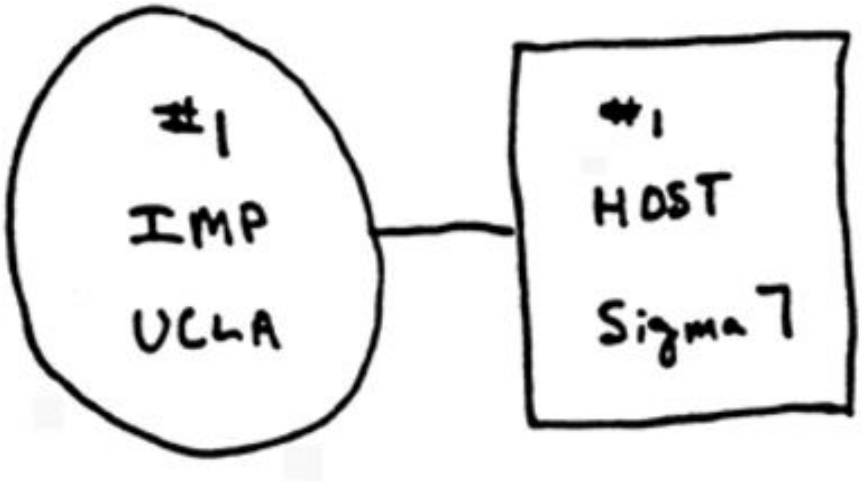
Alencar (2010) nos diz que a área de Segurança da Informação é abordada de forma multidisciplinar e trabalhada por diferentes áreas do conhecimento como a Administração, a Ciência da Computação, a Ciência da Informação, a Economia, as Engenharias, a Tecnologia da Informação, entre outras.

Vanaco (2010) nos diz que a década de 1930, engenheiros construiam circuitos eletrônicos para resolver problemas lógicos e matemáticos, mas a maioria não possuia processos com rigor teórico. Até que surgiu a tese de mestrado de Claude E. Shannon de 1937, *A Symbolic Analysis of Relay and Switching Circuits*. Shannon desenvolveu a teoria da informação no artigo de 1948 "*A Mathematical Theory of Communication"*, cujo conteúdo serve como fundamento para áreas de estudo como compressão de dados e criptografia.

As organizações começaram a proteger seus computadores na década de 1960, qualquer pessoa com conhecimento suficiente sobre como trabalhar um computador poderia invadir uma instalação e começar a acessar dados confidenciais. Várias camadas de proteção e senhas foram adicionadas aos dispositivos.

A partir deste ano, foi criada a Rede da Agência de Projetos de Pesquisa Avançada (Advanced Research Projects Agency Network - ARPANET), que ganhou popularidade como um condutor do intercâmbio eletrônico de informações e dados. A partir daí estava criado o caminho para a rede de transporte conhecida hoje como Internet (Figura 6).

Figura 6 – Diagrama dos dois primeiros nós da ARPANET



Fonte: Computer History Museum - http://www.computerhistory.org/

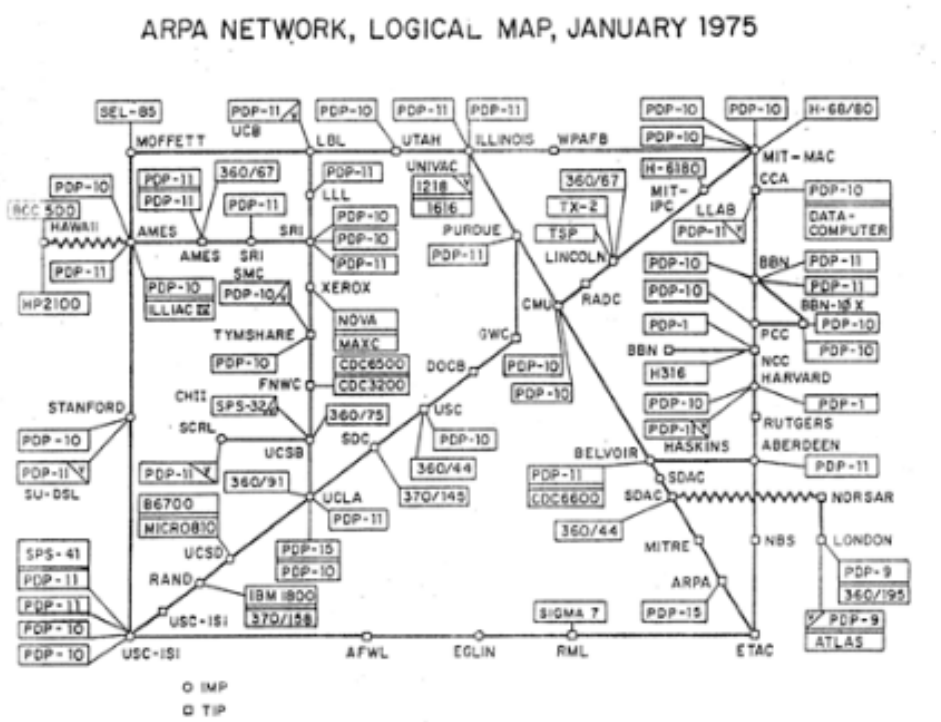
Em 1970, quatro universidades seriam conectadas na rede ARPANET. Eram a UCLA, Universidade da Califórnia em Los Angeles (centro do desenvolvimento do "software"), o Stanford Research Institute, a Universidade da Califórnia em Santa Bárbara e a Universidade de Utah, todos beneficiários de contratos com a ARPA.

Na UCLA, o primeiro site, Vint Cerf, Steve Crocker e Jon Postel trabalham com o Prof. Leonard Kleinrock. Em 7 de abril, Crocker envia um memo intitulado "*Request for Comments*". Este é o primeiro de milhares de RFCs que documentam a arquitetura da ARPANET e da Internet.

Na UCLA, o primeiro site, Vint Cerf, Steve Crocker e Jon Postel trabalham com o Prof. Leonard Kleinrock. Em 7 de abril, Crocker envia um memo intitulado "*Request for Comments*". Este é o primeiro de milhares de RFCs que documentam a arquitetura da ARPANET e da Internet.

Em 1975 o mapa geográfico da ARPANET mostra 61 nós (Figura 7). O departamento nacional de energia (DOE) cria sua própria rede para suportar sua própria pesquisa . Esta rede opera com linhas dedicadas, cada site conectado ao computador central nos Laboratórios Nacionais do DOE. A NASA inicia o planejamento de sua própria rede, a SPAN, que tem conexão com a ARPANET.

Figura 7 – Mapa da ARPANET em 1975



Fonte: Computer History Museum - http://www.computerhistory.org/internethistory/1970s/

O recentemente desenvolvido, protocolo TCP, começa a ser posto em prática. Internamente as novas redes usam uma variedade de protocolos que tornam a interoperabilidade ainda um problema.

Symantec (2009, tradução nossa) nos diz que a exploração da tecnologia de telecomunicações marcou os anos, a partir de 1970, como um período de tempo na história da Segurança da Informação em grande parte intocada pela calamidade digital.Os primeiros hackers apareceram tentando burlar o sistema e fazer telefonemas

gratuitos, uma prática que ficou conhecida como *phone phreaking.*

De acordo com Lynett (2015), a computação em rede estava em sua infância (a internet como a conhecemos hoje não existiria até o final dos anos 1980s). No entanto, embora não houvesse uma rede global maciça conectando todos os dispositivos que desejassem ser conectados, grandes organizações, especialmente os governos, estavam começando a ligar computadores via linhas telefônicas. Reconhecendo isso, as pessoas começaram a procurar maneiras de se infiltrar nas linhas telefônicas conectadas aos computadores, para que pudessem roubar dados. Essas pessoas se tornaram os primeiros grupos de hackers.

Na década de 1980, surgiram várias formas de softwares maliciosos. Os negócios das organizações possuiam a informática como retaguarda, o sigilo dos dados era o principal enfoque, fazia parte da administração e da estratégia da organização. A pirataria tornou-se crime internacional. Vírus de computadores que passavam de computador para computador através de dispositivos infectados configuravam ameaças à integridade e operação de *softwares* e sistemas. Na mesma época surgiram os clubes de computadores. A década de 1980 inaugurou a era do malware, marcando o primeiro vírus, chamado *Brain,* em 1986, bem como o conhecido *Worm*, do estudante Robert Morris, em 1988.

Um pequeno grupo de adolescentes de Milwaukee, conhecido como “414s”, invadiu mais de 60 sistemas de computadores militares e corporativos e roubou mais de US $ 70 milhões de bancos dos EUA e, em resposta a esta crise de Segurança da Informação, os governos começaram a perseguir ativamente os *hackers*.

A década de 1990 trouxe o início da moderna indústria da Segurança da Informação. Como nos ensina Nakamura e Geus (2007), o crescimento das redes baseadas em *Internet Protocol* (IP) fez com que o foco fosse mudado para disponibilidade. Durante essa década surgiram ameaças como vírus Michelangelo, Melissa, e *Concept*. Também nasceram ataques distribuídos de negação de serviço e os bots que os tornaram possíveis, como *Trin00*, *Tribal Flood* e *Stacheldracht*.

A primeira década do século XXI viu a atividade maliciosa da Internet se transformar em uma grande empresa criminosa voltada para o ganho monetário.Grandes ameaças de nome, como *Code Red, Nimda, Welchia, Slammer* e *Conficker* todos começaram a tirar proveito de máquinas sem *patches* de segurança - alteração aplicada a um recurso para corrigir a que dá origem a uma vulnerabilidade.

Atualmente os crimes de computador que incluem sofisticados ataques de negação de serviço, roubo de identidade,novas categorias de softwares como malwares e trojans tem aumentado consideravelmente o problema.

De acordo com, com o advento da Internet e com a ubiquidade de seu uso e

com o crescimento de navegadores da *World Wide Web (WWW)* do início até meados de 1990, outras ameaças foram alimentadas tais como disseminação de softwares maliciosos de propagação em rede, virus polimórficos,ciberterrorismo e outras formas de crimes de computador. Essas ameaças, em paralelo, aprimoraram a segurança de informação criando áreas de estudo com departamentos de ciências da computação em universidades, aumento de despesas com aquisições governamentais e particulares, além da rápida expansão da indústria de softwares.

2.1.3 Princípios da Segurança da Informação

Pode-se definir Segurança da Informação como a “Área do conhecimento dedicada à proteção de ativos de informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

A norma NBR ISO 27002 define da seguinte forma: “Segurança da informação é 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”.

Para Cooper (2009), Segurança da Informação é a prática em garantir que as informações possam estar seguras contra os acessos não autorizados. Tais acessos podem alterar as informações de um determinado ativo, impedindo que organizações alcancem seus objetivos, uma vez que dados foram violados por acessos indevidos.

Tradicionalmente, a Segurança da Informação (SI) é definida nos termos de Confidencialidade, Integridade e Disponibilidade. E que é definida por National Institute of Standards and Technology-NIST (1995 apud STALLINGS, 2008) como:

> a proteção oferecida para um sistema de informação automatizado a fim de alcançar os objetivos de preservar a integridade, a disponibilidade e a confidencialidade dos recursos do sistema de informação (incluindo hardware, software, firmware, informações/dados e telecomunicações).

Esses três conceitos formam os pilares fundamentais da segurança tanto para dados como para serviços de informação e computação. O NIST - National Institute of Standards and Technologies - listam a confidencialidade, integridade e disponibilidade como os três objetivos de segurança para informação e sistemas de informação.

Alguns conceitos adicionais devem ser considerados para que o quadro esteja mais completo. Dois desses conceitos que são mais comumente mencionados são :

Autenticidade: a propriedade de ser genuíno e capaz de ser verificado e confiável; confiança na validação de uma transmissão, em uma mensagem ou na origem de uma mensagem. Isso significa verificar que os usuários são quem dizem ser e, além disso, que cada entrada no sistema vem de uma fonte confiável.

Responsabilização: a meta de segurança que gera o requisito para que ações de uma entidade sejam atribuídas exclusivamente a ela. Isso provê irretratabilidade, dissuasão, isolamento de falhas, detecção e prevenção de intrusão, além de recuperação pós-ação e ações legais.

De acordo com Goodrich e Tamassia (2013), confidencialidade é evitar a revelação não autorizada da informação, pois significa limitar o acesso somente às entidades autorizadas (pessoas, sistemas) e negar o acesso às demais.

Outro princípio é a integridade, que é a garantia de que a informação não foi alterada de maneira não autorizada. Em um sistema de computação a integridade dos dados pode ser facilmente comprometida, por isso existem várias ferramentas que suportam a integridade, tais como:

- **Cópias de Segurança**: que é o arquivamento periódico dos dados, permitindo que os mesmos possam ser restaurados caso tenham sido alterados de forma não autorizada.

- **Somas de Verificação**: uma função que transforma o conteúdo de um arquivo em um valor numérico e, caso haja alguma alteração no conteúdo deste arquivo de entrada, teremos uma mudança no valor de saída.

- **Códigos de correção de dados**: métodos para armazenar dados de forma que pequenas alterações podem ser detectadas e automaticamente corrigidas.

Todas essas ferramentas usam a redundância, a replicação de algum conteúdo de informação de modo que possamos corrigir as falhas na integridade dos dados.

Stallings (2008) nos diz que a integridade abrange dois conceitos:

- I**ntegridade de dados:** assegura que as informações e os programas sejam modificados somente de uma maneira especificada e autorizada.

- **Integridade do sistema**: assegura que um sistema execute as suas funcionalidades de forma ilesa, livre de manipulações deliberadas ou inadvertidas do sistema.

A Disponibilidade é a propriedade que permite que a informação esteja sempre disponível para o uso quando solicitada. Assegura que os sistemas operem prontamente e seus serviços não fiquem indisponíveis para usuários autorizados.

Com uma visão social e sistêmica, reconhecendo o papel do indivíduo na segurança admitindo sua estreita relação com os sistemas de informação, Marciano e Lima-Marques (2006) definem Segurança da Informação como

> um fenômeno social no qual os usuários (aí incluídos os gestores) dos sistemas de informação têm razoável conhecimento acerca do uso destes sistemas, incluindo os ônus decorrentes expressos por meio

> de regras, bem como sobre os papéis que devem desempenhar no exercício deste uso.

Muitos conceitos de SI são empregados sob o ponto de vista tecnológico, onde ferramentas são aplicados para buscar soluções muitas vezes consequentes daquela mesma tecnologia. É necessária uma compreensão mais ampla da Segurança da Informação e de seus problemas. Novos conceitos, precisam ser capazes de representar os atores e o ambiente envolvidos na Segurança da Informação.

Marciano e Lima-Marques (2006) nos mostram que existe uma via de mão dupla entre o contexto social no qual se inserem os sistemas de informação e a sua segurança: a partir do contexto social chega-se à definição dos requisitos necessários à Segurança da Informação.

A definição de Segurança da Informação que nos apresentam visa abranger todos os componentes de sua estrutura:

1) os atores do processo (os usuários);

2) o ambiente original de sua atuação (os sistemas computacionais de informação, potencializados pelos recursos tecnológicos);

3) o alcance final dessa mesma atuação (a própria sociedade, mediante o impacto causado pelas modificações introduzidas pela utilização dos sistemas de informação).

Além dos três conceitos importantes que foram vistos, existem outros que a Norma ISO 27001 preconiza e que auxilia no entendimento da dinâmica da Segurança da Informação:

a) Risco – combinação da probabilidade de um evento e de suas consequências;

b) Ativos – qualquer coisa que tenha valor para a organização;

c) Ameaças – causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

d) Vulnerabilidade – fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

e) Agentes ameaçadores – atores responsáveis pelas ameaças.

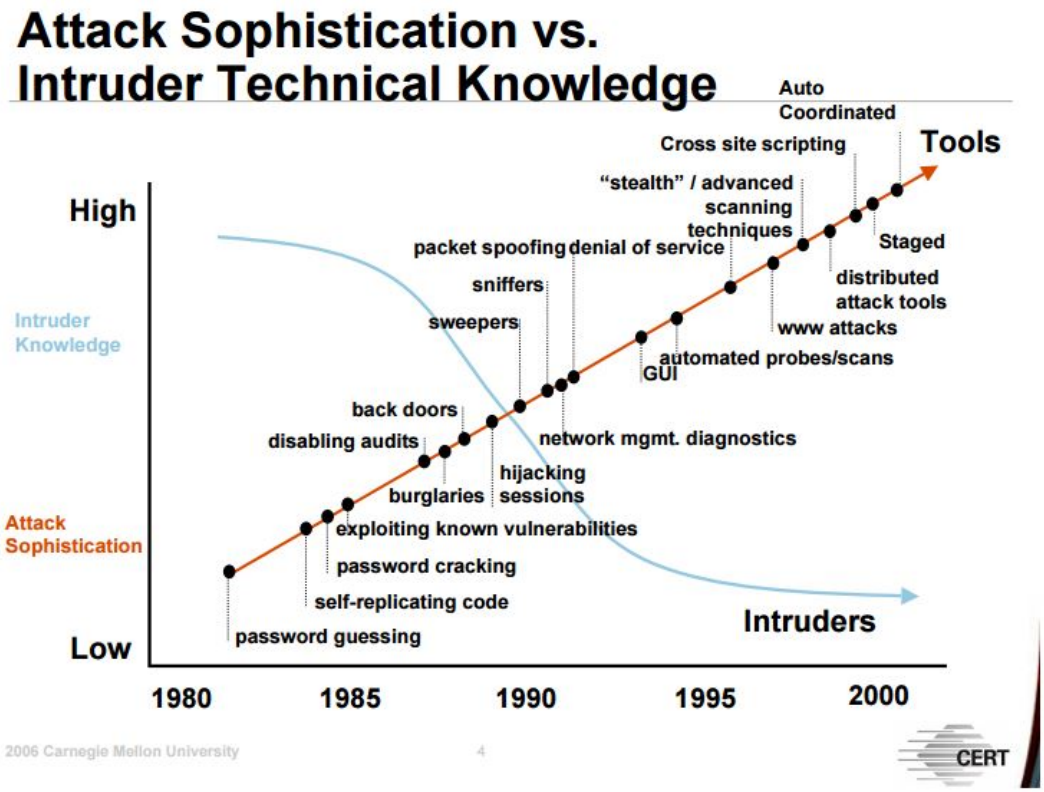
Costa e Silva (2009) nos dizem que, embora os três pilares sejam importantes, para que a SI seja sustentável, é necessária a inclusão do fator humano como um novo princípio, de igual tamanho e responsabilidade.

2.1.4 Ameaças

Com o crescimento exponencial da Internet, as Tecnologias de Informação e Comunicações estão sendo usadas também por terroristas. Mais e mais criminosos estão explorando a velocidade, conveniência e anonimato da Internet para cometer diversas atividades criminosas, sem conhecer fronteiras.

De acordo com Mandarino Júnior (2010) a complexidade dos ataques cibernéticos estão cada vez maiores, enquanto a necessidade de conhecimentos técnicos para efetuá-los vem decrescendo (Figura 8).

Figura 8 – Sofisticação de ataques x Conhecimento técnico do atacante



Fonte: CERT

Os ataques que anteriormente buscavam quebrar uma senha, necessitavam de um grande conhecimento de programação, enquanto que nos dias de hoje ferramentas que permitem ataques maciços a senhas são encontrados facilmente na web.

Novas tendências no cibercrime[1] estão surgindo o tempo todo, com custos estimados para a economia global em execução de milhares de milhões de dólares. No passado, o cibercrime costumava ser cometido por indivíduos ou pequenos grupos.

[1] O termo Cibercrime utilizado pela primeira vez por Willian Gibson, em sua obra Neuromancer (1984).

Hoje, estamos vendo redes de cibercriminosos altamente complexas reunir pessoas de todo o mundo em tempo real para cometer crimes numa escala sem precedentes.

O ciberespaço (ou espaço cibernético) é o espaço não físico criado por redes de computadores, onde as pessoas podem se comunicar de diferentes maneiras, como mensagens eletrônicas, salas de bate-papo, grupos de discussão, dentre outros.

A guerra cibernética e o hackitivistmo são termos que estão na mídia, um assunto da moda, mas não um assunto novo. O termo “cibernético” é uma evolução natural da tecnologia aplicada a um cenário de conflitos. Hoje, vários países consideram o Ciberespaço como o “quinto domínio da guerra” e a guerra cibernética é uma variação da guerra eletrônica. Todas as forças armadas, de todos os países tem desenvolvido infraestruturas para guerra eletrônica.

Percebe-se o emprego, cada vez maior, de expressões como ataque cibernético, segurança cibernética, espaço cibernético, regulamentação da Internet, direitos de privacidade, crimes cibernéticos, violação de direitos de propriedade intelectual, dentre outros, quer sejam nas mídias convencionais e digitais, quer em fóruns e eventos de governo e da academia, nacionais e internacionais. A Internet, as redes de comunicações estão na linha de frente das atenções das lideranças de vários países é a nova Sociedade da Informação e seus desafios.

Para INTERPOL (2016), o aumento do uso da tecnologia e da Internet em todos os aspectos da vida coloca cidadãos diariamente em risco, tornando-se alvos de cibercriminosos. A sociedade está confiando sempre mais na Internet e nas inúmeras opções de operações comerciais online. Tais ameaças estão presentes de diversas formas e atingem uma variedade de dispositivos tecnológicos e seus usuários.

De acordo com relatório da VERISIGN INC. (2016), os profissionais de segurança foram forçados a aceitar uma realidade em que os agressores não se interessam mais apenas em derrubar redes de grandes empresas ou roubar dados.

> A partir de 2016, as equipes de segurança também devem se proteger de ameaças puramente destrutivas e punitivas, além de proteger suas cadeias de abastecimento, canais de mídias sociais e outros elementos no ecossistema empresarial, tanto on-line como offline.

O cenário de ameaça cibernética deve ser entendido em sua complexidade, para que, assim, os criminosos cibernéticos sejam acompanhados. Esses elementos estão sempre aproveitando as falhas de segurança, as tecnologias e práticas padronizadas para obter lucro, notoriedade, ideologia ou combinações dessas três coisas. Em 2015, as ameaças cibernéticas evoluíram, e os agentes maliciosos aprimoraram suas táticas para acompanhar um terreno de ameaça cada vez maior e mais lucrativo.

Entre suas escolhas estão as novas vulnerabilidades e explorações, malware automatizado e cada vez mais discreto e ferramentas de ataque disponíveis e acessíveis. Embora os órgãos de execução da lei tenham tido algum sucesso contra os grupos de criminosos cibernéticos e suas campanhas, a prática de aproveitar os ataques cibernéticas para obter ganhos financeiros cresceu e evoluiu em 2015. Quando os criminosos cibernéticos abandonaram os canais de comunicação e coordenação, que antes eram confiáveis, e migraram para outros que oferecem mais discrição, alguns grupos tiveram sucesso ao utilizar uma prática criminosa antiga para alcançar seu objetivo: a extorsão.

Em 2015, a Verisign INC. (2016) observou que os agentes maliciosos começaram a adotar cada vez mais a *darknet*[2] como uma plataforma para atividades de crimes cibernéticos, embora várias comunidades notáveis da *darknet* estivessem chegando ao fim. Surgiram comunidades criminosas baseadas em Tor[3], embora a vida útil desses fóruns e mercados fossem menores do que a vida útil daqueles baseados na internet convencional (*Clearnet*[4]).

Os analistas da Verisign observaram que as comunidades criminosas da darknet e da clearnet apareceram em taxas alarmantes em 2015. A maioria das comunidades criminosas da *clearnet* exigia muito pouca - ou nenhuma - verificação para entrar. No entanto, essas comunidades da *clearnet* ganharam notoriedade em ritmo muito mais lento do que as comunidades da *darknet*.

