UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA – DAELN
CURSO DE ESPECIALIZAÇÃO EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

DANIEL PITANGA DOS SANTOS

A ENGENHARIA SOCIAL NO BRASIL E SEUS RISCOS

MONOGRAFIA DE ESPECIALIZAÇÃO

Curitiba - PR

2016

DANIEL PITANGA DOS SANTOS

A ENGENHARIA SOCIAL NO BRASIL E SEUS RISCOS

Trabalho de Conclusão de Curso apresentado na Universidade Tecnológica Federal do Paraná como requisito básico para a conclusão do Curso de Especialização em Gestão da Tecnologia da Informação e Comunicação.

Orientador Prof. Eng. Christian Mendes

Curitiba – PR
2016

DANIEL PITANGA DOS SANTOS

A ENGENHARIA SOCIAL NO BRASIL E SEUS RISCOS

Esta monografia foi apresentada às 17 horas, do dia 11 de novembro de 2016, como requisito parcial para obtenção do título de **ESPECIALISTA EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**, do Programa de Pós-Graduação da Universidade Tecnológica Federal do Paraná. O estudante foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho: **APROVADO**.

_____

Prof. Msc. Alexandre J. Miziara
Coordenador de Curso
Departamento Acadêmico de Eletrônica

BANCA EXAMINADORA

Curitiba, ____ de _____ 2016

_____

Prof. Msc. Alexandre J. Miziara
Coordenador do Curso

_____

Prof. Eng. Christian Mendes
Orientador – UTFPR

“A Folha de Aprovação assinada encontra-se na Coordenação do Curso”

AGRADECIMENTOS

Agradeço e