A aparente camada extra de anonimato das plataformas *darknet*, como a Tor, continua atraindo agentes maliciosos, independente de sanções severas sofridas por execução de lei e vetores de ataque revelados pela comunidade de segurança. A pesquisa do iDefense sugere que esses contratempos não impediram que os agentes continuassem a oferecer produtos e serviços ilícitos na *darknet*.

Os criminosos estão cada vez mais usando a Internet para facilitar suas atividades criminosas e maximizar o seu lucro no menor tempo possível. Os crimes em si não são novos - como roubo, fraude, a venda de medicamentos falsificados - estamos evoluindo em linha com as oportunidades *online*, sempre mais difundidas.

Para a Verisign, os mercados da *darknet* sempre atrairão usuários de forma muito mais rápida do que aqueles que residem na *clearnet*. No entanto, devido à migração rápida e constante de criminosos cibernéticos para a *darknet*, essas comuni-

[2] Darknet é uma rede que só pode ser acessada com um software específico, configurações, ou autorização, muitas vezes utilizando protocolos e portas de comunicação não-padrão.

[3] TOR é uma rede aberta que ajuda a defender contra análise de tráfego ou monitoramento de rede que ameaça a liberdade e privacidade, negócios confidenciais e relacionamentos,além da segurança do Estado. https://torproject.org

[4] *Clearnet* é um termo usado por usuários da web oculta (como Tor, I2P, Freenet) para descrever a internet regular.

dades atrairão muita atenção indesejada dos órgãos de execução da lei, pesquisadores de segurança e da imprensa. Como resultado, a vida útil dos mercados de *darknet* diminuirá, o que contribuirá para um aumento das comunidades de menor duração.

2.2 Engenharia Social

Este capítulo apresenta o referencial teórico que aborda aspectos conceituais de engenharia social, estratégias e recursos empregados nesse tipo de ataque.

Dentre as várias definições para o termo, o ponto comum entre todas as interpretações é que a engenharia social envolve métodos que pretendem controlar o comportamento humano como um meio para a concretização de um objetivo que, muitas vezes, só é atingido depois da aplicação de diferentes técnicas.

A engenharia social é um dos principais desafios da segurança. Com a dificuldade, cada vez maior, para os atacantes ultrapassarem as barreiras tecnológicas, o ser humano tornou-se o principal alvo de ataques (SILVA, 2013).

2.2.1 Conceitos

Influenciar pessoas a divulgar informações sigilosas é uma atividade conhecida como engenharia social e o processo em si é conhecido com ataque de engenharia social. Existem várias definições e um número variado de tipos de ataques de engenharia social. Muitos pesquisadores em todo o mundo tentam conceituar engenharia social (ES) de acordo com suas crenças e opiniões.

Chantler e Broadhurst (2006) em seu artigo *Social Engineering and Crime Prevention in Cyberspace,* conceitua engenharia social como “o uso de armadilhas psicológicas, manipulação do comportamento através de farsas por Cybercriminosos em usuários desavisados para obter acesso a informações.”

A engenharia social é “o ato de obter acesso não autorizado a um sistema ou informações sensíveis, como senhas, através do uso de confiança e construção de relacionamento com aqueles que têm acesso a essas informações” (CHITREY; SINGH; SINGH, 2012 apud KUMAR; CHAUDHARY; KUMAR, 2015).

Com base em Mitnick e Simon (2003), engenharia social é um conjunto de práticas utilizadas para a obtenção de informações relevantes ou sigilosas de uma organização ou indivíduo, por meio da persuasão, manipulação e influência das pessoas, seja com o uso ou não da tecnologia.

Aproveitando-se dos aspectos psicológicos da mente humana e dos padrões de interação social entre as pessoas, faz com que as pessoas cumpram seus desejos. Os aspectos de interação humana, padrões de comportamento humano e estrutura

social criam um estado de confiança com a vítima, tornando assim mais fácil reunir informações ou fazer a vítima executar alguma ação involuntária“ (HEIKKINEN, 2010).

Diante do exposto, pode-se conceituar a engenharia social como a arte de obter informações ou vantagens através de armadilhas psicológicas, persuasão ou qualquer técnica que explore a fraqueza do elemento humano.

A engenharia social envolve a exploração do senso comum das pessoas para adquirir informações vitais ou críticas de uma organização (como senhas, logins, informações corporativas) através de funcionários incautos. Esta técnica é geralmente utilizada por hackers em situações nas quais os meios técnicos não foram suficientes para penetrar em um sistema de destino.

Segundo Hadnagy (2011):

> ”engenharia social é a arte ou, melhor ainda, a ciência, de habilidosamente manobrar seres humanos a realizar ações em algum aspecto de suas vidas“.

Compreende-se que a engenharia social pode ser usada por qualquer pessoa no dia-a-dia. O autor argumenta que pode ser utilizada na maneira em que professores interagem com seus alunos, na forma em que médicos, advogados ou psicólogos obtêm informações de seus pacientes e clientes, entre outras situações.

O autor apresenta um conceito que aborda a engenharia social sob um enfoque psicológico e sob a ótica da Segurança da Informação. Por ter um papel fundamental em relação a processos e tecnologias, o elemento humano é um aspecto crítico na Segurança da Informação.

Conforme Mann (2008), a segurança humana é a conexão que falta entre segurança de TI e segurança física. O maior risco para a Segurança da Informação em uma organização não está relacionado à tecnologia, mas sim na omissão ou ação de funcionários da organização que, consequentemente, leva a incidentes de segurança.

> ”A engenharia social não está morrendo. Na realidade, a maioria dos ataques bem sucedidos em agências governamentais e empresas, hoje, tem na engenharia social um importante componente. Em toda avaliação de segurança em engenharia social até hoje, fomos 100% bem sucedidos. Então a pergunta é: somos realmente bons, ou as empresas ignoram a ameaça do fator humano¿‘ - Kevin Mitnick[5]

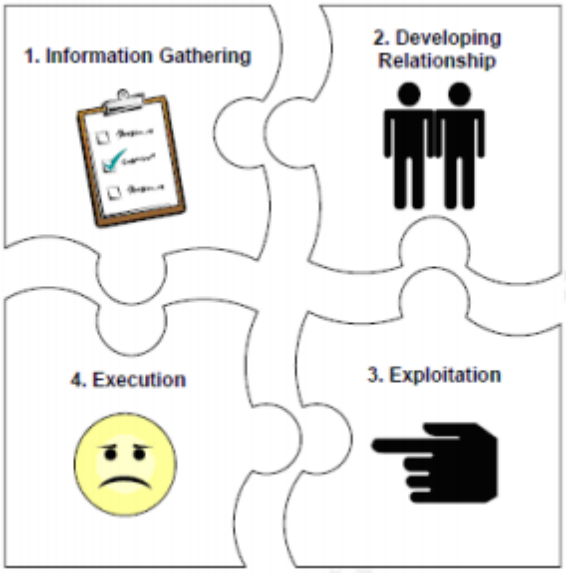
2.2.2 Estratégias de ataque de engenharia social

[5] Kevin Mitnick em resposta a fã, durante entrevista ao canal Gizmodo US. http://gizmodo.com/5925114/kevin-mitnick-the-worlds-most-notorious-hacker-is-here-to-talk-about-what-got-him-started#replies

Existe um vasto número de ataques de engenharia social para adquirir acesso a sistemas através da exploração de empregados desavisados.

Mitnick e Simon (2003) descreve o ”Ciclo de engenharia social“, com quatro estágios distintos que são: a obtenção de informações, o desenvolvimento de relacionamento ou confiança, a exploração da confiança e a execução objetivando a realização. Os ataques seguem um ciclo padrão, demonstrado pela figura 9:

Figura 9 – Ciclo de ataque da engenharia social



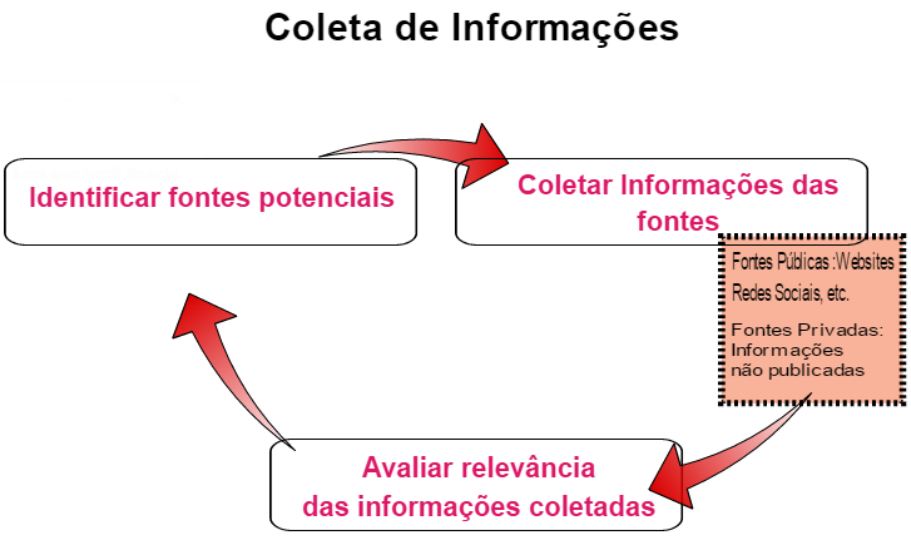
Fonte: Allen,2007

2.2.2.1 **Coleta de Informações**

A primeira etapa da coleta de informações é ”identificar as possíveis fontes“ a partir das quais a informação pode ser obtida. As fontes podem ser qualquer coisa ou qualquer pessoa com acesso às informações necessárias para o ataque**.** *Footprinting* é o processo de observar e coletar informações sobre um potencial alvo com a intenção de achar uma forma de atacar o alvo.

A fase de ”coleta de informação“ é repetida até que o engenheiro social tenha obtido informação suficiente, de modo que possa iniciar a sua preparação para o ataque. Conforme ilustrado na figura 10:

Figura 10 – Fase 1 do Ciclo de engenharia social



Fonte: Autor - Adaptado do ciclo de ataque de Engenharia Social. Mitnick (2008)

O engenheiro social visa um alvo, que pode ser uma pessoa ou uma organização e prepara-se algum tempo reunindo informações sobre o mesmo. Esta etapa pode ser realizada através de monitoramento passivo do tráfego da rede e o reconhecimento dos edifícios da organização e horários de trabalho das pessoas. O processo pode ser obtido através de várias fontes de acesso público, tais como redes sociais, páginas web, portais, entre outros.

Nesta etapa as informações são coletadas para que, em um próximo passo haja um relacionamento com a vítima. A possibilidade de sucesso para a maioria dos ataques depende dessa fase, por isso é natural investir a maior parte do tempo e da atenção aqui. A qualidade da informação que um alvo possui, define o tamanho da relação entre este e o atacante (HADNAGY, 2017a).

Princípios de influência, e outros fatores psicológicos são normalmente necessários para utilizar com êxito estes métodos. Nenhuma fonte de informação é única ou é o principal método a ser usado, nem um único método pode fornecer dados suficientes para garantir suas melhores chances de sucesso, são vários os métodos de coleta de informações utilizados. O caminho que muitos criminosos tomam, é utilizar múltiplos métodos de coleta de informações e, em seguida, a partir desses dados, definir qual o ataque adequado para o trabalho.

2.2.2.2 **Desenvolvimento de Relacionamento**

De acordo com , o desenvolvimento da relação e da confiança pode ser feito usando informação privilegiada, deturpando uma identidade, citando pessoas conhe-

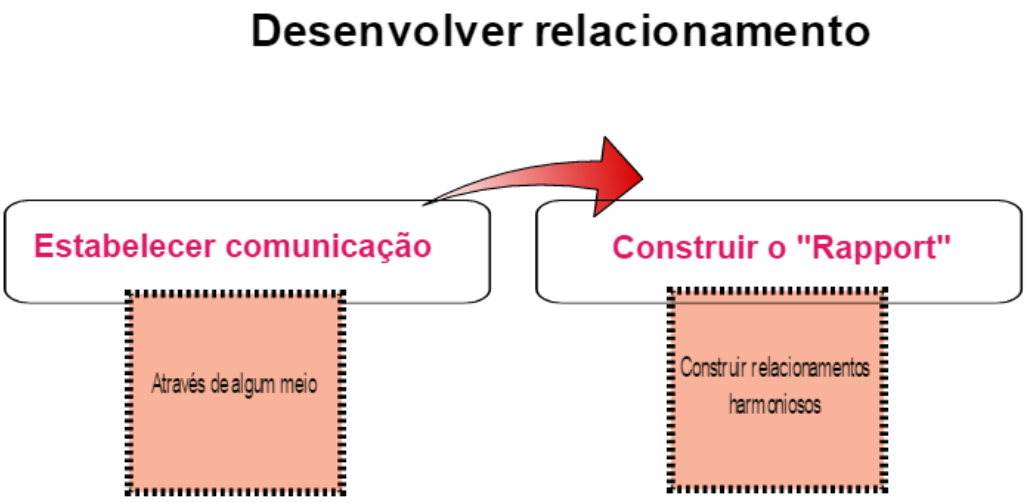
cidas da vítima, mostrando uma necessidade de assistência ou ocupando um papel de autoridade. Bem como conectar-se com a vítima em nível pessoal, por telefone ou através de fotos de família, ou algo mais extenso como manter relacionamento com o alvo através de um perfil falso em site de relacionamento on-line.

Hadnagy (2017a), nos diz que a qualidade do relacionamento entre atacante e vítima é um ponto crítico e determina o nível de cooperação e extensão em que o alvo irá ter para ajudar o atacante a realizar a meta.

Essa interação entre atacante e vítima é denominado *Rapport*, a capacidade de construir um relacionamento com alguém e incluir elementos como o gosto mútuo e conforto. O sucesso de um engenheiro social depende de desenvolver rapidamente um vínculo positivo com alguém para que a pessoa se sinta confortável compartilhando informações com ele.

Uma vez que o engenheiro social construiu um bom relacionamento com o alvo, o relacionamento pode ser explorado para obter as informações que o atacante exige deste. Conforme ilustrado na Figura 11.

Figura 11 – Fase 2 do Ciclo de engenharia social



Fonte: Autor - Adaptado do Ciclo de Engenharia Social - Mitnick(2008)

Após o atacante estabelecer a comunicação com a vítima, o próximo passo é a construção do *Rapport*. Isso implica a construção real do relacionamento e estabelecimento de confiança usando o plano planejado. Várias técnicas podem ser empregadas para estabelecer a confiança. Esta etapa pode ser demorada. Após o engenheiro social construir uma boa relação com o alvo, o relacionamento pode ser explorado para obter a informação que o engenheiro social exige.

No processo de estabelecimento de *Rapport*, o atacante habilmente procura

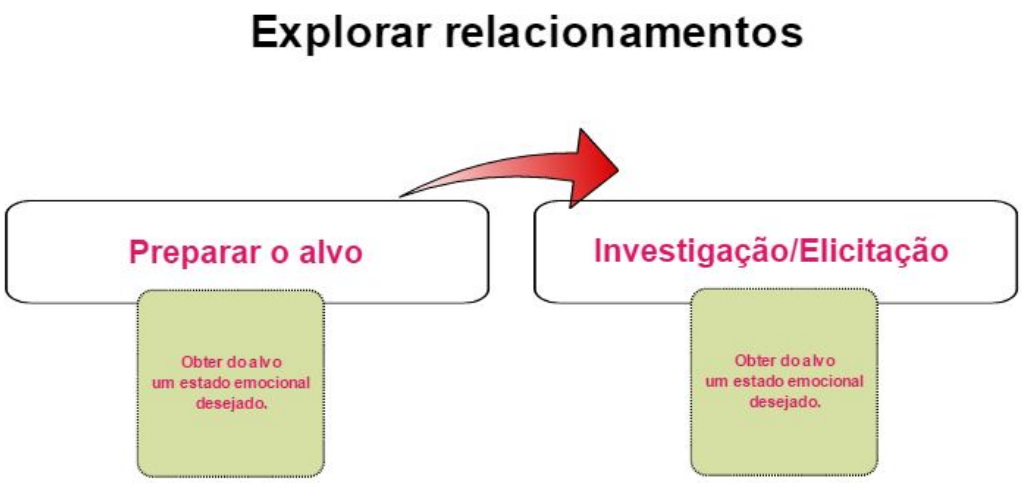
imitar, de forma sutil, os gestos do alvo, postura e demonstrar, através das estruturas principais da comunicação que está se importando com sua vítima.

2.2.2.3 **Exploração de relacionamento**

Na fase de exploração do relacionamento, o alvo pode então ser manipulado pelo atacante - supostamente confiável - para revelar informações ou executar uma ação que normalmente não ocorreria. Nesta fase o atacante está focado em manter o vínculo que foi construído na fase anterior.

Conforme ilustrado na figura 12, explorar o relacionamento consiste na preparação do alvo e investigação.

Figura 12 – Fase 3 do Ciclo de engenharia social



Fonte: Autor - Adaptado do ciclo de ataque de Engenharia Social. Mitnick (2008)

A primeira parte é para o atacante usar táticas de manipulação e sua preparação para obter do alvo um estado emocional desejado adequado ao plano, como sentir-se triste ou feliz. Ao criar uma relação com uma estória triste, por exemplo, pode-se evocar no alvo a lembrança de um incidente infeliz e, posteriormente,entristecê-lo.

Uma vez que o alvo está no estado emocional desejado, o processo de investigação ou elicitação[6], pode começar. Na conclusão dessa etapa, o engenheiro social obtém a informação necessária do alvo. Esta pode ser uma senha que é necessária para a eventual satisfação do objetivo do ataque de engenharia social Hadnagy (2017a).

A exploração é feita com várias técnicas de manipulação e, para que essas técnicas funcionem, o alvo precisa estar em um estado emocional onde a exploração

[6] ”elicitação“ é uma adaptação do inglês *Elicitation*, obtenção gradual ou dedução (ver Dicionário Inglês-Português da Porto Editora).

seja possível. Após a fase de exploração, é necessário determinar qual o estado emocional do alvo. É importante para o mesmo não perceber que estava sobre ataque.

2.2.2.4 **Execução**

Mitnick e Simon (2003) diz que a quarta fase do ataque de engenharia social consiste em usar a informação para um objetivo específico, entretanto, Mouton et al. (2014) argumenta que o uso da informação não é ataque de engenharia social. Por exemplo, se a informação é uma senha para o sistema, obter essa senha através de métodos junto a uma vítima é um ataque de engenharia social, enquanto que usar a senha para invadir o sistema não tem nenhum elemento humano e, portanto, não considera um ataque.

Bhagyavati (2008) nos diz que as técnicas utilizadas pelos engenheiros sociais podem variar dependendo de vários fatores, como o tempo de resposta necessário, o tempo de preparação necessário, as circunstâncias do ataque ou a consciência/inconsciência entre as pessoas que gerenciam os dados e a informação.

Após a finalizar a interação com o alvo, o atacante muitas vezes deseja completar essa etapa sem levantar suspeitas. Por exemplo, em um ataque de *Phishing, p*ara que o ataque seja bem-sucedido, o engenheiro social fornecerá garantias para que as vítimas não suspeitem e alterem suas senhas.

Em outras circunstâncias o engenheiro social não se preocupa em despertar suspeitas:

- Falta de rastreabilidade: quando um engenheiro social utiliza celulares pré-pagos, onde, após a conclusão de um ataque o aparelho é descartado.
- Falta de aplicação da lei, onde o engenheiro social conduz negócios a partir de locais no exterior, tornando-se difícil de rastrear e além do alcance da aplicação da lei.
- Não há ameaça de retração das informações. Algumas informações são sensíveis ao tempo (as senhas podem ser redefinidas se divulgadas), mas se a informação primária for propriedade intelectual, o alvo não poderá redefini-la assim que for divulgada.

De modo geral, não é uma boa prática finalizar um ataque de forma que o alvo questione o que acabou de acontecer. É melhor deixar o alvo com o sentimento de que fez algo de bom para alguém e que isso possibilite possíveis interações futuras. Neste momento, todos os possíveis ”rastros digitais“ são apagados, garantindo que nenhuma informação sobre o atacante seja deixada para trás. O objetivo do atacante em seu ato final é sair de forma bem planejada e sem levantar suspeitas (HADNAGY, 2017a).

2.3 Tipos de ataque

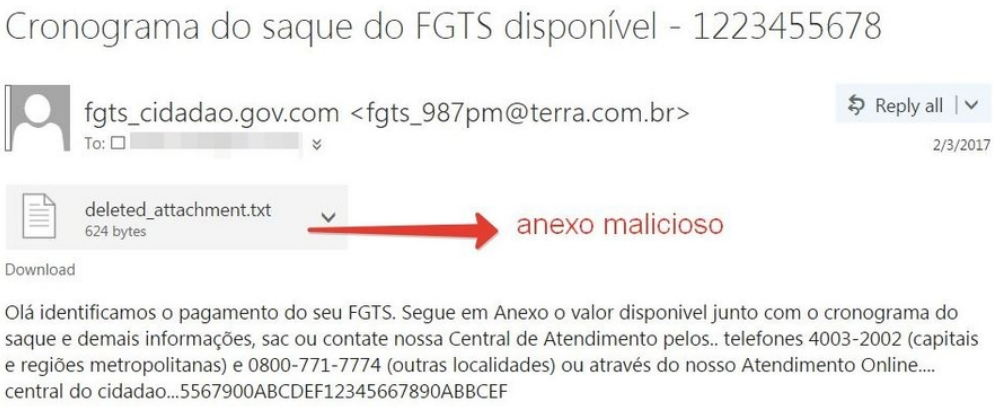
Ghafir et al. (2016) nos ensina que as técnicas de engenharia social podem ser classificadas em duas categorias: ataques baseados nas localizações físicas (ataques baseados em computador) e ataques baseados em meios psicológicos (ataque humano).

Nos ataques baseados em localizações físicas, para que o alvo envie informações ao invasor, os ataques dependem da tecnologia para manipular e enganar a vítima e permitir a execução das ações maliciosas. Os métodos mais comuns de ataques baseados em computador são:

- ***E-mails****:* As formas mais comuns de engenharia social através de E-mail são o ***phishing*** e o ***spear phishing****. Phishing* é uma exploração criada por um agente definido como *phisher*, que representa um terceiro elemento confiável para obter acesso a dados privados (GUPTA; SINGHAL; KAPOOR, 2016).

Em geral o *phisher* envia um email que parece vir de um negócio ou indivíduo legítimo solicitando a confirmação de informações. O e-mail normalmente contém um link para uma página da web fraudulenta que parece legítima, conforme figura 13.

Figura 13 – E-mail com anexo malicioso.



Fonte: @assolini (2017)

Emails podem conter anexos que incluem código malicioso. Esses anexos podem incluir *keyloggers* [7] para capturar senhas de usuários, vírus, trojans ou worms. Às vezes janelas pop-up também podem ser usadas em ataques de engenharia social, onde anunciam ofertas especiais podem tentar os usuários a instalarem software mal-intencionado inadvertidamente.

[7] Programa de computador do tipo spyware cuja finalidade é registrar tudo o que é digitado, quase sempre a fim de capturar senhas, números de cartão de crédito e afins.

O *spear phishing*, segundo definição do Kaspersky Lab[8]:

> é um golpe de e-mail direcionado com o objetivo único de obter acesso não autorizado aos dados sigilosos. Diferente dos golpes de phishing, que realizam ataques amplos e dispersos, o spear phishing foca em um grupo ou organização específicos. A intenção é roubar propriedade intelectual, dados financeiros, segredos comerciais ou militares e outros dados confidenciais.

No s*pear phishing* as tentativas de ataque não são iniciadas de forma aleatória por hackers, são mais prováveis de serem conduzidas por interessados em ganhos financeiros, segredos comerciais ou informações militares. É uma tentativa de fraude por e-mail que visa uma organização específica, buscando acesso não autorizado a dados confidenciais (ROUSE, 2011).

Um exemplo de *spear phishing* que envolveu a unidade de segurança RSA[9], pertencente à empresa de armazenamento de dados EMC Corp. mostra como até mesmo uma empresa conhecida pela segurança no ramo cibernético pode ser alvo e vítima de um ataque. No ano de 2011, a RSA foi atacada usando um objeto *flash*[10] inserido em uma planilha eletrônica anexada em um e-mail com o assunto: ”Plano de Recrutamento 2011“. Embora filtrado e encaminhado para o lixo eletrônico dos usuários, o e-mail foi recuperado e, uma vez aberto, um backdoor foi instalado através de uma vulnerabilidade no Adobe Flash.

A atividade de *phishing* colheu credenciais causando preocupação para a EMC Corp. e ameaçando a segurança de importantes empresas contratantes de seus serviços, como Northrop Grumman, Lockheed Martin, e L-3 Communications[11](INSTITUTE, 2016).

- **Baiting:** Usa alguma mídia física (*pendrive*, CD, DVD, etc.)e depende da curiosidade da vítima.Neste tipo de ataque, o atacante deixa a mídia infectada por algum malware[12] em um local fácil de ser encontrado (banheiro, elevador, es-

[8] http://brazil.kaspersky.com/internet-security-center/definitions/spear-phishing.Acesso em: 30/01/2017

[9] RSA Data Security é uma empresa americana que foi comprada pela EMC Corporation em 2012. Sediada em Bedford, Massachusetts, mantém escritórios na Irlanda, Reino Unido, Singapura e Japão. https://www.rsa.com/en-us

[10] Tecnologia desenvolvida pela empresa Adobe usada para a produção de animações, jogos de navegador, aplicativos de Internet, aplicativos de desktop, aplicativos móveis e jogos para celular.

[11] A Northrop Grumman Corporation é uma multinacional norte-americana que atua no ramo da indústria aeroespacial e defesa. A Lockheed Martin é uma empresa fabricante de produtos aeroespaciais e a L-3 Communications fabrica equipamentos de ”Controle e Comando“, Comunicações, Inteligência, Monitoramento, sistemas de reconhecimento, aviônica, além de instrumentação e produtos oceânicos e aeroespaciais.

[12] Termo do inglês ”*malicious software*“ (software nocivo ou software malicioso), é um software destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações.

tacionamento, etc), dá a essa mídia uma aparência de legítima - atribuindo um título ”atraente“ - e aguarda a vítima que a encontrar, usar o dispositivo. O simples fato de inserir o dispositivo no computador para ver o conteúdo, já instalaria o *malware* dando ao invasor acesso ao computador pessoal e, provavelmente, à rede interna da empresa alvo.

Um desses ataques foi documentado por Steve Stasiukonis - fundador da *Secure Network Technologies,Inc.* - em 2006, situação em que, juntamente com sua equipe, Steve dispersou vários *pendrives* infectados com um vírus Trojan, próximos ao estacionamento da organização. Muitos dos funcionários que acharam os *pendrives* e os conectaram em seus computadores, ativaram um *keylogger* [13]que lhe deu acesso a uma série de credenciais de logins de funcionários (JOHANSON, 2008 apud ALEXANDER, 2016).

- ***Websites*:** ataques de engenharia social muitas vezes utilizam sites maliciosos como um canal de ataque. Este modo de ataque é baseado em várias plataformas, tais como plataformas de mensagens instantâneas on-line, mídias sociais, páginas falsas e possui diversos modos de implementação.

Através de um site falso um atacante deseja que um alvo instale programas maliciosos em sua máquina, como *worms*[14] ou vírus.O atacante pode também obter informações através da realização de pesquisas na web relacionadas com informações da empresa em casos onde as organizações colocam informações detalhadas em seus sites, incluindo serviços, produtos, detalhes de pessoal, entre outros que seriam utilizados na aquisição de alvo.

Outro método é através do uso de *curriculum vitae on-line* através do qual fornecem informações pessoais detalhadas relacionadas ao local de trabalho de um alvo e classificação organizacional a ser usado na fase de aquisição do alvo

De acordo com último relatório da Mcafee[15], o terceiro trimestre de 2016 apontou mais de 15 milhões de URLs suspeitas. Conforme figura 14.

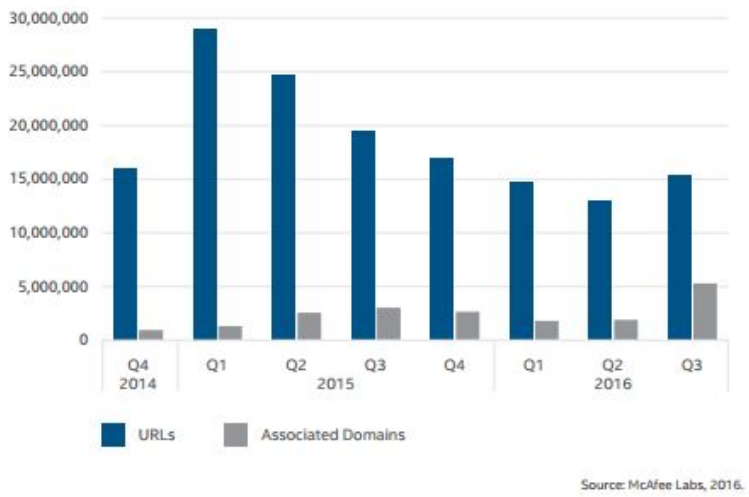
---

[13] Keylogger é um programa de computador do tipo spyware cuja finalidade é registrar tudo o que é digitado, quase sempre a fim de capturar senhas, números de cartão de crédito e afins.

[14] Os worms de computador são programas semelhantes aos vírus ,que replicam cópias funcionais de si mesmos e podem causar o mesmo tipo de dano.

[15] https://www.mcafee.com/uk/resources/reports/rp-quarterly-threats-dec-2016.pdf. Acesso em: 30/01/2017

Figura 14 – Número de URLs suspeitas entre os anos de 2015 e 2016



Fonte: Mcafee (2016)

- **Telefone:** Em muitas vezes o atacante simula uma situação onde se faz passar por alguém da confiança da vítima, solicitando auxílio financeiro ou induzindo a vítima através de uma situação simulada.Mensagens de texto também são usadas como instrumentos de ataques.Neste tipo de ataque, os fraudadores direcionam as vítimas para seguir um link ou chamar um número para atualizar uma conta ou corrigir um suposto problema. Deve-se desconfiar de mensagens que indicam um problema ou perguntam sobre suas contas financeiras.
- **Abordagem Pessoal:** Neste ataque um empregado pode ser abordado e enganado / coagido a fornecer informações ao atacante.
- **Serviço Postal**: É uma das formas menos frequentes de ataques de engenharia social mas há relatos de que os alvos são solicitados a inserir dados pessoais em um formulário e devolvê-lo para reivindicar seu prêmio.

Nos ataques baseados em interação humana, o atacante utiliza diferentes técnicas de contato para obter a informação desejada. Os métodos mais populares são:

- ***Pretexting*** / **Representação**: É o ato de criar um cenário de forma a conseguir com que a vítima forneça a informação ou execute uma determinada ação, consiste na personificação de alguém com autoridade legítima como via de estabelecimento de confiança. Nesse tipo de ataque o engenheiro social passa-se por um empregado ou um usuário válido do sistema. O atacante pode obter acesso se passando por um zelador, um empregado ou um contratante. (HADNAGY, 2017b)

O Engenheiro Social ao longo de sua vida cria vários papéis, tais como fazer-se passar por alguém importante ou um gerente de alta patente, que teria acesso aos arquivos ou sistemas de computador. Na maioria das vezes, os empregados não questionam alguém que se apresenta nessa posição.

Passar-se por um terceirizado, onde, neste ataque, o atacante finge ter permissão de uma pessoa autorizada para usar o sistema de computador. Ele funciona quando a pessoa autorizada não está disponível por algum tempo.

Criar uma nova identidade e depois utilizar essa identidade para manipular o alvo , é mais do que apenas criar uma mentira, é personificar papéis e trabalhos nunca feitos antes. O *Pretexting* também não possui um tamanho único para todas as soluções (HADNAGY, 2017b).

A seguir alguns exemplos de *Pretexting:*

1) usando Similaridade**:** Um atacante pode, através de uma simples conversa, desenvolver conexões interpessoais com seu alvo. Através de uma conversa casual, o atacante pode obter influência sobre um alvo que estaja destinado a desenvolver conexões. De acordo com Ghafir et al. (2016), existe uma tendência natural dos seres humanos a associarem com indivíduos de interesses ou origens semelhantes.

2) usando Compromisso: Os atacantes também exploram a natureza dos funcionários de quererem ser vistos como confiáveis e comprometidos para executarem seus ataques. Por exemplo, um atacante instrui um funcionário a executar uma determinada tarefa e o avisa de terríveis conseqüências caso a ordem seja descumprida. Esse ataque pode ser efetuado instruindo um novo funcionário a implementar certas políticas de segurança e, durante o processo, exigir que o alvo compartilhe suas credenciais com o objetivo de garantir o cumprimento da tarefa, obtendo assim o acesso desejado.

O fato de que as agências governamentais e as empresas de segurança estão no centro dos ataques de phishing de grande proporção é a prova de que, independentemente da magnitude das soluções de segurança técnica empregadas, as ações de até mesmo um usuário inconsciente podem ser potencialmente perturbadoras. A postura de segurança integrada de hoje não é suficiente para superar essa ameaça. Soluções técnicas só podem ajudar na tentativa de identificar e-mails mal-intencionados, mas somente o treinamento adequado pode ajudar - embora não impeça - os usuários de serem vítimas de esquemas de engenharia social ou e-mails ilegítimos (INSTITUTE, 2016).

- **Tailgating:** Esse tipo de ataque envolve um indivíduo não autorizado que segue um funcionário autorizado em uma área restrita. Personificando um mensageiro ou entregador, o atacante espera fora do edifício. O ser humano tem uma tendência natural para ajudar aqueles que precisam de alguma ajuda. Isso é muito bem aproveitado por engenheiros sociais. O atacante faz-se passar por um entregador com muitas caixas na mão e obtém acesso a um prédio enquanto um funcionário decide ajudá-lo mantendo a porta aberta.

Esse método de ataque não funciona em todas as configurações cooperativas, como em empresas que possuem controle de acesso e as pessoas que entram no edifício são obrigadas a usar um cartão (ALEXANDER, 2016).

- **Quid pro quo:** Termo do Latim, que significa ‘uma coisa por outra’. Um ataque Quid pro quo acontece quando o atacante oferece um benefício em troca de acesso ou informações. É uma técnica que deriva do *Bating* , a diferença é que no ataque Quid pro quo, o atacante promete um serviço ou benefício baseado em uma ação.

Um exemplo deste ataque ocorre quando o atacante faz-se passar por um técnico de TI e, através de diversas chamadas telefônicas, contata funcionários da empresa oferecendo-lhes uma ”atualização“ do sistema, quando na verdade está permitindo o acesso do atacante à seu sistema. Esse tipo de ataque dificilmente funciona em empresas menores, onde os funcionários de TI são conhecidos por todos da organização (VAULT, 2017).

- **Dumpster Diving:** Esse ataque caracteriza-se pela exploração do lixo que empregados desavisados jogam fora, que podem incluir dados de cartão de crédito, faturas com informações pessoais, lista de telefones da empresa, gráficos que fornecem números e locais que facilitam a representação de membros da equipe gerencial. É a verificação do lixo físico de alguma localidade visando a busca de informações que possam facilitar ataques por agentes maliciosos.

A falta de preocupação com o lixo não só pode causar uma invasão bem sucedida, como também ocultar os rastros do atacante, pois dessa forma, ninguém saberá de que forma a informação foi obtida.

O atacante pode ser um funcionário descontente e explorar essa insatisfação é simples. Um administrador de sistemas insatisfeito, pode possuir uma rede de contatos de outras pessoas que ainda trabalham na empresa, com os quais ele ainda pode coletar importantes informações, tais como códigos de acesso e informações da alta administração (LINS, 2016).

2.4 Motivação

Segundo Allen (2007) uma variedade de motivações existem e motivam um ataque de engenharia social, entre elas:

- **Ganhos financeiros**: por várias razões o indivíduo pode tornar-se fascinado por ganhos monetários. Por exemplo, ele pode acreditar que ganha menos do que merece.
- I**nteresse próprio**: o indivíduo pode querer obter vantagens em benefício próprio, como por exemplo, modificar informações associadas a algum membro da família ou a si mesmo.
- **Vingança**: Por razões apenas conhecidas ao próprio indivíduo ele pode definir um alvo como sendo um amigo,uma organização ou até mesmo um estranho, apenas para satisfazer o desejo de vingança.
- **Pressão Externa:** O indivíduo pode receber pressão de amigos, familia ou crime organizado, por razões como ganhos financeiros, vingança, e/ou pressão externa.

De um modo geral, observa-se um conjunto de características que influenciam um indivíduo para ser alvo de práticas de engenharia social (MITNICK; SIMON, 2003):

- Poder e autoridade: os indivíduos dificilmente questionam a autoridade de outros que se fazem passar por seus superiores;
- Tendência para querer agradar e ser útil: na expectativa de posteriormente ser recompensado, face a uma pretensa figura de autoridade, a reação mais usual é a de tentar ser afável;
- Ligação e similaridade: colocar-se na posição do outro permite criar um ambiente de empatia que é favorável à troca de informação. *Hobbies,* gostos em comum ou apenas o acesso ao nome do interlocutor são suficientes para o atacante estabelecer uma ligação com este;
- Reciprocidade: busca de benefícios futuros com base no favor prestado. É uma ferramenta muito útil ao engenheiro social;
- Envolvimento e consistência: um ataque é planejado com paciência e premeditação, de modo que o engenheiro social ambientar-se-á com o cotidiano da organização e daqueles que pretende abordar.

2.5 Panorama Mundial

De acordo com Kroll (2016), em seu relatório Global Fraud & Risk Report 2016, 82% afirmaram que suas companhias sofreram algum tipo de fraude – em 2015 eram 75%, e em 2013 o percentual era de 70%. O cenário é ainda pior considerando-se ameaças cibernéticas: 85% dos respondentes disseram ter sofrido incidentes desse tipo.

O relatório aponta que as fraudes e incidentes foram causados, em boa parte, por atacantes posicionados dentro das companhias; entre os colaboradores ouvidos, 60% afirma ter identificado funcionários, ex-funcionários e prestadores de serviços entre os atacantes, com 49% dos ataques sendo perpetrados por uma combinação dos três grupos.

> Entre os incidentes mais citados estão a infecção por vírus e worms, mencionada por 33% dos respondentes, ataques de phishing por 26% e para 23%, incidentes como o vazamento de dados causaram a perda de informações de clientes ou colaboradores e 22% afirmaram ter dados perdidos ou corrompidos por malware.Kroll (2016)

A engenharia social foi identificada como um elemento-chave na última invasão no Departamento de Justiça dos EUA em que hackers alegaram ter exposto os detalhes de contato de mais de 9.000 funcionários do Departamento de Segurança Interna e mais de 22.000 funcionários do FBI. Mais de 70% dos quase 500 especialistas em segurança de TI consultados pela empresa de tecnologia de segurança européia Balabit[16] consideraram as ameaças internas de mais alto risco.Ashford (2016)

Pesquisa da mesma empresa informa que mais da metade dos respondentes disseram que as organizações ainda têm medo de hackers invadirem sua rede de TI por meio de seu firewall, mas ao mesmo tempo mais de 40% deles disseram que as ferramentas de defesa de primeira linha, como firewalls não são efetivas o bastante para mantê-los longe.

Conforme o relatório, a facilidade de criar contas de mídia social fraudulentas para marcas conhecidas impulsiona uma clara preferência por phishing em ataques baseados em mídia social. Pesquisadores da Proofpoint[17] descobriram que 40% das contas do Facebook e 20% das contas do Twitter alegando representar uma marca global, 100 não são autorizadas.

Os atacantes cada vez mais envolveram pessoas em suas artimanhas, infectando sistemas, roubando dados e transferindo dinheiro usando a engenharia social

[16] https://www.balabit.com
[17] Disponível em: https://www.proofpoint.com. Acesso em 01/02/2017

para enganar pessoas onde antes dependiam de equipamentos, tecnologia e códigos maliciosos.

Conforme o relatório Proofpoint (2016), os atacantes cronometraram campanhas de e-mail e de mídia social para se alinharem com os momentos em que as pessoas estão mais envolvidas. Os atacantes usaram ameaças de mídia social e aplicativos móveis, e não apenas e-mails, para enganar os usuários a infectar seus próprios sistemas.

Um em cada cinco cliques em URLs mal-intencionadas ocorrem em mídias sociais e dispositivos móveis. Aplicativos móveis maliciosos são ameaças reais. Uma análise feita em lojas de aplicativos Android autorizadas descobriu mais de 12.000 aplicativos móveis maliciosos - capazes de roubar informações, criar backdoors e outras funções - respondendo por mais de 2 bilhões de downloads.

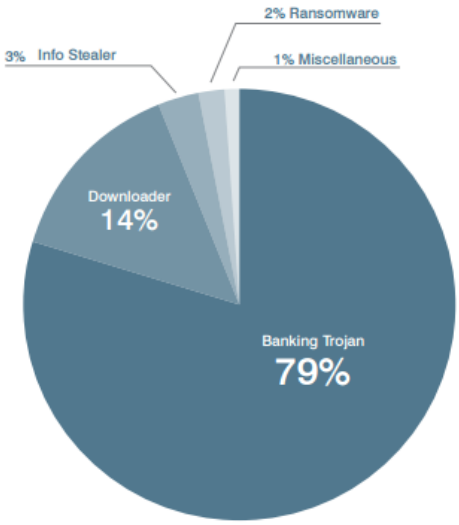
Cerca de 40% de grandes empresas amostradas pelos pesquisadores responsáveis pelo relatório citado, possuiam aplicativos maliciosos que podem roubar informações pessoais, senhas e dados.

Campanhas de e-mails de phishing estão altamente direcionadas, concentram-se em uma ou duas pessoas dentro de uma organização para transferir fundos diretamente para atacantes. As mensagens de phishing são direcionadas a pessoas com acesso a transferências bancárias e atingem organizações de todos os tamanhos. Os e-mails possuem remetentes falsificados para que eles pareçam ser do Diretor Executivo ou outro executivo com forte poder de decisão dentro da empresa, raramente têm links ou anexos e incluem instruções urgentes ao destinatário para transferir fundos para uma conta designada.

O relatório *The Human Factor 2016 Report*[18] nos diz que em 2015, os trojans bancários eram o tipo mais popular de anexos de documentos maliciosos, vide figura 15:

[18] Disponível em : https://www.proofpoint.com/sites/default/files/human-factor-report-2016.pdf. Acesso em 04/02/2017

Figura 15 – Malwares mais frequentemente entregues por anexo de documento



Fonte: The Human Factor 2016 Report

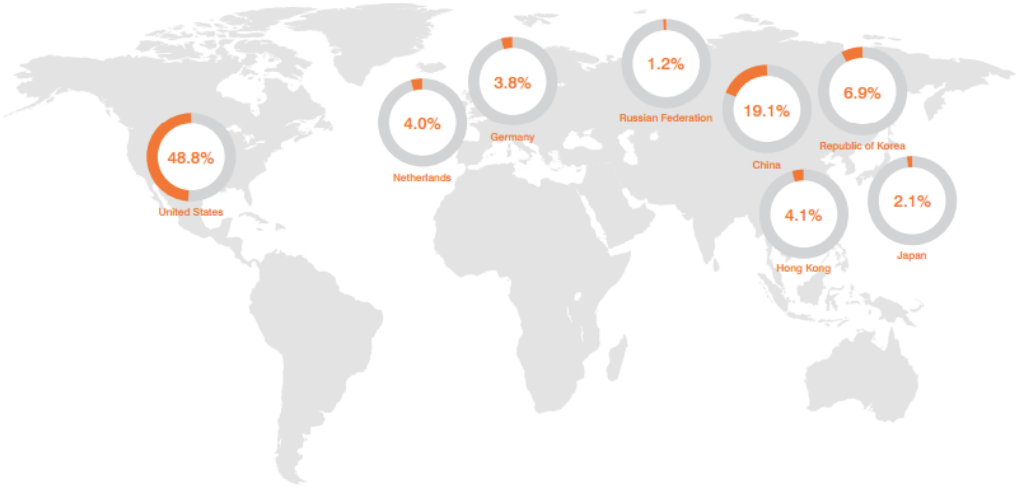
Eles representavam 79% de todos os anexos entregues,os próprios documentos usavam macros maliciosas extensivamente e usam engenharia social para enganar o usuário na execução do código malicioso para infectar seu computador.

2015 foi o ano em que os vetores de ataques móveis passaram ao patamar de ameaças reais difundidas. O roubo de dados e o mau uso de recursos se aplicam a uma ampla gama de aplicativos móveis, desde malware conhecido até a categoria mais ampla de ”riskware“[19].

Conforme figura 16, aplicativos maliciosos enviam dados para servidores em 56 países fora dos EUA.Os 10 principais destinos vieram de 86% de aplicativos maliciosos, sendo a China o destino nº 1 fora dos EUA para dados de aplicativos mal-intencionados.

[19] Riskware é o nome dado a programas legítimos capazes de causar danos quando explorados por usuários maliciosos para excluir, bloquear, modificar ou copiar dados e atrapalhar o bom desempenho de computadores e redes.

Figura 16 – Principais destinos de dados enviados por aplicativos para dispositivos móveis



Fonte: Human Factor Report 2016

2.6 Conscientização e Treinamento

Conscientização é ”a percepção individual das consequências de uma ação, aliada à habilidade de avaliar sua intenção e seu impacto”. A consciência de Segurança da Informação (SI) antecede treinamentos em SI e é um estímulo à participação nestes treinamentos.(SANTARCANGELO, 2010)

O principal objetivo de um programa de conscientização em Segurança da Informação é fazer com que as pessoas mudem seu comportamento, motivar o empregado a querer fazer parte do programa. Explicar como a participação das pessoas vai beneficiar a empresa e os empregados de forma individual. Os colaboradores precisam estar conscientes de que as informações, sejam elas pessoais ou corporativas, são ativos de muito valor e que seu papel na proteção desse ativo é muito importante.(FONSECA, 2009)

Conforme Kumar, Chaudhary e Kumar (2015) há três maneiras comumente sugeridas para se defender contra ataques de engenharia social: educação, treinamento e conscientização;

Essa conscientização em profundidade reduz o risco de ataques e torna a organização menos vulnerável.

- As políticas de segurança devem fornecer informações aos funcionários sobre o manuseio correto das informações da empresa ou de pessoal;
- As auditorias devem ser realizadas para garantir que os funcionários da organização estejam seguindo as políticas e procedimentos;

- As cópias impressas de dados organizacionais, registros ou informações pessoais devem ser destruídas antes de serem descartadas. A utilização de incineradores e trituradores são formas eficazes para destruir as informações;
- Os funcionários ou indivíduos devem ser treinados para questionar as credenciais da pessoa que está se promovendo para estar em posição de autoridade na organização;
- As organizações devem ter cuidado com o que estão postando no site da empresa. Detalhes da empresa como nomes de pessoas com autoridade e números de contato devem ser evitados.

Conscientização é definida na publicação especial NIST [20]800-16 como segue:

> "Conscientização não é formação. O objetivo das apresentações de conscientização é simplesmente focalizar a atenção na segurança. As apresentações de conscientização destinam-se a permitir que indivíduos reconheçam preocupações de segurança de TI e respondam adequadamente.

Os funcionários ou indivíduos da organização devem ser educados através de treinamento e conscientização. Isso pode torná-los mais cuidadosos ao divulgar informações pessoais.

O primeiro passo para a construção de um programa bem-sucedido de conscientização de segurança é entender o conceito de conscientização, como definir a conscientização de segurança e como isso afeta o negócio de uma forma que faça sentido apoiá-la. O aspecto mais importante do programa é estabelecer protocolos de segurança adequados e, então, motivar os funcionários para que assimilem esses protocolos.

Mitnick e Simon (2005) nos apresenta algumas orientações para treinamento:

- Estar ciente dos ataques de engenharia social.

Muitas pessoas sequer têm consciência de que essa ameaça existe. Geralmente elas não esperam ser manipuladas e enganadas, e são apanhadas desprevenidas por um ataque de engenharia social. Exemplos de usuários da Internet têm recebido um e-mail supostamente enviado da Nigéria solicitando ajuda para fazer a transferência de uma soma substancial de dinheiro para os Estados Unidos. No e-mail é oferecida uma porcentagem da soma bruta em troca de assistência. Mais tarde, solicita-se que

[20] NIST - Instituto Nacional de Padrões e Tecnologia dos EUA. Disponível em: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf. Acesso em: 31/01/2017

a vítima adiante uma quantia referente a algumas taxas para iniciar o processo de transferência, e ela fica de bolso vazio.

> Em algum momento os engenheiros sociais irão atacar, talvez repetidamente. Muitas pessoas não tem consciência dessa ameaça e acreditam que não serão pegas desprevenidas.(MITNICK; SIMON, 2005)

- Usar a simulação de papéis para treinar funcionários.

Muitas pessoas acreditam que são ”espertas“ e não vão ser manipuladas, enganadas ou influenciadas.A maioria das pessoas opera sob a ilusão de invulnerabilidade, considerando-se espertas demais para serem manipuladas, persuadidas, enganadas ou influenciadas. Acreditam que isso só acontece com os outros.

Dois métodos são usados para demonstrar a efetividade da engenharia social: (1)Analisar casos de engenharia social para ilustrar o quanto as pessoas estão suscetíveis a esses ataques e (2) fazer com que os funcionários relatem suas experiências durante um seminário de segurança da informação. O treinamento vai servir para examinar o funcionamento dos ataques, analisar por que funcionou e discutir como podem ser reconhecidos e evitados.

- Esclarecer aos trainees que eles se sentirão tolos se forem manipulados em um ataque de engenharia social depois do treinamento. As pessoas são motivadas a não se sentirem ”tolas“ ou ”estúpidas“.

A responsabilidade de cada funcionário em ajudar a proteger os ativos da organização deve ser enfatizada. Um ataque de engenharia social bem-sucedido pode pôr em risco as informações dos funcionários da empresa. O banco de dados dos recursos humanos da empresa pode conter informações pessoais extremamente valiosas para ladrões de identidade.

- Desenvolver procedimentos para ações dos funcionários quando houver suspeita de um ataque de engenharia social ou quando ele for detectado.

Políticas devem ser consideradas como referência,depois que os procedimentos da empresa forem desenvolvidos e colocados em prática, a informação deve ser divulgada na Intranet da empresa, que pode ser rapidamente acessada.

> Durante o treinamento em consciência da segurança, os instrutores devem dar exemplos da proteção assegurada pelo protocolo e dos danos que podem recair sobre a empresa se as pessoas o ignorarem ou forem negligentes com relação a seu cumprimento.(MITNICK; SIMON, 2005)

- Desenvolver orientações simples para funcionários, definindo que informações a empresa considera confidenciais.

É importante transmitir aos funcionários que até as informações que não são consideradas tão confidenciais podem ser úteis a um atacante, que pode coletar qualquer informação aparentemente inútil e juntá-las para criar a ilusão de credibilidade e confiabilidade.

Ferreira e Araújo (2008) diz que, para um programa de conscientização e treinamento ser eficaz deve-se realizar o planejamento, implementação manutenção e avaliação periódicos do programa. Alguns pontos devem ser considerados ao se elaborar um programa de treinamento e conscientização contra ataques de engenharia social:

a) Definir escopo, metas e objetivos: o escopo deve contemplar todos os profissionais que interagem com os sistemas e com a informações sensíveis para a organização;

b) Identificar os instrutores: é importante que os profissionais dominem as técnicas e os princípios de segurança;

c) Identificar o público-alvo: Identificar e separar os grupos de profissionais que receberão o treinamento. Somente os conceitos necessários devem ser apresentados para obter o melhor resultado;

d) Motivação dos funcionários e da alta administração: O apoio dos funcionários e da alta administração é fundamental para que o programa tenha efetividade e é responsabilidade da alta administração assegurar que todos os usuários dos sistemas de informação saibam como proteger seus ativos;

e) Continuidade: dar atenção às mudanças tecnológicas e de segurança de informação. um programa desenvolvido hoje pode tornar-se obsoleto e ineficaz quando houver mudança no ambiente tecnológico;

f) Avaliação: a avaliação dos funcionários após a realização do treinamento é uma boa opção para verificar o aprendizado dos conceitos e avaliar o nível de conscientização e no direcionamento do reforço necessário.

3 COLETA DE DADOS

Este capítulo descreve o planejamento da pesquisa e o processo de coleta de dados que envolve a criação de um questionário prévio com profissionais do setor de segurança da informação para validação do mesmo.

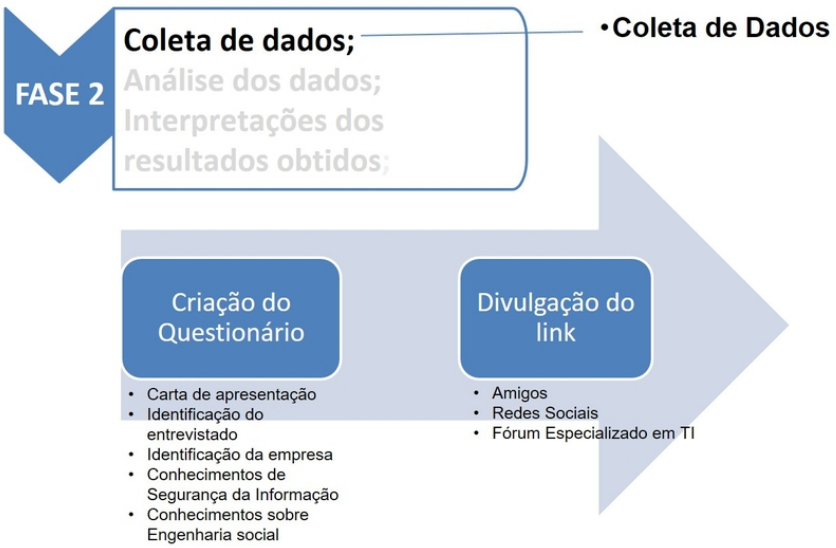
Visando cumprir os objetivos definidos no primeiro capítulo, foi realizada uma pesquisa com usuários de TI em diversos segmentos de mercado com empresas de pequeno a grande porte.

O instrumento de coleta de dados deste trabalho foi o questionário, um meio de documentação direta para obter respostas a questões de forma que o próprio informante o preencha (GIL, 2008).

A utilização dessa técnica propicia vantagens como atingir grande número de pessoas, mesmo que estejam dispersas numa área geográfica muito extensa, já que o questionário pode ser enviado pelo correio ou e-mail, além de permitir que os custos financeiros sejam reduzidos, já que não exige o treinamento dos pesquisadores. Vale destacar, adicionalmente, a flexibilidade de respondê-lo quando se julgar mais conveniente e a não exposição dos pesquisados à influência das opiniões do entrevistador.

A fase 2 da pesquisa é marcada pela coleta, análise e interpretação dos resultados obtidos. A coleta de dados é demonstrada na Figura 17, a seguir:

Figura 17 – Coleta de Dados



Fonte: Autor (2017)

3.1 Pré-teste do Questionário

Antes de ser aplicado definitivamente, um pré-questionário foi feito e submetido a um grupo de 10 pessoas para avaliação. Profissionais de segurança e professores do meio acadêmico foram convidados a responder ao questionário para que pudessem ser observadas falhas na redação ou estrutura do questionário.

De acordo com Vieira (2009),

> a finalidade desta prova, geralmente designada como pré-teste, é evidenciar possíveis falhas na redação do questionário, tais como: complexidade das questões, imprecisão na redação, desnecessidade das questões, constrangimentos ao informante, exaustão etc. O pré-teste é realizado mediante a aplicação de alguns questionários (de 10 a 20) a elementos que pertencem à população pesquisada.

O pré-teste de um instrumento de coleta de dados tem por objetivo assegurar-lhe validade e precisão. Deve assegurar que o questionário esteja bem elaborado, sobretudo no referente a:

a) clareza e precisão dos termos;

b) forma de questões;

c) desmembramento das questões;

d) ordem das questões;

e) introdução do questionário.

3.2 Questionário

O questionário, é uma técnica de investigação composta por diversas questões submetidas a pessoas a fim de obter informações sobre conhecimentos, crenças, sentimentos, valores, interesses, expectativas, aspirações, temores, comportamento presente ou passado e podem apresentar resultados inesperados, pois os itens podem significar, para cada respondente, coisas diferentes.(GIL, 2008)

Os itens podem ter significados diferentes para cada respondente e a limitação da quantidade de questões, torna-se um problema, pois questionários muito extensos apresentam alta probabilidade de não serem respondidos.

Entende-se como a validade de um questionário a evidência de que o mesmo mede o que se propõe a medir de acordo com diferentes tipos de validade: de face, de conteúdo, preditiva e de construção.(VIEIRA, 2009)

Vieira (2009) nos diz que a validade de face é determinada por:

1) Especialistas na questão ;

2) Uma amostra de respondentes, que dirão se o instrumento mede a característica de interesse.

Após feitas as correções, um link diferente foi criado para cada mídia de divulgação para que, desta forma, fosse possível medir o número de respostas ao questionário em cada local divulgado (e-mails, redes sociais, sites, etc). A seguir:

- Link para Telegram e campanha de página no Facebook: **https://pt.surveymonkey.com/r/RM28KFS** ;
- Link para redes sociais: **https://pt.surveymonkey.com/r/5YH8JYH** ;
- Link para fórum de TI especializado em Concursos de TI e afins: **https://pt.surveymonkey.com/r/T1M4573RS**

Cabe observar que, embora os links sejam diferentes, todos apontam para o mesmo questionário.

O questionário foi dividido em 5 partes:

1) Carta de apresentação: cujo objetivo principal é dar uma primeira impressão sobre o trabalho, apresentando o pesquisador e os objetivos da pesquisa.

2) Identificação do entrevistado: com o objetivo de conhecermos qual o público-alvo da pesquisa, foram feitas perguntas com o intuito de conhecermos qual a faixa etária dos respondentes, Estado de residência, nível de escolaridade e ocupação profissional

3) Identificação da empresa: com o objetivo de obtermos informações sobre a empresa do entrevistado, seu tamanho e área de atuação.

4) Conhecimentos de Segurança da Informação: com o objetivo de coletar informações sobre o conhecimento que o entrevistado tem dos conceitos de Segurança da Informação e como a empresa em que trabalha lida com estes conceitos.

5) Sobre engenharia social: com o objetivo de coletar informações sobre o nível de conhecimento que o entrevistado e a empresa onde trabalha tem sobre conceitos de engenharia social e fraudes eletrônicas.

Cada questionário possuía as questões explicadas a seguir:

A partir da questão 1 até a questão 6 são coletadas informações sobre o aceite do entrevistado em responder o questionário e informações gerais sobre o respondente. A seguir:

Questão 1: Você concorda com os termos acima? Clicando em Sim, você concorda que está disposto a responder às perguntas deste questionário.

Explicação: O objetivo da pergunta era saber se o respondente do questionário concordava em responder ao questionário e dar a opção de sair do questionário e contabilizar sua opção.

Questão 2: Qual sua faixa etária?

Explicação: O objetivo é saber qual a faixa etária dos respondentes e obter dados para comparar com outras variáveis como grau de escolaridade.

Questão 3: Em que Estado você mora?

Explicação: O objetivo é saber a localidade onde cada um dos respondentes reside para que se possa fazer uma análise comparativa entre o percentual de cada estado brasileiro que participou da pesquisa.

Questão 4: Qual o seu endereço de email ? (Necessário e-mail válido caso queira concorrer ao brinde.)

Explicação: O objetivo foi coletar o e-mail dos respondentes e, após o encerramento do questionário, fazer um sorteio de um brinde entre os respondentes como forma de incentivo.

Questão 5:Qual seu último nível de escolaridade completo ?

Explicação: O objetivo foi medir o nível de escolaridade dos respondentes e avaliar a relação entre nível de escolaridade e conhecimento sobre os conceitos de Segurança da Informação e engenharia social.

Questão 6: Qual das seguintes opções melhor descreve a sua ocupação atual?

Explicação: O objetivo é saber qual a ocupação do respondente e avaliar qual segmento tem mais respondentes.

Da questão 7 à questão 9, são coletadas infomrações sobre o ambiente de trabalho do entrevistado. A seguir:

Questão 7: Qual das seguintes opções melhor descreve a área de ATUAÇÃO PRINCIPAL da sua empresa?

Explicação: O objetivo é saber qual a principal de atuação das empresas e verificar se existe alguma relação entre as empresas que responderam.

Questão 8:Qual o setor de atuação de sua empresa?

Explicação: Visa apresentar um perfil de empresas que responderam ao questionário, mostrando qual dos segmentos mais participou da pesquisa.

Questão 9: De acordo com a tabela abaixo, classifique a empresa em que trabalha quanto ao porte.

Quadro 1 – Classificação dos estabelecimentos de acordo com o SEBRAE

Classificação dos estabelecimentos segundo porte

Porte	Setores	
	Indústria[1]	Comércio e Serviços[2]
Microempresa	até 19 pessoas ocupadas	até 9 pessoas ocupadas
Pequena empresa	de 20 a 99 pessoas ocupadas	de 10 a 49 pessoas ocupadas
Média empresa	de 100 a 499 pessoas ocupadas	de 50 a 99 pessoas ocupadas
Grande empresa	500 pessoas ocupadas ou mais	100 pessoas ocupadas ou mais

Fonte: SEBRAE
Elaboração: DIEESE
Nota: (1) As mesmas delimitações de porte foram utilizadas para o setor da construção
(2) O setor serviços não inclui administração pública e serviço doméstico

Fonte: SEBRAE

Explicação: Classificação do porte das empresa que os respondentes trabalham.

Classificam-se em pequena, média e grande empresa de acordo com classificação dos estabelecimentos elaborada pelo SEBRAE.

Da questão 10 à questão 16, trata-se de perguntas sobre Segurança da Informação. São informações sobre o nível de conhecimento que o entrevistado tem sobre conceitos de engenharia social e fraudes eletrônicas

Questão 10: Quanto possui de conhecimento do papel da Segurança da Informação em sua empresa?

Explicação: O objetivo é avaliar o nível de conhecimento do respondente sobre o quanto a Segurança da Informação é importante na empresa em que trabalha.

Questão 11: Sua empresa possui alguma Política de Segurança de Informação e Comunicações (POSIC)?

Explicação: O objetivo da pergunta é descobrir se a empresa onde o respondente trabalha possui uma política de segurança e comparar o percentual de empresas entrevistadas que possuem a política de segurança com as que não possuem.

Questão 12: Em caso afirmativo, essa política é divulgada para os funcionários?

Explicação: O objetivo da pergunta é avaliar se a política de segurança é formalizada,divulgada na empresa e se todos os funcionários a conhecem.

Questão 13: Quanto possui de conhecimento acerca das normas de Segurança da Informação (SI) relacionadas à sua atividade na empresa?

Explicação: O objetivo da pergunta é verificar o percentual de pessoas que conhecem as normas de SI que estão relacionadas à sua atividade profissional.

Questão 14: Conhece as informações que devem ser protegidas na empresa em que trabalha?

Explicação: O objetivo da pergunta é avaliar se o respondente conhece as informações importantes e quais as que devem ser protegidas em sua empresa.

Questão 15: Sua empresa realiza treinamento de conscientização em Segurança da Informação para funcionários e parceiros de negócio?
Explicação: A pergunta tem por objetivo avaliar qual o nível de envolvimento da empresa em desenvolver uma política de treinamento em SI.

Questão 16: Você tem percepção que o assunto ”Segurança da Informação“ é debatido de forma estratégica na sua empresa?

Explicação: O objetivo desta questão é verificar se a empresa compreende o valor da Segurança da Informação na empresa e se possui planos para tratar o assunto de forma estratégica. Visa avaliar se os usuários consideram a Segurança da Informação algo importante para o negócio

Da questão 17 à questão 29, são as questões relacionadas ao conhecimento sobre engenharia social e o nível de conhecimento que o entrevistado tem a respeito do assunto.

Questão 17: Você já tinha ouvido falar no termo ”engenharia social“?

Explicação: A questão visa avaliar qual o percentual de pessoas entrevistadas que sabem o que é a engenharia social.

Questão 18: Qual o nível de consciência que você possui a respeito da potencial ameaça de ataques de engenharia social ?

Explicação: A questão visa avaliar o quanto as pessoas entrevistadas conhecem o perigo dos ataques de engenharia social.

Questão 19: Sua organização já sofreu algum ataque de engenharia social?

Explicação: A questão visa avaliar se os respondentes sabem se suas empresas já sofreram ataques de engenharia social e verificar a relação com a questão que trata do conhecimento do conceito de engenharia social.

Questão 20: Na sua opinião, qual a motivação por trás de ataques de engenharia social.

Explicação: A questão visa saber qual a opinião do respondente sobre os motivos que levam o Engenheiro Social a atacar uma organização.

Questão 21: Na sua opinião, que tipo de pessoal é o mais suscetível a ataques de engenharia social?

Explicação: A questão busca saber qual funcionário seria mais suscetível a ataques de engenharia social.

Questão 22: O que sua organização está fazendo para prevenir ataques de engenharia social?

Explicação: O objetivo desta pergunta é avaliar se a empresa tem a preocupação de promover treinamentos, cursos ou outro eventos junto aos funcionários / terceirizados e se possui algum direcionamento para tal.

Questão 23: Na sua opinião qual é a fonte mais comum de ataques de engenharia social?

Explicação: Essa questão visa descobrir qual a principal fonte de ataques de engenharia social na opinião do respondente.

Questão 24: Na sua opinião, qual o nível de importância (1 = menos importante, 5 = mais importante) dos seguintes meios de proteção contra a engenharia social.(Cada nota deve ser individual e única de acordo com seu grau de importância)

Treinamento de funcionários e terceirizados em Segurança da Informação

Definir Políticas de Segurança

Investimento em Firewalls e outras ferramentas de Segurança

Investimento em Segurança Física

Definir um Plano de Gerenciamento de Segurança

Explicação: O objetivo da questão é avaliar, na opinião do respondente, qual seria o item mais importante na proteção contra ataques de engenharia social nas empresas.

Questão 25: Você recebeu nos últimos 6 meses algum contato através de email, chamadas telefônicas ou SMS e desconfiou que tenha sido um ”trote“ para capturar informações suas?

Explicação: O objetivo da questão é medir a frequência e o nível de percepção que o respondente tem sobre situações que apontam para um ataque de engenharia social.

Questão 26: Conhece alguém que já foi vítima de engenharia social?
des Eletrônicas,Golpes, Vazamento de Informações, etc)

Explicação: O objetivo da questão é medir o número de pessoas dentro do universo estudado que já tiveram contato com ações de engenharia social nas mais

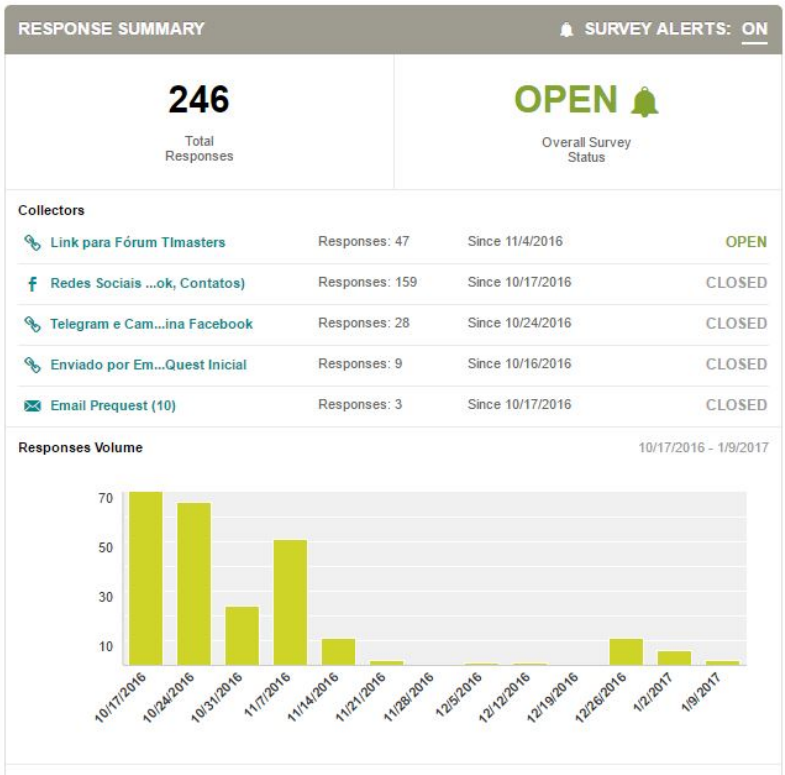
diversas formas, além de medir a frequência e o nível de percepção que o respondente tem sobre situações que apontam para um ataque de engenharia social.

Questão 27: Você publica informações pessoais nas redes sociais?

Explicação: O objetivo da questão é verificar o percentual de pessoas no universo estudado, que publicam informações pessoais nas redes sociais, expondo seus hábitos e preferências pessoais, tornando-se um alvo em potencial para Engenheiros Sociais.

O questionário foi disponibilizado em 03/10/2016 e encerrado no dia 09/01/2017, para o qual foram obtidas 246 respostas, conforme figura 18.

Figura 18 – Número de questionários obtidos



Fonte: Autor - www.surveymonkey.com

O público-alvo abrange profissionais de qualquer segmento de mercado, que exercem qualquer atividade profissional e que são usuários (gestores ou não) de sistemas de informação, sem restrição.

3.3 Divulgação da pesquisa em Redes Sociais

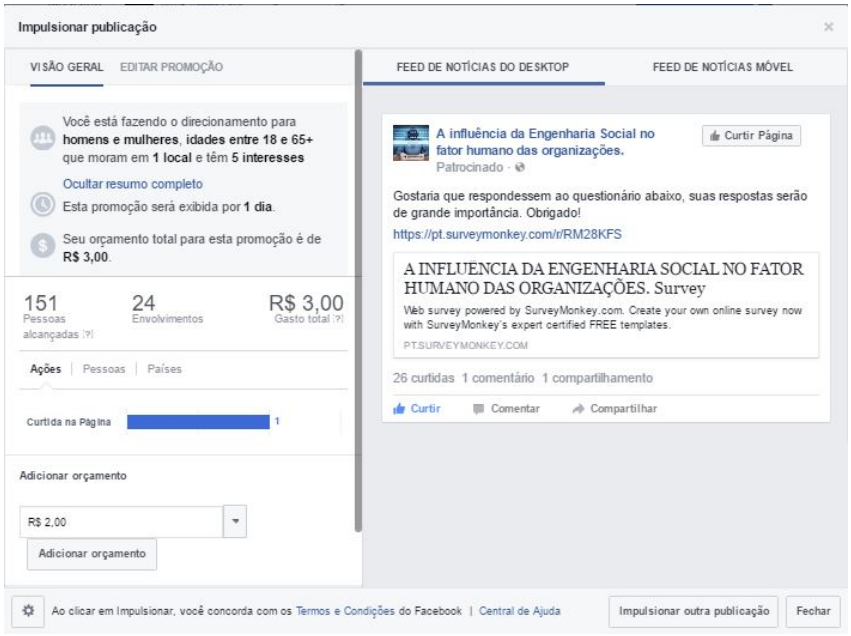
A fim de obter o maior número possível de respostas, a figura 19 mostra uma página criada em rede social com *link* que direcionava para o questionário. O objetivo maior com a criação da página é torná-la um ponto de informações sobre Segurança da Informação e engenharia social.

Figura 19 – Página em rede social para divulgação da pesquisa

Fonte: Autor - www.facebook.com/pesquisaengsocial

A página criada direcionava alguns links e publicações para o questionário. A mesma obteve 152 visitas. O público-alvo da página eram pessoas do sexo masculino e feminino com idade entre 18 e 65 anos de idade, no Brasil e que possuem interesse nos temas engenharia social, Fraude Virtual, Phishing, Redes Sociais, Tecnologia e Tecnologia da informação, conforme figura 20.

Figura 20 – Caracteristicas do público atingido em página de Rede Social



Fonte: Autor - https://www.facebook.com

Houve uma distribuição de links que direcionavam para a página na rede social, com o intuito de divulgar a pesquisa e manter o fornecimento de informações sobre engenharia social e outros crimes de infomática, a página permanecerá no ar mesmo após a conclusão da pesquisa.

4 RESULTADOS E DISCUSSÃO

Neste capítulo são apresentados e analisados os resultados do questionário aplicado para atender aos objetivos definidos no capítulo 1.

A partir dos dados obtidos, analisa-se principalmente 3 grupos de variáveis importantes para identificar o impacto dos ataques de engenharia social nas organizações:

- A estrutura social das empresas e empregados;
- O nível de conhecimento dos respondentes sobre a Segurança da Informação;
- O nível de conhecimento dos respondentes sobre a engenharia social.

4.1 Dos entrevistados e empresas pesquisadas

A população da pesquisa foram pessoas de qualquer atividade profissional, do setor privado ou público, usuários de sistemas de tecnologia em seu cotidiano.

Para o cálculo amostral, foi utilizada a fórmula $n = \frac{N.Z.p.(1-p)}{Z.p.(1-p)+e.(N-1)}$, onde:

n - amostra calculada

N - população

Z - variável normal padronizada associada ao nível de confiança

p - verdadeira probabilidade do evento

e - erro amostral

Para uma população indeterminada,foi admitido um erro amostral de 6% e um nível de confiança de 90%, isso implica em uma amostra necessária de 118 respostas. Após 3 meses de coleta de dados, foram obtidas 246 respostas ao questionário, sendo que 223 pessoas responderam o questionário totalmente, o que equivale a 91% de respostas completas, conforme figura 21.

Figura 21 – Tela de aplicativo Survey Monkey para dispositivos móveis

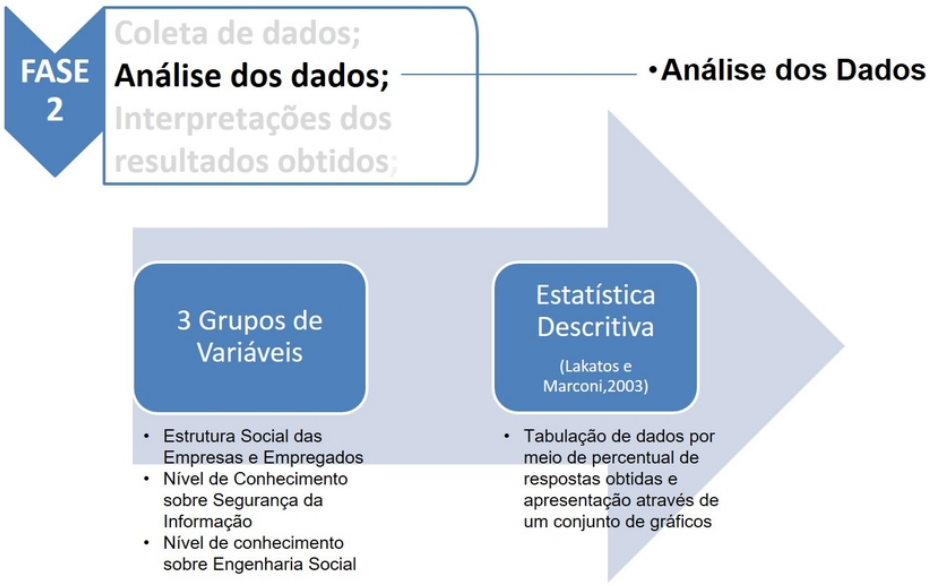
Fonte: Autor

A análise dos dados visa interpretar os dados obtidos na pesquisa. De acordo com Lakatos e Marconi (2003),utilizamos o modelo de estatística descritiva que tabula os dados por meio de percentual das respostas obtidas e apresentação através de um conjunto de gráficos, sendo mais uma etapa no processo de investigação.

> “A análise tem como objectivo organizar e sumariar os dados de tal forma que possibilitem o fornecimento de respostas ao problema proposto para investigação” (GIL, 2008)

A análise dos dados é descrita na figura 22, a seguir:

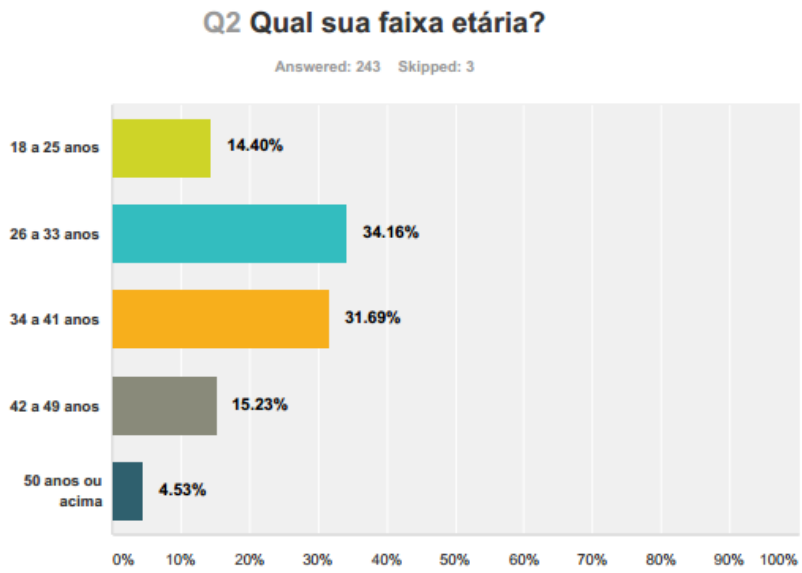
Figura 22 – Análise dos dados



Fonte: Autor

Encerrando a fase 2, tem-se os relatórios e a geração de gráficos a partir de amostra estudada e representada por um público, em sua maioria, entre 26 e 33 anos de idade, o que equivale a 34,18% dos que responderam a esta questão. Da amostra total de 246 questionários respondidos, foram consideradas 223 respostas completas.

Gráfico 1 – Faixa etária dos respondentes

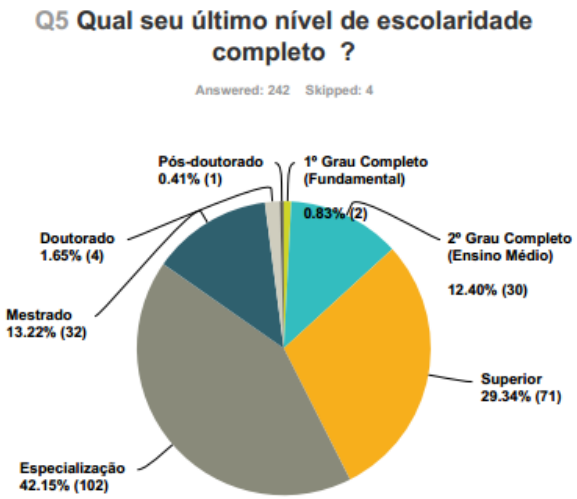


Answer Choices	Responses	
18 a 25 anos	14.40%	35
26 a 33 anos	34.16%	83
34 a 41 anos	31.69%	77
42 a 49 anos	15.23%	37
50 anos ou acima	4.53%	11
Total		243

Fonte: Autor

O nível de escolaridade é relativamente alto entre os respondentes. A parcela que compreende a faixa que vai do nível superior ao doutorado , compreende 85,1% dos respondentes. O último grau de escolaridade completo, em sua maioria é a Especialização (42,1%), e conforme observamos também no gráfico abaixo, 29,3% dos respondentes possuem nível superior completo.

Gráfico 2 – Nível de escolaridade dos respondentes



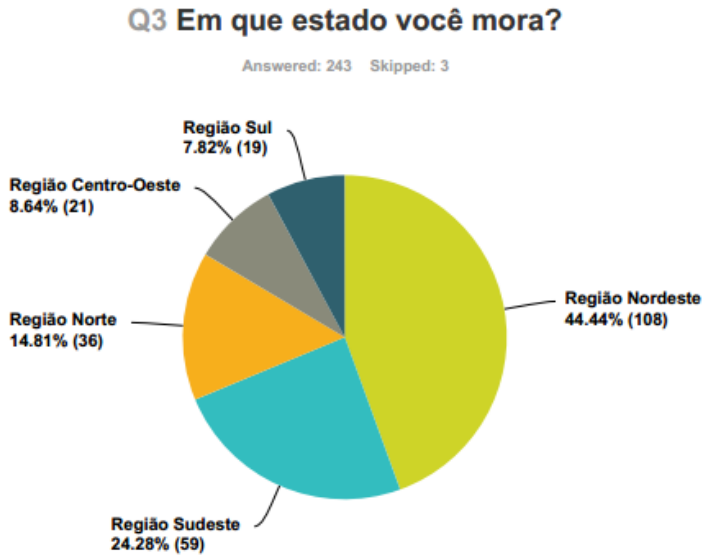
Answer Choices	Responses	
1º Grau Completo (Fundamental)	0.83%	2
2º Grau Completo (Ensino Médio)	12.40%	30
Superior	29.34%	71
Especialização	42.15%	102
Mestrado	13.22%	32
Doutorado	1.65%	4
Pós-doutorado	0.41%	1
Total		242

Fonte: Autor

A pesquisa contou com respondentes residentes em praticamente todo o território nacional - com exceção dos estados de Roraima e Amapá - em sua maioria nos estados do Rio Grande do Norte, Maranhão e São Paulo, com 40, 23 e 20 respondentes respectivamente, em um universo de 243 respostas.

O gráfico abaixo apresenta o quantitativo de respondentes agrupados por região geográfica do país,dispostos em sua maioria na região Nordeste (44,4%).

Gráfico 3 – Percentual de respondentes por Região geográfica.

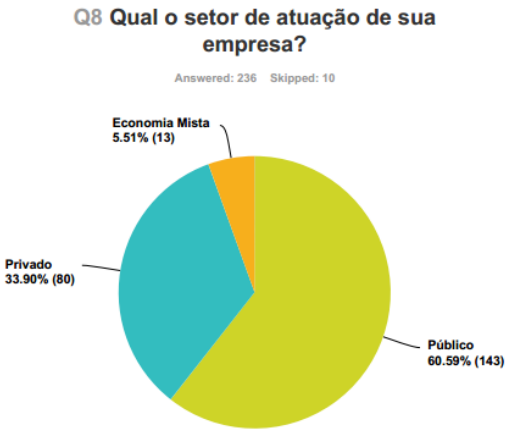


Answer Choices	Responses	
Região Nordeste	44.44%	108
Região Sudeste	24.28%	59
Região Norte	14.81%	36
Região Centro-Oeste	8.64%	21
Região Sul	7.82%	19
Total		243

Fonte: Autor

A amostra de respondentes foi de 236 e é representada por 60,5% de empregados do setor público, 33,9% do setor privado e 5.5% de empresas de economia mista, conforme mostrado no gráfico 4.

Gráfico 4 – Setor de atuação da empresa



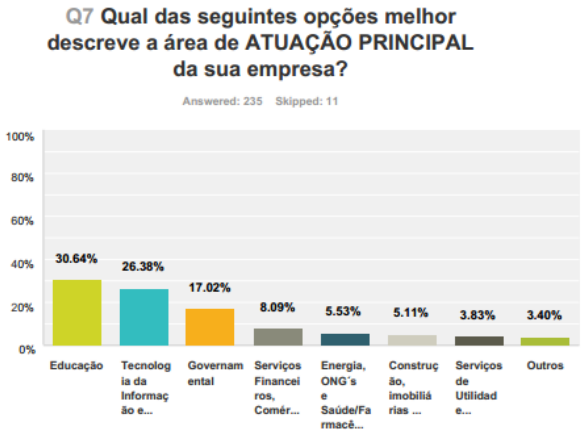
Answer Choices	Responses	
Público	60.59%	143
Privado	33.90%	80
Economia Mista	5.51%	13
Outro	0.00%	0
Total		236

Fonte: Autor

A variável ”atuação principal da empresa“ é demonstrada no gráfico 5 e observa-se que a maioria de 30,9% das empresas dos respondentes pertence à área da Educação, seguida pelas áreas de Tecnologia da Informação e área governamental, com 26,4% e 17,0% respectivamente.

O maior percentual da área educacional já era esperado, tendo em vista que houve uma ampla participação por parte de respondentes que fazem parte do quadro funcional dos Institutos Federais de Ciência e Tecnologia do país.

Gráfico 5 – Área de atuação da empresa dos respondentes



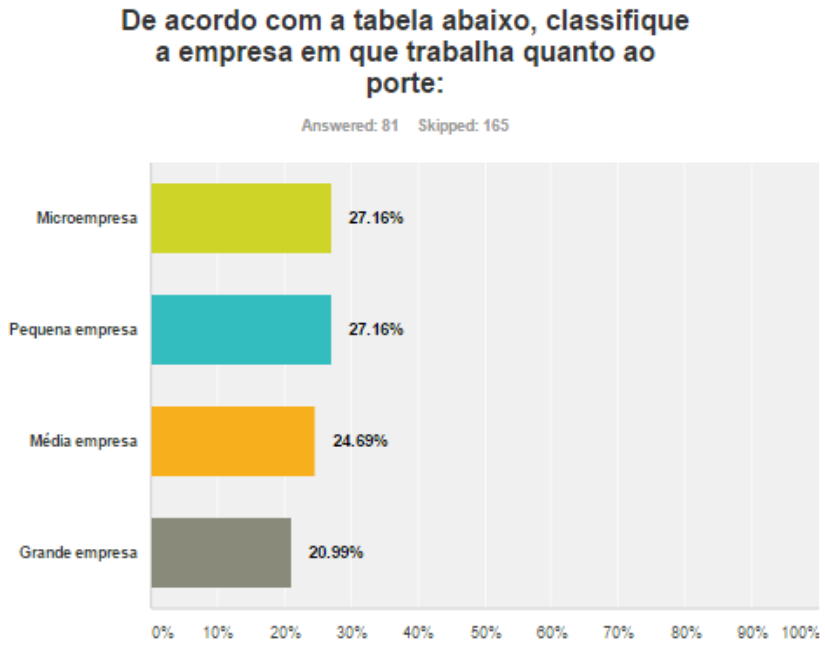
Answer Choices	Responses	
Educação	30.64%	72
Tecnologia da Informação e Eletrônicos	26.38%	62
Governamental	17.02%	40
Serviços Financeiros, Comércio, Alimentos e Bebidas	8.09%	19
Energia, ONG´s e Saúde/Farmacêutica	5.53%	13
Construção, imobiliárias e manufatura	5.11%	12
Serviços de Utilidade Pública, Marketing	3.83%	9
Outros	3.40%	8
Total		235

Fonte: Autor

Dentre os 246 respondentes, 81 infomaram que trabalham em empresas privadas, perfazendo um total de 54,2%.

Desse total, 24,6% são respondentes das médias empresas com 24,6% e 20,9% são de pequenas empresas, conforme mostra o gráfico a seguir:

Gráfico 6 – Porte das empresas dos respondentes



Answer Choices	Responses	
Microempresa	27.16%	22
Pequena empresa	27.16%	22
Média empresa	24.69%	20
Grande empresa	20.99%	17
Total		81

Fonte: Autor

4.2 Dos conhecimentos sobre Segurança da Informação

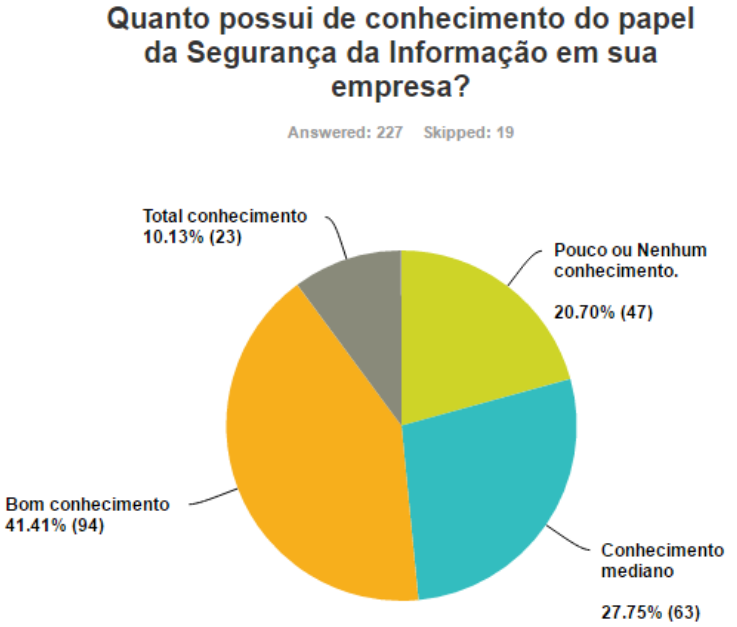
O nível de conhecimento em Segurança da Informação (SI) foi uma variável pesquisada, visto que é um tema relacionado à pesquisa. Dos 246 respondentes, 227 responderam, perfazendo um total de 92,2% do total de respostas válidas.

Na Seção 2.1.1 é citado que o conhecimento e a informação devem ser levados a toda a organização e que, como qualquer outro ativo importante, a informação deve ser bem protegida. Considerando que 20,7% dos respondentes possuem pouco ou nenhum conhecimento sobre o papel da SI na empresa, inferimos que a necessidade de maior investimento em uma cultura de segurança seja necessário. É importante conscientizar os usuários sobre as ações de um Engenheiro Social, as pessoas precisam conhecer o valor das informações que elas manipulam.

Como demonstra o gráfico 7, 41,1% dos que responderam a pergunta julga possuir um bom conhecimento sobre o papel da SI em sua empresa (41,1%) ao passo

que 27,7% alegam ter conhecimentos medianos sobre tal.

Gráfico 7 – Papel da Segurança da Informação na empresa



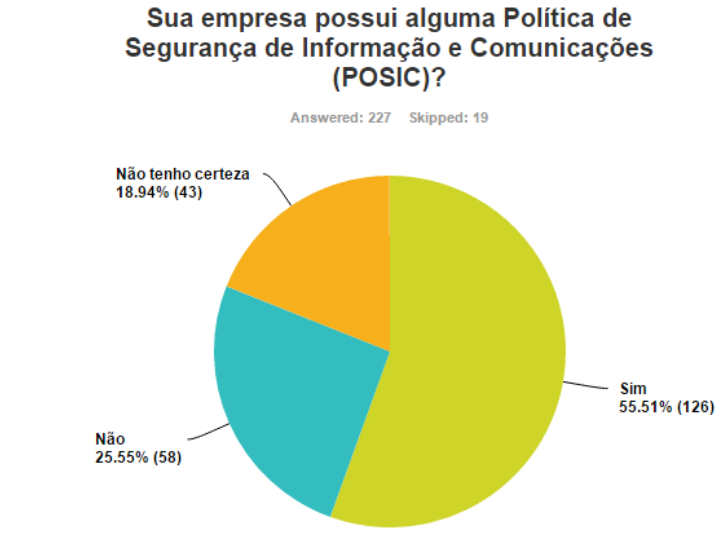
Answer Choices	Responses	
Pouco ou Nenhum conhecimento.	20.70%	47
Conhecimento mediano	27.75%	63
Bom conhecimento	41.41%	94
Total conhecimento	10.13%	23
Total		227

Fonte: Autor

Conforme preconiza a ABNT (2013), a POSIC da empresa deve ser uma estrutura que deve conter os conceitos de Segurança da Informação, uma estrutura para estabelecer as formas de controle e os objetivos de segurança da organização é um elemento de controles efetivos para combater as possíveis ameaças à segurança.

Sobre as questões que avaliam a existência e o conhecimento da Política de Segurança de Informação e Comunicações (POSIC) por parte dos respondentes, podemos observar que, das 227 pessoas que responderam a pergunta, obtivemos um percentual de 55,1% de respondentes cuja empresa possui uma política de segurança, 25,5% não possui e 18,9% não tem certeza da existência de uma política de segurança em sua empresa. O percentual de pessoas cuja empresa não possui ou não tem certeza sobre a existência de uma POSIC, é alto (44,4%).

Gráfico 8 – Gráfico de existência da Política de Segurança



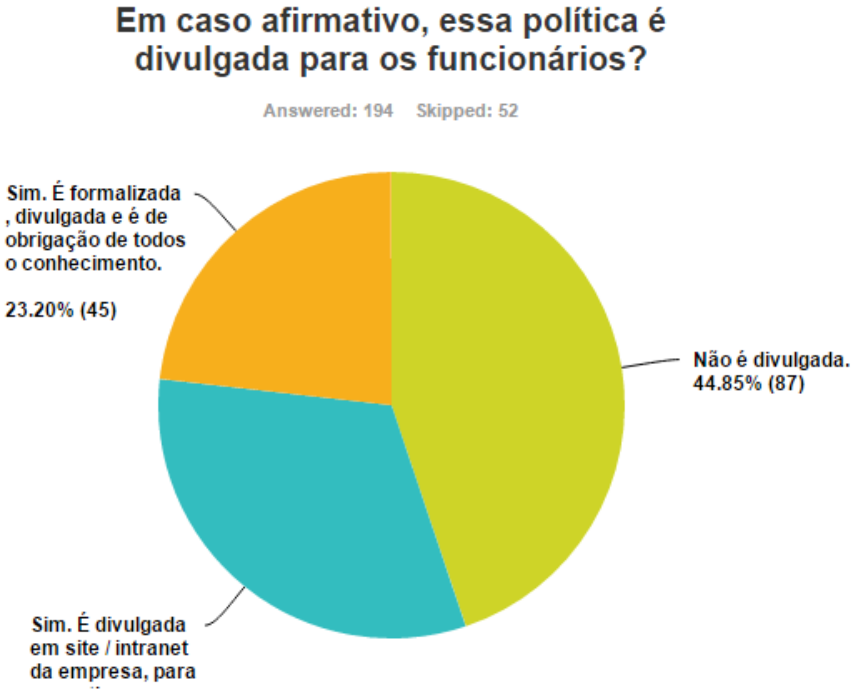
Answer Choices	Responses	
Sim	55.51%	126
Não	25.55%	58
Não tenho certeza	18.94%	43
Total		227

Fonte: Autor

Devido o conhecimento da importância da POSIC e de sua relação com o posicionamento estratégico das empresas, o questionário perguntou sobre a existência da Política de Segurança e constatou que dos 194 respondentes que informaram a existência da POSIC em sua organização, 44,8% informaram que a POSIC não é divulgada, conforme gráfico abaixo, e apenas 23,2% informaram que a POSIC é amplamente divulgada e de obrigação de todos. A POSIC deve ser conhecida por todos os funcionários da organização, inclusive para novos colaboradores.

> Convém que um conjunto de políticas de Segurança da Informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes (ABNT, 2013).

Gráfico 9 – Percentual de divulgação da POSIC nas empresas



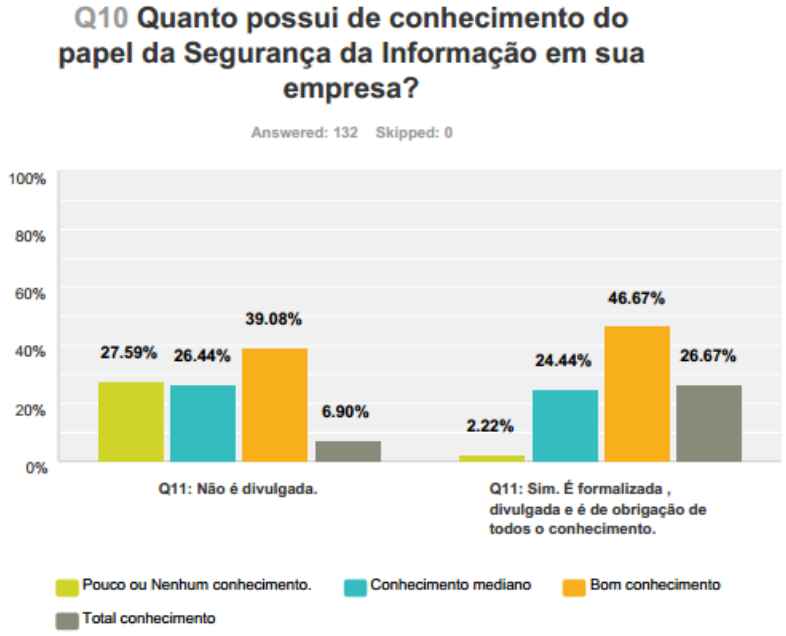
Answer Choices	Responses
Não é divulgada.	44.85% 87
Sim. É divulgada em site / intranet da empresa, para quem tiver interesse em conhecer.	31.96% 62
Sim. É formalizada , divulgada e é de obrigação de todos o conhecimento.	23.20% 45
Total	194

Fonte: Autor

De acordo com Nakamura e Geus (2007) a política de segurança deve tornar-se parte da cultura da empresa, com suas regras estruturais e seus controles disseminados de forma que todos sejam conscientizados. Comunicações internas, reuniões de divulgação, treinamentos específicos entre outras ações são exemplos de formas de divulgação.

Diante o exposto, observa-se que, quando a empresa não possui uma política de segurança divulgada de forma consistente, o nível de conhecimento acerca da importância da segurança na empresa diminui consideravelmente, conforme exposto no gráfico abaixo:

Gráfico 10 – Conhecimento acerca do papel da Segurança da Informação



	Pouco ou Nenhum conhecimento.	Conhecimento mediano	Bom conhecimento	Total conhecimento	Total
Q11: Não é divulgada.	27.59% 24	26.44% 23	39.08% 34	6.90% 6	65.91% 87
Q11: Sim. É formalizada , divulgada e é de obrigação de todos o conhecimento.	2.22% 1	24.44% 11	46.67% 21	26.67% 12	34.09% 45
Total Respondents	25	34	55	18	132

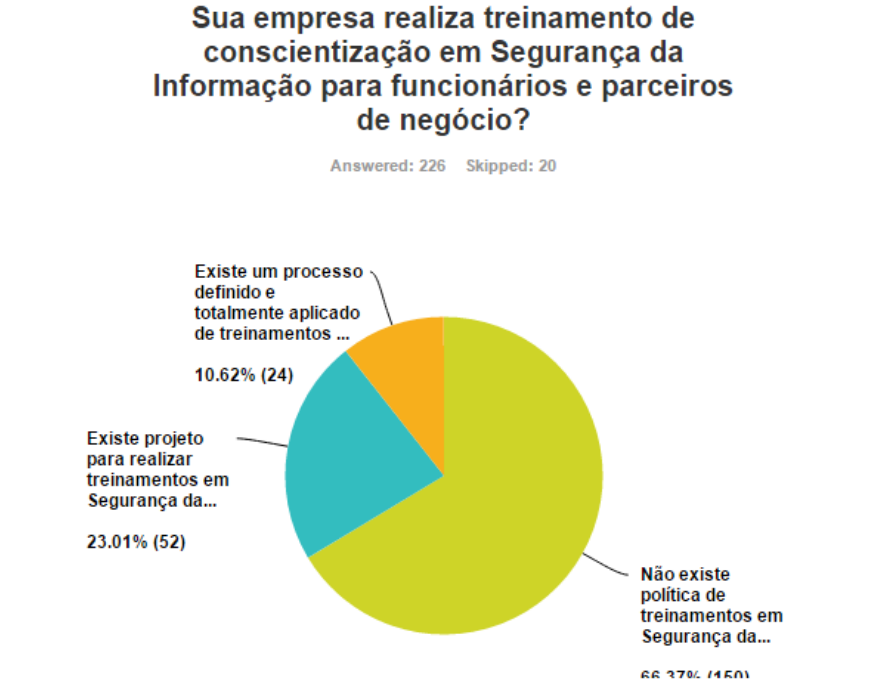
Fonte: Autor

Observa-se que nos casos em que a POSIC não é divulgada temos um percentual de 27,59% de pessoas com pouco ou nenhum conhecimento sobre o papel da Segurança de Informação em sua empresa.

Comparando com empresas onde existe uma política formalizada e divulgada , o índice de desconhecimento cai de 27,9% para 2,2% (uma variação percentual de 92,1%) e há um aumento nos níveis de pessoas que se julgam com bom ou total conhecimento do papel de SI na empresa,com uma variação de 19,42% e 286,5%, respectivamente.

Analisando a questão sobre treinamentos em Segurança da Informação, dos 226 elementos que responderam a pergunta, apenas 10,6% possui um processo definido e aplicado de treinamento, 23% possui um projeto pra realizar treinamentos e, o maior percentual, 66,3% informa a não existência de treinamentos em SI, conforme gráfico abaixo:

Gráfico 11 – Percentual de treinamentos de conscientização em Segurança da Informação



Answer Choices	Responses
Não existe política de treinamentos em Segurança da Informação	66.37% 150
Existe projeto para realizar treinamentos em Segurança da Informação	23.01% 52
Existe um processo definido e totalmente aplicado de treinamentos em Segurança da Informação	10.62% 24
Total	226

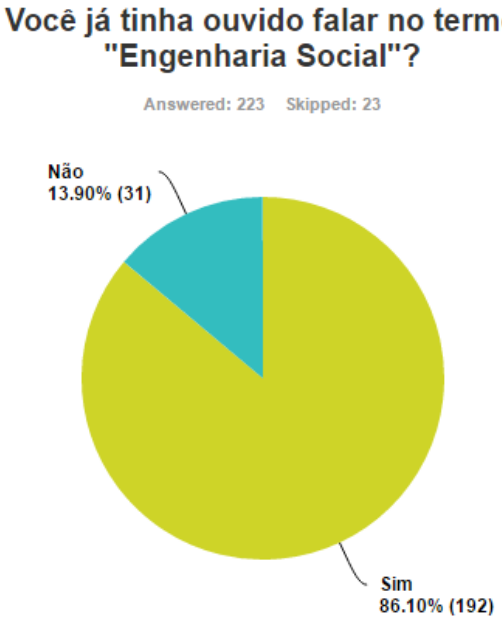
Fonte: Autor

4.3 Dos conhecimentos sobre engenharia social

De acordo com Hadnagy (2011), engenharia social ”é o ato de manipular uma pessoa para tomar uma ação que pode ou não estar no melhor interesse do “alvo” “. Ou ainda, ” a arte ou, melhor ainda, a ciência, de habilidosamente manobrar seres humanos a realizar ações em algum aspecto de suas vidas.“

Dos 223 respondentes que responderam à pergunta sobre o nível de conhecimento sobre engenharia social, 86,1% informaram que já tinham ouvido falar do termo ”engenharia social“ e 13,9% não conheciam o termo. De acordo com o gráfico abaixo:

Gráfico 12 – Percentual de conhecimento do termo ”engenharia social“

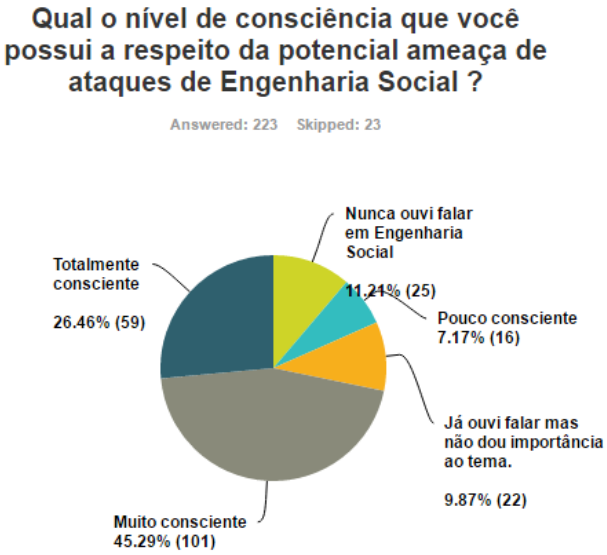


Answer Choices	Responses	
Sim	86.10%	192
Não	13.90%	31
Total		223

Observa-se no gráfico abaixo que dos respondentes que responderam a questão, 45,2% se consideram muito conscientes sobre a real ameaça dos ataques de engeharia Social, 26,4% consideram-se totalmente conscientes. Entretanto,o percentual de pessoas que nunca ouviram falar em engenharia social, que são pouco conscientes ou que ouviram mas não dão importância ao assunto atingem o patamar de 28.2%.

Os ataques a informações sensíveis de uma organização usando a engenharia social estão cada vez mais sofisticados. Os treinamentos de conscientização sobre Segurança da Informação não acompanham o nível de sofisticação dos ataques de engenharia social.

Gráfico 13 – Percentual de consciência sobre a ameaça de engenharia social



Answer Choices	Responses	
Nunca ouvi falar em Engenharia Social	11.21%	25
Pouco consciente	7.17%	16
Já ouvi falar mas não dou importância ao tema.	9.87%	22
Muito consciente	45.29%	101
Totalmente consciente	26.46%	59
Total		223

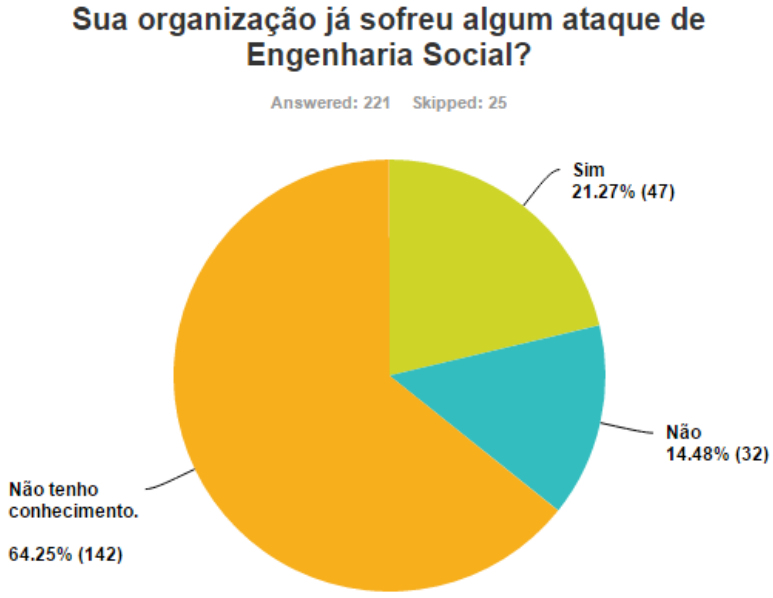
Fonte: Autor

A falta de conhecimento sobre os ataques de engenharia social é comprovada pelo gráfico 14.

Observa-se que 64,25% dos 221 respondentes informam que não tem conhecimento se sua empresa já sofreu algum tipo de ataque de engenharia social e 21,27% afirmam que sua empresa já foi atacada por engenharia social. Ante o exposto, temos um percentual de 85,52% dos respondentes respondentes em posição vulnerável frente à engenharia social.

A engenharia social é sem dúvida a maneira mais fácil para um atacante penetrar nas defesas de uma organização. Como parte da proteção de uma organização, a maioria dos especialistas concorda que treinar os usuários finais para que estejam cientes dos tipos de ameaças que eles podem encontrar é essencial para uma efetiva estratégia de Segurança da Informação (MITNICK; SIMON, 2003).

Gráfico 14 – Percentual de ataques de engenharia social



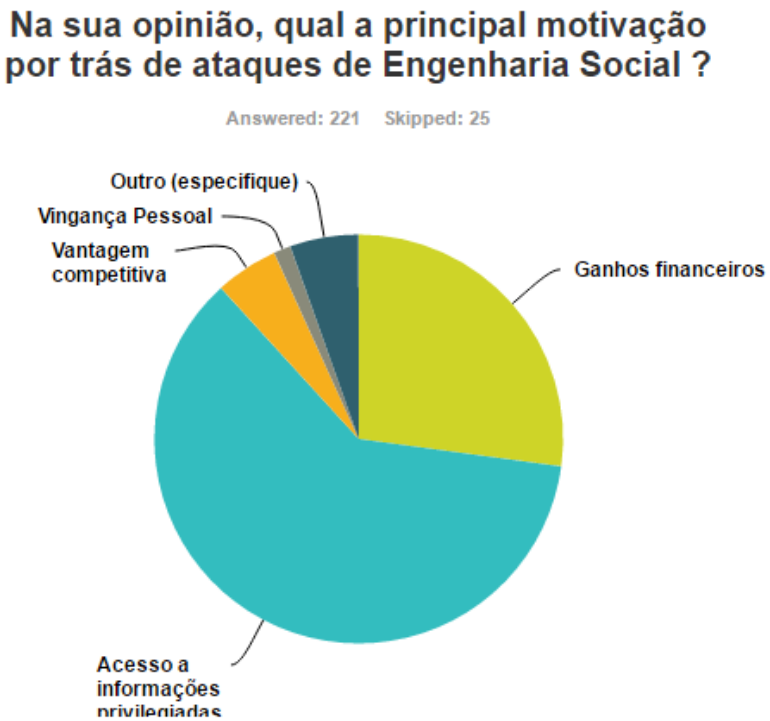
Answer Choices	Responses	
Sim	21.27%	47
Não	14.48%	32
Não tenho conhecimento.	64.25%	142
Total		221

Fonte: Autor

No gráfico 15, demonstra-se o percentual que indica os motivos por trás de ataques de engenharia social, das 221 pessoas que responderam o questionário, a maioria (61%) acredita que a principal motivação dos ataques de engenharia social é o acesso a informações privilegiadas, seguido por ganhos financeiros e vantagens competitivas, respectivamente 27,1% e 4,9%. A motivação vingança pessoal apresentou 1,3%.

Outros motivos entraram na estatística como respondentes que corroboram com a idéia que todos os itens são motivos para um ataque de engenharia social, perfazendo um total de 5,43%.

Gráfico 15 – Gráfico de motivação de ataques de engenharia social



Answer Choices		Responses	
Ganhos financeiros		27.15%	60
Acesso a informações privilegiadas		61.09%	135
Vantagem competitiva		4.98%	11
Vingança Pessoal		1.36%	3
Outro (especifique)	Responses	5.43%	12
Total			221

Fonte: Autor

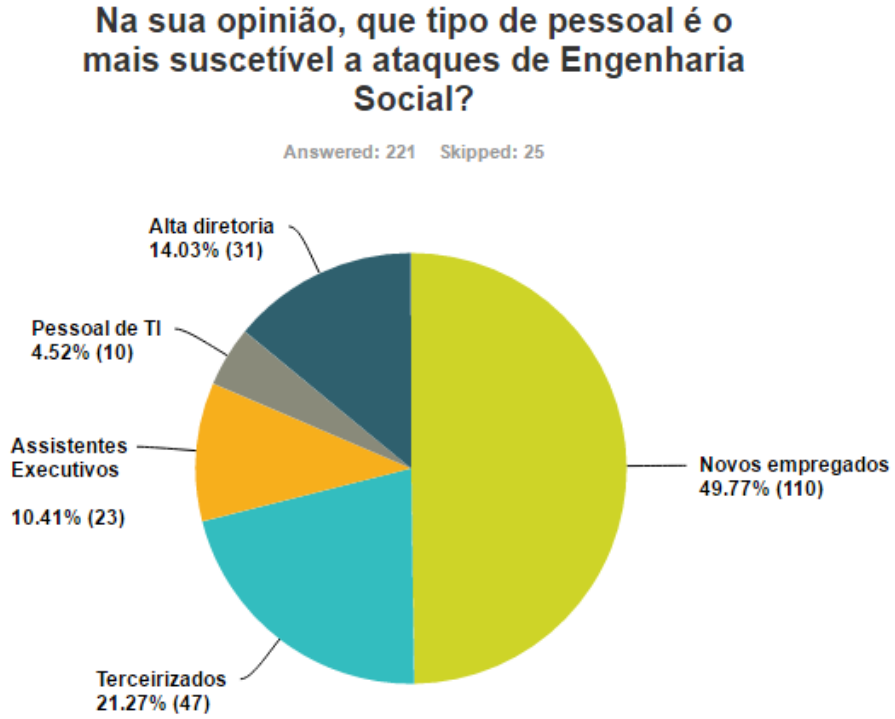
Avaliamos no gráfico 16, o tipo de pessoal mais suscetível a ataques de engenharia social. Constata-se que, dos respondentes da pesquisa, 49,7% considera que os novos empregados são a porta de entrada dos ataques de engenharia social nas empresas, seguidos por Terceirizados (21,2%), Alta diretoria (14 %), Assistentes Executivos (10,4%) e Pessoal de TI, com 4,5%.

Isso vai ao encontro do estudo de Chengalur-Smith (2010), que diz que o atacante procura explorar aqueles que, por sua própria natureza, tendem a ser mais úteis e mais confiáveis, e os novos empregados se encaixam bem nesse perfil. Mitnick e Simon (2005) também diz que ”um atacante visa os empregados do nível iniciante porque geralmente eles não têm consciência do valor das informações específicas da empresa ou dos possíveis resultados de determinadas ações.“

Da mesma forma, eles tendem a ser facilmente influenciados por algumas

das abordagens mais comuns da engenharia social — um interlocutor que invoca a autoridade.

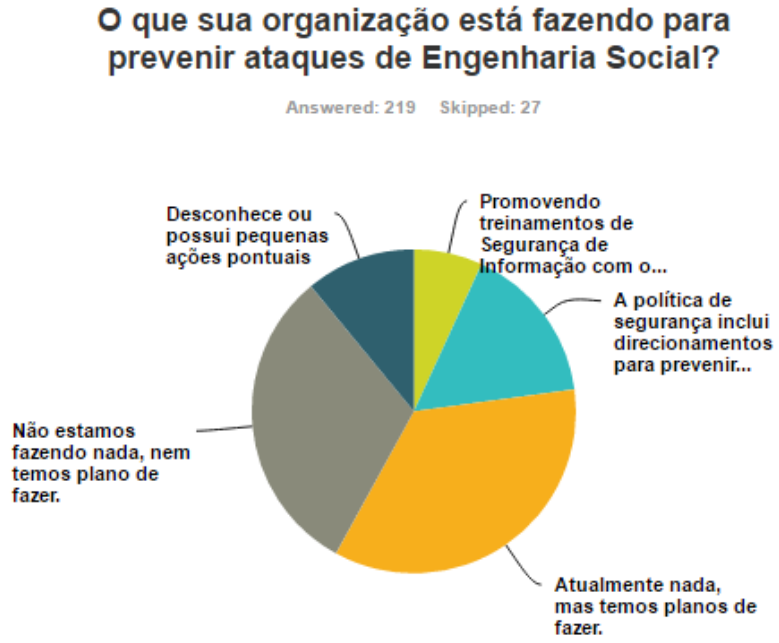
Gráfico 16 – Percentual de pessoal da empresa mais suscetível a ataques



Answer Choices	Responses	
Novos empregados	49.77%	110
Terceirizados	21.27%	47
Assistentes Executivos	10.41%	23
Pessoal de TI	4.52%	10
Alta diretoria	14.03%	31
Total		221

Fonte: Autor

Gráfico 17 – Percentual de ações para prevenção de ataques de engenharia social



Answer Choices	Responses
Promovendo treinamentos de Segurança de Informação com os empregados.	6.85% 15
A política de segurança inclui direcionamentos para prevenir ataques de Engenharia Social.	15.98% 35
Atualmente nada, mas temos planos de fazer.	35.16% 77
Não estamos fazendo nada, nem temos plano de fazer.	31.05% 68
Desconhece ou possui pequenas ações pontuais Responses	10.96% 24
Total	219

Fonte: Autor

O percentual de ações para prevenção contra os ataques de engenharia social é exposto no gráfico 17 acima. Observa-se que 15,9% reportam que incluem direcionamentos para a prevenção de ataques de engenharia social, ao passo que apenas 6,85% reportaram que sua empresa promove treinamentos de Segurança de Informação com os empregados.

O gráfico nos mostra que um percentual muito grande de respondentes que não está fazendo nada ou não tem planos de fazer para a prevenção de ataques, 35,1% não está fazendo nada atualmente, mas pretende fazer algo, 31% não possui qualquer plano de prevenção, tampouco planos de fazer algo e 10,9% desconhece a existência de algum planejamento.

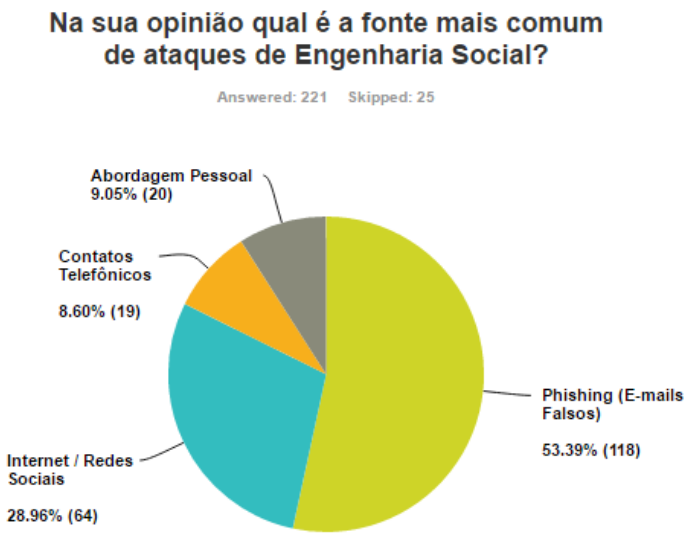
Observa-se que em um contexto macro, o percentual de 77% de pessoas que não promove nenhuma ação de prevenção ou desconhece tal, é alto.

De acordo com, o maior erro que as pessoas cometem quando pensam em proteção contra a engenharia social é pensar somente em conscientização de equipe, que é a primeira e mais importante camada de defesa, entretanto, confiar somente neste mecanismo de proteção é uma estratégia de alto risco. Para uma prevenção eficaz é necessário combinar camadas de conscientização de equipe com proteção sistêmica.

No quesito que trata sobre os tipos de ataque, os respondentes consideram que a maior fonte de ataques de engenharia social é o Phishing, com 53,3% de pessoas que o consideram a forma mais comum, seguido da Internet e Redes Sociais (28,9%), Abordagem pessoal (9,05%) e Contatos Telefônicos (8,6%).

O gráfico 18 corrobora com o relatório da Symantec, que estima que existiam cerca de 190 bilhões de e-mails em circulação por dia em 2015 com previsão de 4% ao final de 2016. Cada usuário recebe em média 42 e-mails por dia, e cada vez mais pessoas leem e-mails em dispositivos móveis. Para cibercriminosos , que visam alcançar o maior número de pessoas eletronicamente, o email é ainda a maneira favorecida de fazê-lo (SYMANTEC CORPORATION, 2016).

Gráfico 18 – Fontes de ataques de engenharia social



Answer Choices	Responses	
Phishing (E-mails Falsos)	53.39%	118
Internet / Redes Sociais	28.96%	64
Contatos Telefônicos	8.60%	19
Abordagem Pessoal	9.05%	20
Total		221

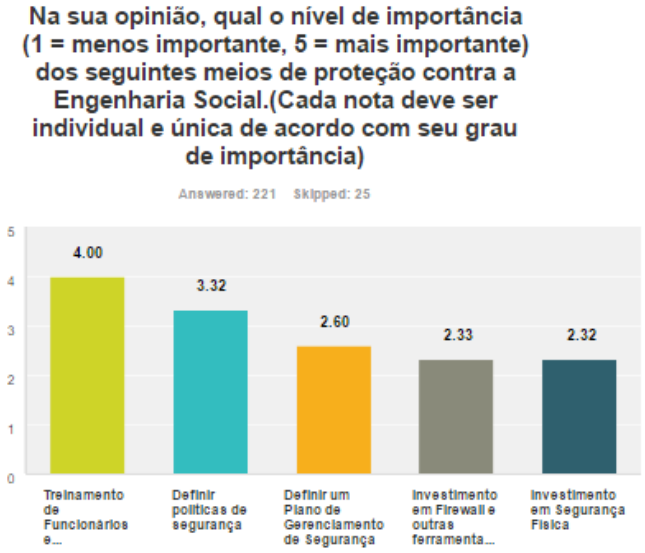
Fonte: Autor

De acordo com pesquisa da Kaspersky Lab, 22% dos golpes de phishing que tem como alvo o Facebook ,mais de 35% está relacionado a sites falsos se fazendo passar por redes sociais verdadeiras (STERN, 2015).

Na questão que trata dos meios de proteção contra ataques de engenharia social, percebe-se que a maioria dos respondentes possui consciência que é necessário investir em treinamento de funcionários e terceirizados. O gráfico abaixo atribui uma pontuação baseda em uma média ponderada aos itens estudados, desta forma, os respondentes consideraram o Treinamento de Funcionários e Tercerizados como o item de proteção contre engenharia social mais importante para a empresa.

Definir políticas de segurança é o segundo item mais importante na proteção contra engenheiros sociais, seguido por definição de planos de gerenciamento de segurança e, por último, investimentos em equipamentos e em segurança física.

Gráfico 19 – Meios de proteção por ordem de importância

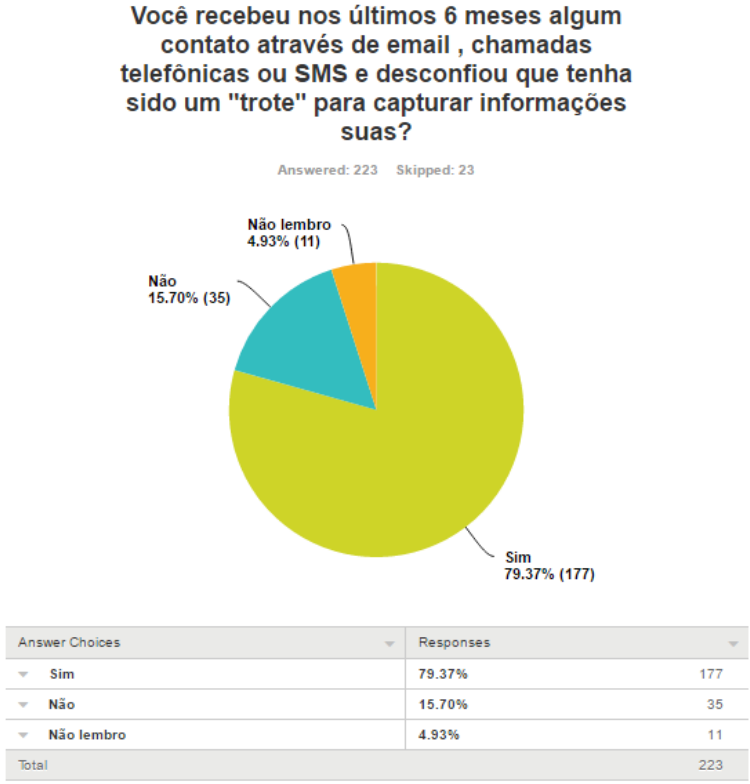


	5	4	3	2	1	Total	Score
Treinamento de Funcionários e Terceirizados	49.3% 101	21.5% 44	14.1% 29	10.7% 22	4.4% 9	205	4.00
Definir políticas de segurança	17.8% 35	32.0% 63	24.9% 49	15.7% 31	9.6% 19	197	3.32
Definir um Plano de Gerenciamento de Segurança	8.8% 19	18.0% 39	22.6% 49	25.8% 56	24.9% 54	217	2.60
Investimento em Firewall e outras ferramentas de segurança	7.2% 14	11.3% 22	17.4% 34	35.4% 69	28.7% 56	195	2.33
Investimento em Segurança Física	9.9% 19	11.5% 22	20.8% 40	16.7% 32	41.1% 79	192	2.32

Fonte: Autor

No quesito que trata sobre a percepção de ataques através de SMS, foi constatado que a maioria dos respondentes (79,3%) recebeu algum tipo de contato por email, SMS ou chamadas telefônicas para capturar seus dados e 15% dos respondentes afirma que não recebeu qualquer contato. 4,9% não se lembram de algum contato que tenham desconfiado ser um ataque para capturar suas informações, conforme gráfico abaixo:

Gráfico 20 – Percentual de ataques nos últimos meses

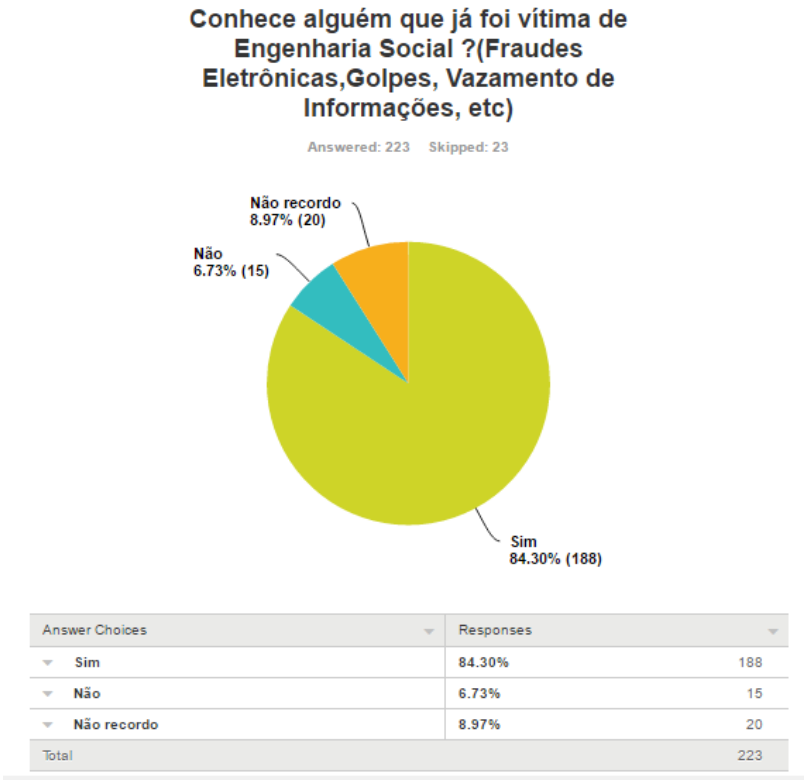


Answer Choices	Responses	
Sim	79.37%	177
Não	15.70%	35
Não lembro	4.93%	11
Total		223

Fonte: Autor

É perceptível o grande número de pessoas que conhece alguém que já foi vítima de ataques de engenharia social. 84,3% dos respondentes afirma conhecer alguém que já foi vítima de ataques de engenharia social sob forma de fraudes eletrônicas, golpes ou afins. Apenas 6,7% dos respondentes afirma não conhecer e 8,9% não se recorda de conhecer alguém vítima de golpe. Conforme gráfico abaixo:

Gráfico 21 – Percentual de conhecimento de vítimas de engenharia social

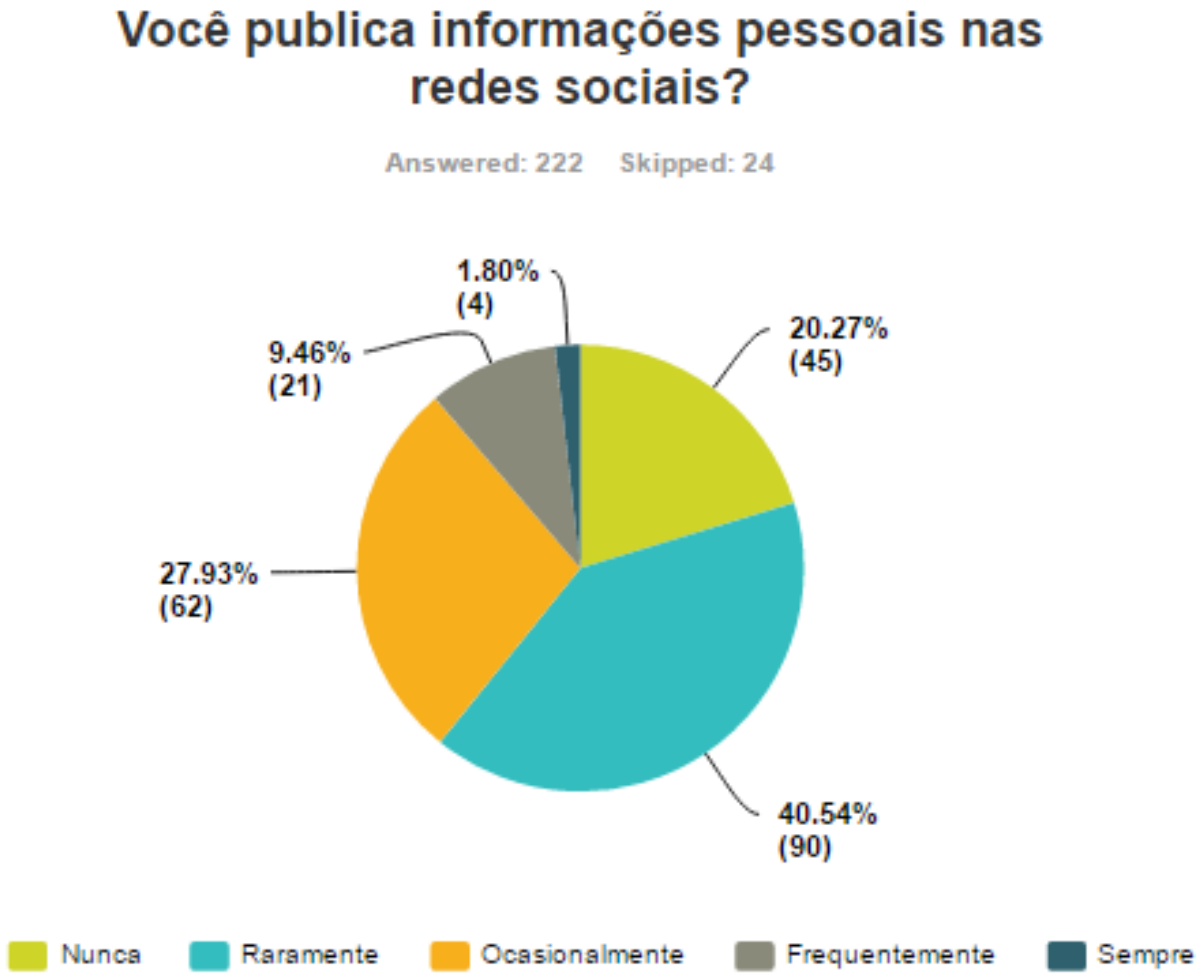


Answer Choices	Responses	
Sim	84.30%	188
Não	6.73%	15
Não recordo	8.97%	20
Total		223

Fonte: Autor

De acordo com, um estudo da empresa de segurança cibernética Agari revela que mais de 200 líderes de segurança respondentes nos Estados Unidos, 60% dizem que suas organizações foram ou podem ter sido vítimas de pelo menos um ataque de engenharia social no ano passado, e 65% dos que foram atacados dizem que as credenciais dos funcionários foram comprometidas como resultado.

Gráfico 22 – Percentual de respondentes que publicam informações em redes sociais

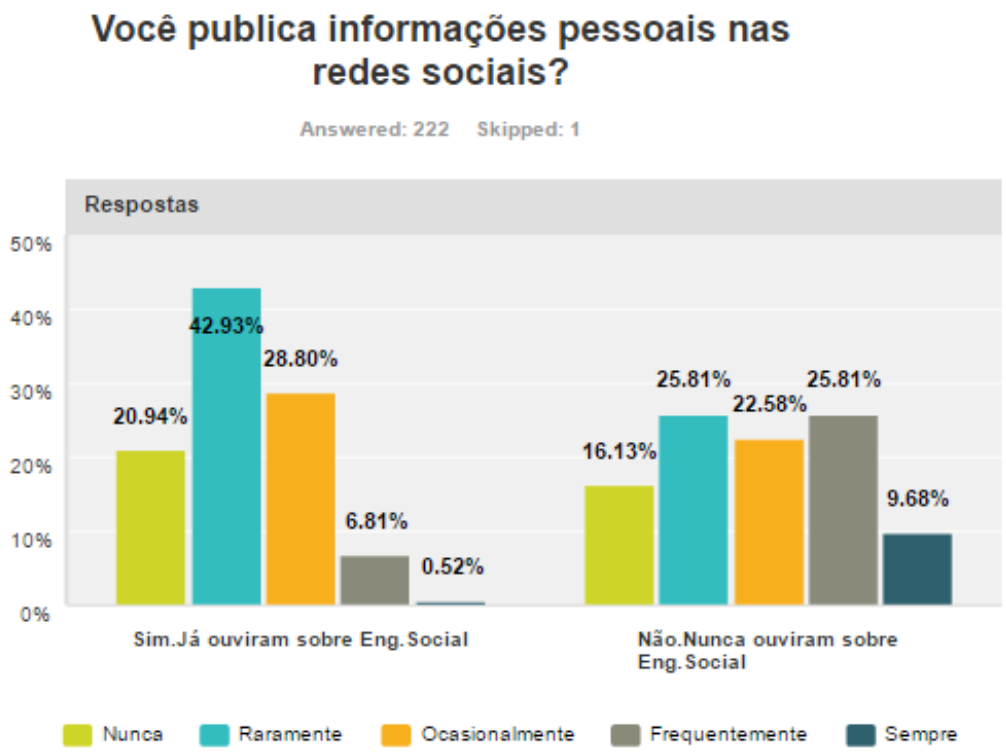


Fonte: Autor

Conforme exposto no gráfico 22, 20,2% dos respondentes nunca publica informações em redes sociais, 40,5% informou que raramente publicam informações pessoais em redes sociais, 27,9% dos respondentes ocasionalmente fazem publicação de dados pessoais e 11,2% informam que frequentemente ou sempre publicam informações pessoais nas redes sociais.

Para um Engenheiro Social, a exposição de informações facilita tanto a aproximação com o usuário quanto o uso indevido destas informações para a construção de perfis falsos, chantagens, sequestros, ou até mesmo a manipulação e influência para a transmissão de informações sigilosas e importantes, seja para a pessoa ou para a organização (HADNAGY, 2011).

Gráfico 23 – Conhecimento de engenharia social x Frequência de publicação de informações em redes sociais



Fonte: Autor

Ante o exposto, foi feita uma comparação entre respondentes que informaram que já ouviram ou não falar sobre o termo ”engenharia social“ com os que responderam a questão que trata sobre a publicação de informações pessoais em redes sociais.

Pode-se constatar que, das pessoas que informaram que já ouviram falar de engenharia social, 42,9% raramente publicam informações pessoais em redes sociais, ao passo que esse número cai para 26,8%, demonstrando uma variação de 37,5%.

Quando os respondentes desconhecem o assunto, a frequencia dos que publicam informações frequentemente nas redes sociais aumenta para 26,8%.Comparando com os que possuem conhecimento sobre engenharia social esse número reduz para 6,8%, isso equivale a uma variação percentual negativa de 74,6%.

A maior diferença percebe-se entre as pessoas que sempre publicam suas informações na rede social. Entre aqueles que conhecem sobre engenharia social, há o baixo percentual de 0,52%, ao passo que aqueles que desconhecem o assunto atingem o patamar de 9,6%, o que equivale a uma diferença de 1.761,5%.

Esse comparativo serve para demonstrar que a informação é uma das principais armas contra ataques de engenharia social.

Segundo Mann (2008),desenvolver uma cultura onde as informações são compartilhadas apenas quando for estritamente necessário, é um bom ponto de partida para manter longe a atenção dos agressores.

5 CONSIDERAÇÕES E TRABALHOS FUTUROS

Para finalizar o trabalho, este capítulo revisará os objetivos propostos, mostrando as conclusões finais e trabalhos futuros.

5.1 Resolução dos Pontos Propostos

A Segurança da Informação é seriamente ameaçada pelos ataques de engenharia social. Funcionários desprevenidos tornam-se alvos fáceis, explorados para fornecer informações ou acesso a sistemas. Esse trabalho apresentou as características dos ataques de engenharia social, suas estratégias e técnicas, além de demonstrar as abordagens de defesa contra os mesmos.

O estudo apresentou dados que confirmam as estatísticas do mercado quanto a incidência de ataques de engenharia social e o quanto as empresas conhecem sobre esses ataques.

Não foi possível efetuar um ataque real de engenharia social sobre as pessoas envolvidas nesse trabalho, pois além de ser necessária a anuência de gestores de qualquer uma das organizações, não se tem conhecimento das implicações legais de tal ação, bem como não é escopo do trabalho.

Foi investigado o conhecimento dos respondentes sobre ataques de engenharia social, suas ações em redes sociais e procedimentos de segurança em seus ambientes de trabalho.

Ante o exposto, observa-se que não é prioridade das empresas tratar de assuntos relacionados ao fator humano da segurança da informação, pois grande parte ainda acha que isso é um problema exclusivo da área de Tecnologia da Informação. Essa pesquisa defende a idéia que ataques de engenharia social é um problema de todos os usuários da organização, do nível mais baixo até o alto escalão, que possui a principal tarefa de investir em treinamento e conscientização sobre as questões de segurança cibernética. A consciência da segurança é um forte aliado à visão técnica de hardwares e softwares para o combate ao crime cinernético.

A divulgação de informações em redes sociais é algo que deve ser observado com muita atenção. As empresas estão cada vez mais inseridas nos conceitos de *Home-Office*, BYOD ou Internet das Coisas, quando uma informação pessoal é inserida em mídias sociais isso pode se tornar uma séria ameaça à sua empresa.

O presente trabalho propôs o seguinte objetivo:

- Determinar como os usuários de TI, gestores ou não, percebem a influência da engenharia social em suas organizações e qual o potencial de vulnerabilidade dessa influência.

E objetivos secundários que cumprem o objetivo proposto ao serem atendidos, que são :

- Investigar aspectos de Segurança da Informação em ambientes corporativos;
- Identificar as técnicas utilizadas em ataques de engenharia social e métodos de defesa;
- Analisar o conhecimento de empregados acerca de Segurança da Informação e ataques de engenharia social;
- Identificar as vulnerabilidades do fator humano que são explorados por ações de engenharia social;
- Sugerir ações para mitigar o risco de ataques de engenharia social às empresas.

Realizou-se uma pesquisa bilbiográfica com vários documentos do meio acadêmico e corporativo. Papers e relatórios técnicos foram subsidiados com um questionário aplicado com uma população de usuários de TI - espalhados em todas as regiões do país - para cumprir os objetivos supracitados. Através dos conhecimentos obtidos com a base teórica e os dados do questionário foi possível verificar como o ambiente corporativo trata a Segurança da Informação.

Foram identificadas as técnicas mais comuns de ataques de engenharia social e o conhecimento que os empregados possuem sobre engenharia social, comprovando a necessidade primordial de treinamentos e aplicação de uma política de conscientização a todos os colaboradores da empresa.

Sugestões de ações para mitigar o risco de ataques às empresas deram-se em função das respostas obtidas com o questionário, bem como o uso de relatórios do meio corporativo, que forneceram informações do cotidiano empresarial que muitas vezes não são encontradas em um perfil apenas acadêmico de estudo.

5.2 Considerações Finais

A engenharia social, é uma grande preocupação dos profissionais de Segurança da Informação. Para uma boa gestão de segurança é necessário que os responsáveis, conheçam as práticas de segurança, bem como acompanhar a evolução da tecnologia e das formas de ataques.

Nesta pesquisa foi possível confirmar que empresas especializadas em segurança da informaçãos relatam que ataques de engenharia social utilizando *phishing* ou outra técnica, obtém um grande índice de sucesso em suas tentativas. As tecnologias de segurança como firewalls, antivírus e filtros de e-mail dificultam esses ataques, isentando as pessoas do processo de tomada de decisão. Entretanto, o único meio verdadeiramente efetivo de amenizar a ameaça da engenharia social é usar a conscientização para a segurança juntamente com políticas de segurança que definem as principais regras para o comportamento do empregado, junto com sua educação e treinamento.

As organizações devem lutar contra ataques de engenharia social, estabelecendo políticas e procedimentos que definem papéis e responsabilidades para todos os usuários e não apenas para o pessoal de segurança. Enquanto as soluções técnicas de software e hardware são importantes no processo de Segurança da Informação, a engenharia social ataca o elo mais fraco: os seres humanos. Visto que há uma interação com todos os sistemas, existe uma vulnerabilidade geral e as melhores soluções de defesa devem incluir camadas técnicas que envolvem controles de acesso, antivirus, firewalls, etc. e camadas de gerenciamento de políticas de segurança, conscientização de usuários e respostas a incidentes.

As organizações devem reforçar sua postura de segurança não apenas de forma técnica, mas com uma perspectiva humana da segurança.

5.3 Trabalhos Futuros

Muitos aspectos da segurança envolvem a tecnologia, então é fácil para queos empregados achem que os problemas são resolvidos com a instalação de *Firewalls*[21] ou outras tecnologias. Um dos objetivos principais do treinamento deve ser a criação em cada empregado da consciência de que eles são responsáveis por uma proteção inicial à segurança geral da organização.

O presente trabalho tem a motivação futura de desenvolver um programa de treinamento voltado para a conscientização de Segurança de Informação voltado para a proteção contra ataques de engenharia social, sensibilizando as pessoas que o fator humano é peça fundamental no combate a essa ameaça. Essa abordagem é voltada para o público sem habilidades técnicas em tecnologia, pois tornam-se os alvos mais fáceis de um Engenheiro Social.

Este trabalho poderá ter novos desdobramentos caso estudos futuros abordem

[21] Firewall é uma solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas. Disponível em :https://www.infowester.com/firewall.php. Acesso em:02/02/2017

pontos como:

- Criação de um modelo de framework para aplicação de treinamento de pessoal em Segurança da Informação, voltado para a engenharia social ;
- Refinar e aprimorar o questionário, bem como sua forma de divulgação e coleta de dados, para que assim, haja uma análise mais abrangente dos respondentes com relação à localização geográfica. Esta investigação permitiria identificar as diferenças comparando com os resultados atualmente apurados;
- Desenvolvimento de um conjunto de políticas de segurança voltadas exclusivamente para ataques de engenharia social;
- Simulação de um ataque de engenharia social a instituições públicas e privadas para validar as políticas de segurança implantadas e identificar as vulnerabilidades, provavelmente os resultados seriam mais próximos da realidade com a simulação de ataques reais;
- Uma pesquisa conjunta com a área de Psicologia, a fim de avaliar aspectos comportamentais que envolvem a engenharia social, com o intuito de prover ferramentas para melhor identificar e mitigar os ataques de engenharia social.

Referências

ABNT. *Tecnologia da informação –Técnicas de segurança – Código de prática para controles de segurança* : ABNT NBR ISO/IEC 27002:2013. 1. ed. Rio de Janeiro, 2013.

ALENCAR, Gliner Dias. *Estratégias para mitigação de ameaças internas*. 2010. 137 p. Dissertação (Ciência da Computação) — Universidade Federal de Pernambuco - UFPE, Pernambuco.

ALEXANDER, Michael. *Methods for Understanding and Reducing Social Engineering Attacks*. [S.l.], 2016. Disponível em: <https://www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972>.

ALLEN, Malcolm. *Social Engineering*: A Means To Violate A Computer System. 2007. Disponível em: <https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529>. Acesso em: 17/01/2017.

ALVES, Leonardo Lacerda. *Problema de pesquisa não é o problema – TCC o q?* 2015. Disponível em: <http://lacerda.eti.br/2015/02/problema-de-pesquisa-nao-e-o-problema-tcc-o-q/>. Acesso em: 15/01/2017.

ANGELONI, Maria Terezinha. *Organizações do conhecimento*: infra-estrutura, pessoas e tecnologias. . São Paulo: Saraiva, 2003.

ASHFORD, Warwick. *Social engineering is top hacking method, survey shows*. 2016. Disponível em: <http://www.computerweekly.com/news/4500272941/Social-engineering-is-top-hacking-method-survey-shows>. Acesso em: 02/02/2017.

BHAGYAVATI, B.. Social Engineering. In: COLARICK, Andrew M..; JANCZEWSKI, Lech J.. (Ed.). *Cyber Warfare and Cyber Terrorism*. New York: Information Science Reference, 2008. p. 182 – 190. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.670.9033&rep=rep1&type=pdf>.

CASTELLS, Manuel. *A Era da Informação*: economia, sociedade e cultura. São Paulo: Paz e terra, 1999.

CERVO, Amado Luiz.; BERVIAN, Pedro Alcino. *Metodologia científica.* . 5. ed. [S.l.]: Prentice Hall, 2002.

CHANTLER, Alan N..; BROADHURST, Roderic. Social Engineering and Crime Prevention in Cyberspace. Draft Technical Report for the Australian Institute of Criminology - Futures of High Tech Crime Project. 2006. Disponível em: <http://eprints.qut.edu.au/7526/>.

CHENGALUR-SMITH, Abraham. An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, n. 32, p. 183 – 186, 2010. Disponível em: <https://www.researchgate.net/publication/248493666_An_overview_of_social_engineering_malware_Trends_tactics_and_implications>.

CHIAVENATO, Idalberto. *Comportamento Organizacional*: a dinâmica do sucesso das organizações. 2. ed. Rio de Janeiro: Elsevier, 2005.

CHITREY, Anubhav.; SINGH, Dharmendra.; SINGH, Vrijendra. A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model . *International Journal of Information and Network Security*, v. 1, n. 2, p. 45 – 53, 2012.

COSTA, Veridiana Alves de Sousa Ferreira.; SILVA, Maicon Herverton Lino Ferreira da. *O fator humano como pilar da Segurança da Informação*: uma proposta alternativa. 2009. IX Jornada de Ensino Pesquisa e Extensão (JEPEX) da UFRPE. Disponível em: <http://www.eventosufrpe.com.br/jepex2009/cd/resumos/R0052-3.pdf>. Acesso em: 20/12/2016.

DANTAS, Marcos. *A lógica do capital informação*: monopólio e monopolização dos fragmentos num mundo de comunicações globais. Rio de Janeiro: Contraponto, 1996.

DIAS, Guilherme Ataíde. *Dado, informação e conhecimento* . 2014. Vídeo. Disponível em: <https://www.youtube.com/watch?v=lC52aRxI-_s>.

DRESCH, Aline.; LACERDA, Daniel Pacheco.; ANTUNES JÚNIOR, José Antonio Valle. *Design science research*: método de pesquisa para avanço da ciência e tecnologia. Porto Alegre: Bookman Editora, 2015. ISBN 978-85-8260-298-0.

DRUCKER, Peter F. *Landmarks of Tomorrow*: A Report on the New. [S.l.]: Transaction Publishers, 2011.

FERNANDES, Jorge Henrique.; BORGES, Díbio Leandro. Pesquisa de Estudo de Caso em Gestão da Segurança da Informação. Curso de Especialização em Gestão da Segurança da Informação e Comunicações CEGSIC 2012/2014. Campus Universitário Darcy Ribeiro: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2012. Acesso em: 01/11/2016.

FERNANDES, Jorge Henrique Cabral. *Ciclo de vida da Informação*. 2013. Vídeo. Disponível em: <https://vimeo.com/7179114>. Acesso em: 01/11/2016.

FERREIRA, Fernando Nicolau Freitas.; ARAÚJO, Márcio Tadeu de. *Política de Segurança da Informação - Guia Prático para Elaboração e Implementação*. 2. ed. Rio de Janeiro: Ciência Moderna, 2008.

FONSECA, Paula Fernanda. *FONSECA, Paula F. Gestão de Segurança da Informação*:. 2009. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/PaulaFernandaFonseca-Artigo.pdf>. Acesso em: 25/01/2017.

FONTES, Edison. *Políticas e Normas para a Segurança da Informação*. 1. ed. Rio de Janeiro: Brasport, 2012. ISBN 978-85-7452-515-0.

GHAFIR, Ibrahim. et al. Social Engineering Attack Strategies and Defence Approaches. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud*, v. 1, n. 1, p. 15 – 19, 2016. Disponível em: <http://ieeexplore.ieee.org/document/7575856/>.

GIL, Antonio Carlos. *Métodos e técnicas de pesquisa social*. 6. ed. São Paulo: Atlas, 2008.

GOODRICH, Michael T..; TAMASSIA, Roberto. *Introdução à Segurança de Computadores*. 1. ed. Porto Alegre: Bookman, 2013. ISBN 978-85-407-0192-2.

GUPTA, Surbhi.; SINGHAL, Abhishek.; KAPOOR, Akanksha. A Literature Survey on Social Engineering Attacks: Phishing Attack. In: *2016 International Conference on Computing, Communication and Automation (ICCCA)*. [s.n.], 2016. p. 537 – 540. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7813778&isnumber=7813678>.

HADNAGY, Christopher. *The Art of Human Hacking*. 1. ed. Indianapolis: Wiley Publishing, Inc, 2011.

HADNAGY, Christopher. *The Social Engineering Framework - Attack Vectors*. 2017. Disponível em: <http://www.social-engineer.org/framework/attack-vectors/attack-cycle/>. Acesso em: 20/01/2017.

HADNAGY, Christopher. *The Social Engineering Framework - Pretexting*. 2017. Disponível em: <http://www.social-engineer.org/framework/influencing-others/pretexting/>.

HEIKKINEN, Seppo. *Social engineering in the world of emerging communication technologies*. 2010. 1 – 10 p. Disponível em: <http://www.cs.tut.fi/~sheikki/docs/WWRF-Heikkinen-SocEng.pdf>. Acesso em: 19/01/2017.

INC., VERISIGN. *Tendências e ameaças técnicas 2016 Verisign iDefense® Security Intelligence Services*. [S.l.], 2016. Disponível em: <https://www.verisign.com/assets/report-cyber-threats-2016_pt_BR.pdf>.

INSTITUTE, Infosec. *Spear Phishing*: Real Life Examples. 2016. Disponível em: <http://resources.infosecinstitute.com/spear-phishing-real-life-examples/>. Acesso em: 13/02/2017.

INTERPOL. *Internacional Police Criminal Organization*. 2016. Disponível em: <https://www.interpol.int/Crime-areas/Cybercrime/The-threats>. Acesso em: 26/12/2016.

JOHANSON, Jesper. *Island Hopping*: The Infectious Allure of Vendor Swag. . 2008. Disponível em: <https://technet.microsoft.com/enus/magazine/2008.01.securitywatch.aspx>.

KROLL. *GLOBAL FRAUD & RISK REPORT Building Resilience in a Volatile World*. [S.l.], 2016.

KUMAR, Anshul.; CHAUDHARY, Mansi.; KUMAR, Nagresh. Social Engineering Threats and Awareness: A Survey . *European Journal of Advances in Engineering and Technology*, India, v. 2, n. 11, p. 15 – 19, 2015. ISSN 2394 - 658X. Disponível em: <http://www.ejaet.com/PDF/2-11/EJAET-2-11-15-19.pdf>.

LAKATOS, Eva Maria.; MARCONI, Marina de Andrade. *Fundamentos de metodologia científica*. São Paulo: Atlas, 2003. ISBN 978-85-224-3397-1.

LINS, Diego. *Engenharia Social #4 - O Lixo é Rico & Pessoas Descontentes*. 2016. Vídeo. Disponível em: <https://www.youtube.com/watch?v=Gd43r_K5RME>. Acesso em: 16/02/2017.

LYNETT, Mike. *A History of Information Security From Past to Present*. 2015. Disponível em: <http://blog.mesltd.ca/a-history-of-information-security-from-past-to-present>. Acesso em: 20/06/2016.

MANDARINO JÚNIOR, Raphael. *Segurança e Defesa do espaço cibernético brasileiro*. 1. ed. Recife: Cubzac, 2010.

MANN, Ian. *Hacking the human*: social engineering techniques and security countermeasures. Aldershot, England ; Burlington, VT: Gower, 2008. ISBN 978-0-566-08773-8.

MARCIANO, João Luiz.; LIMA-MARQUES, Mamede. O enfoque social da segurança da informação. *Ciência da Informação*, v. 35, p. 89 – 98, 2006. ISSN 0100-1965.

MEIRA, Silvio Lemos. *Novos negócios inovadores de crescimento empreendedor no Brasil*. Rio de Janeiro: Casa da Palavra. 416 p.

MICHAELIS. *Moderno Dicionário da Lingua Portuguesa*. 2016. Online. Disponível em: <http://michaelis.uol.com.br>. Acesso em: 10/10/2016.

MITNICK, Kevin D..; SIMON, William L. *A arte de enganar*. 1. ed. São Paulo: Makron Books, 2003. ISBN 85-346-1516-0.

MITNICK, Kevin D..; SIMON, William L.. *A arte de invadir*: as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos . São Paulo - SP: Pearson Prentice Hall, 2005.

MOUTON, Francois. et al. Social engineering attack framework. IEEE, Johannesburg, p. 1 – 9, Agosto 2014. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6950510>. Acesso em: 21/11/2016.

NAKAMURA, Emilio Tissato.; GEUS, Paulo Lício de. *Segurança de Redes em ambientes cooperativos*. 1. ed. São Paulo: Novatec Editora, 2007. ISBN 978-85-7522-136-5.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY-NIST. *An Introduction to Computer Security*: The nist handbook. Special publication 800-12. [S.l.], 1995. Disponível em: <http://www.davidsalomon.name/CompSec/auxiliary/handbook.pdf>.

PRODANOV, Cleber Cristiano.; FREITAS, Ernani Cesar de. *Metodologia do Trabalho Científico*: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. [S.l.]: Editora Feevale, 2013.

PROOFPOINT. *The Human Factor 2016 Report*. [S.l.], 2016. Disponível em: <https://www.proofpoint.com/sites/default/files/human-factor-report-2016.pdf>.

ROUSE, Margaret. *Spear Phishing*. 2011. Disponível em: <http://searchsecurity.techtarget.com/definition/spear-phishing>. Acesso em: 12/02/2017.

SANTARCANGELO, Michael. *Why the definition of security awareness matters*. 2010. Disponível em: <https://securitycatalyst.com/why-the-definition-of-security-awareness-matters/>. Acesso em: 31/01/2017.

SCHNEIER, Bruce. *Beyond fear* : thinking sensibly about security in an uncertain world. 1. ed. New York: Copernicus Books, 2003. ISBN 0-387-02620-7.

SCHRÖEDER, Christine da Silva.; ANTUNES, Mônica da Pieve.; OLIVEIRA, Julcimar Luiz de. Gestão do Conhecimento Corporativo: Um Fator de Competitividade para as Organizações. *Revista de Administração IMED*, v. 1, n. 1, p. 29 – 53, dezembro 2011. ISSN 2237-7956. Disponível em: <https://seer.imed.edu.br/index.php/raimed/article/view/69/67>.

SILVA, Edna Lúcia Da.; MENEZES, Estera Muszkat. *Metodologia da pesquisa e elaboração de dissertação*. 2005. Disponível em: <https://projetos.inf.ufsc.br/arquivos/Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes_4ed.pdf>. Acesso em: 25/09/2016.

SILVA, Francisco José Albino Faria Castro e. *Classificação Taxonómica dos Ataques de Engenharia Social. Caracterização da Problemática da Segurança de Informação em Portugal relativamente à Engenharia Social*. 2013. 132 p. Dissertação (Segurança dos Sistemas de Informação) — Universidade Católica Portuguesa, Lisboa. Disponível em: <http://repositorio.ucp.pt/bitstream/10400.14/15690/1/TesedeMestrado-EngenhariaSocial.pdf>.

STALLINGS, William. *Criptografia e segurança de redes - Princípios e práticas*. 4ª edição. ed. São Paulo SP: Pearson Education do Brasil, 2008.

STERN, Aaron. *Cuidado com as redes sociais*: Facebook é o maior portal de phishing. 2015. Disponível em: <https://blog.kaspersky.com.br/cuidado-com-as-redes-sociais-facebook-e-o-maior-portal-de-phising/3301/>.

SYMANTEC. *A brief history of internet security*. 2009. Disponível em: <https://www.scmagazine.com/a-brief-history-of-internet-security/article/556389/>. Acesso em: 17/11/2016.

SYMANTEC CORPORATION. *ISTR - Internet Security Threat Report*. Symantec Corporation World Headquarters 350 Ellis Street Mountain View, CA 94043 USA, 2016. Disponível em: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>.

TOFLER, Alvin.; TOFLER, Heidi. *Guerra e Anti-Guerra*. Lisboa: Livros do Brasil, 1994.

VANACO, Adriane. *A História da Computação e da Segurança de Informação - Parte 1*. 2010. Disponível em: <http://www.oarquivo.com.br/temas-polemicos/historia/425-a-historia-da-computacao-e-da-seguranca-de-informacao-parte-1.html>. Acesso em: 22/12/2016.

VAULT, Bank. *Definition of the Day*: Quid Pro Quo Attack. 2017. Disponível em: <https://www.bankvaultonline.com/knowledge-base/definition-of-the-day/definition-quid-pro-quo-attack/>. Acesso em: 13/02/2017.

VIEIRA, Sônia. *Como elaborar questionários*. 1. ed. São Paulo: Atlas, 2009.

Apêndices

Apêndice A

QUESTIONÁRIO DE PESQUISA

1. Apresentação

OLÁ ! SEI QUE SEU TEMPO É VALIOSO, MAS TENHO UM BRINDE BEM LEGAL AQUI E GOSTARIA DE ENVIAR A VOCÊ !!!

Meu nome é Francisco Henriques, sou aluno do Mestrado em Ciência da Computação da Universidade Federal de Pernambuco (UFPE).

O motivo dessa nossa interação é para falar de um problema cada vez mais frequente em nosso cotidiano. . . ataques de ENGENHARIA SOCIAL!

Engenharia Social é a manipulação de pessoas, enganando-as, para que forneçam informações ou executem uma ação (Mann,2011). O atacante utiliza técnicas psicológicas para a obtenção de confiança por parte da vítima, bem como pesquisa sobre o alvo em redes sociais e quaisquer técnicas para obter informações e violar a segurança da organização.

Convido você a participar dessa pesquisa, que tem como objetivo determinar como os usuários de sistemas de Informação percebem a influência da Engenharia Social em suas organizações e como o nivel de conhecimentos em Segurança da Informação auxilia no combate a essa ameaça. Sua ajuda será de grande importância para montarmos,juntos, um perfil dos ataques de Engenharia Social nas empresas e propor ações para mitigar essa ameaça.

Observações:

1)O seguinte questionário obedecerá a Política de Privacidade SurveyMonkey.

2) Dados para Contato: Francisco Henriques

fafh@cin.ufpe.br

Mestrando em Ciência da Computação

Orientador: Prof. Dr. Ruy Queiroz

Professor do Centro de Informática (Cin/UFPE)

3) Ao enviar o questionário respondido você concorrerá a 1 LIVRO, de sua preferência, até o valor de R$ 100,00 (Cem Reais). O sorteio será efetuado após a análise dos questionários enviados e o vencedor será contatado por e-mail. Esse brinde é uma forma de agradecimento por sua imensa colaboração.

A INFLUÊNCIA DA ENGENHARIA SOCIAL NO FATOR HUMANO DAS ORGANIZAÇÕES.

1. Você concorda com os termos acima?

Clicando em Sim, você concorda que está disposto a responder às perguntas deste questionário.

* Sim

* Não

2. Identificação do Entrevistado

* 2. Qual sua faixa etária?

18 a 25 anos

26 a 33 anos

34 a 41 anos

42 a 49 anos

50 anos ou acima

* 3. Em que estado você mora?

4. Qual o seu endereço de email ? (Necessário e-mail válido caso queira concorrer ao brinde.)

* 5. Qual seu último nível de escolaridade completo ?

1º Grau Completo (Fundamental)

2º Grau Completo (Ensino Médio)

Superior

Especialização

Mestrado

Doutorado

Pós-doutorado

* 6. Qual das seguintes opções melhor descreve a sua ocupação atual?

Ocupações de gestão

Ocupações de operações financeiras e comerciais

Ocupações na matemática e informática

Ocupações na engenharia e arquitetura

Ocupações nas ciências da vida, físicas e sociais

Ocupações no serviço social e comunitário

Ocupações jurídicas

Ocupações educacionais, de treinamento e bibliotecárias

Ocupações artísticas, de design, entretenimento, esportivas e de mídia

Ocupações na técnica e prática dos cuidados da saúde

Ocupações no serviço de proteção

Ocupações relacionadas ao serviço e preparação de alimentos

Ocupações na manutenção e limpeza de imóveis e instalações

Ocupações no serviço e cuidado pessoal

Ocupações relacionadas a vendas

Ocupações de apoio administrativo

Ocupações no florestamento, pesca e agropecuária

Ocupações na construção e extração

Ocupações de conserto, manutenção e instalação

Ocupações na produção

Ocupações no transporte e mudança de materiais

Gestor de TI

3. Identificação da Empresa

7. Qual das seguintes opções melhor descreve a área de ATUAÇÃO PRINCIPAL da sua empresa?

Agricultura

Alimentício e de bebidas

Automobilístico

Comércio e logística

Construção

Educação

Eletrônicos

Energia e extração

Entretenimento e Lazer

Governamental

Manufatura

Máquinas e moradia

ONGs

Publicidade e marketing

Saúde e farmacêutico

Seguros

Serviços de utilidade pública

Serviços financeiros

Serviços imobiliários

Tecnologia da informação

Telecomunicações

Transporte aéreo e indústria aeroespacial (incluindo defesa)

Transporte e entrega

Varejo e bens duráveis de consumo

8. Qual o setor de atuação de sua empresa?

Público

Privado

Economia Mista

4. Identificação da Empresa

9. De acordo com a tabela abaixo, classifique a empresa em que trabalha quanto ao porte:

Microempresa

Pequena empresa

Média empresa

Grande empresa

5. Conhecimentos sobre Segurança da Informação

Informações sobre o conhecimento que o entrevistado tem sobre conceitos de Segurança da Informação e como a empresa em que trabalha lida com estes conceitos.

10. Quanto possui de conhecimento do papel da Segurança da Informação em sua empresa?

Nenhum conhecimento

Pouco conhecimento

Conhecimento mediano

Bom conhecimento

Total conhecimento

11. Sua empresa possui alguma Política de Segurança de Informação e Comunicações (POSIC)?

Sim

Não

Não tenho certeza

12. Em caso afirmativo, essa política é divulgada para os funcionários?

Não é divulgada.

Sim. É divulgada em site / intranet da empresa, para quem tiver interesse em conhecer.

Sim. É formalizada , divulgada e é de obrigação de todos o conhecimento.

13. Quanto possui de conhecimento acerca das normas de Segurança da Informação relacionadas à sua atividade na empresa?

Nenhum conhecimento

Pouco conhecimento

Conhecimento mediano

Bom conhecimento

Total conhecimento

14. Conhece as informações que devem ser protegidas na empresa em que trabalha?

Nenhum conhecimento

Pouco conhecimento

Conhecimento mediano

Bom conhecimento

Total conhecimento

15. Sua empresa realiza treinamento de conscientização em Segurança da Informação para funcionários e parceiros de negócio?
Não existe política de treinamentos em Segurança da Informação

Existe projeto para realizar treinamentos em Segurança da Informação

Existe um processo definido e totalmente aplicado de treinamentos em Segurança da Informação

16. Você tem percepção que o assunto “Segurança da Informação” é debatido de forma estratégica na sua empresa?

Não.A empresa não dá a importância devida .

Não. Mas a empresa já possui planos para tratar o assunto.

Desconheço.

Sim. O assunto é debatido mas não sai do papel

Sim. É tratado com importância total.

6. Conhecimentos sobre Engenharia Social

* 17. Você já tinha ouvido falar no termo “Engenharia Social”?

Sim

Não

18. Qual o nível de consciência que você possui a respeito da potencial ameaça de ataques de Engenharia Social ? *

Nunca ouvi falar em Engenharia Social

Pouco consciente

Já ouvi falar mas não dou importância ao tema.

Muito consciente Totalmente consciente

19. Sua organização já sofreu algum ataque de Engenharia Social?

Sim

Não

Não tenho conhecimento.

20. Na sua opinião, qual a motivação por trás de ataques de Engenharia Social ?

Ganhos financeiros

Acesso a informações privilegiadas

Vantagem competitiva

Vingança Pessoal

Outro (especifique)

* 21. Na sua opinião, que tipo de pessoal é o mais suscetível a ataques de Engenharia Social?

Novos empregados

Terceirizados

Assistentes Executivos

Pessoal de TI Alta diretoria

22. O que sua organização está fazendo para prevenir ataques de Engenharia Social?

Promovendo treinamentos de Segurança de Informação com os empregados.

A política de segurança inclui direcionamentos para prevenir ataques de Engenharia Social.

Atualmente nada, mas temos planos de fazer.

Não estamos fazendo nada, nem temos plano de fazer.

Outro (especifique)

* 23. Na sua opinião qual é a fonte mais comum de ataques de Engenharia Social? Phishing (E-mails Falsos)

Internet / Redes Sociais

Contatos Telefônicos Abordagem Pessoal

24. Na sua opinião, qual o nível de importância (1 = menos importante, 5 = mais importante) dos seguintes meios de proteção contra a Engenharia Social.(Cada nota deve ser individual e única de acordo com seu grau de importância)

Treinamento de funcionários e terceirizados em Segurança da Informação

Definir Políticas de Segurança

Investimento em Firewalls e outras ferramentas de Segurança

Investimento em Segurança Física

Definir um Plano de Gerenciamento de Segurança

7. Conhecimentos sobre Engenharia Social

*25. Você recebeu nos últimos 6 meses algum contato através de email , chamadas telefônicas ou SMS e desconfiou que tenha sido um “trote” para capturar informações suas?

Sim

Não

Não lembro

*26. Conhece alguém que já foi vítima de Engenharia Social ?(Fraudes Eletrônicas,Golpes, Vazamento de Informações, etc) *

Sim

Não

* 27. Você publica informações pessoais nas redes sociais?

Nunca Raramente Ocasionalmente Frequentemente Sempre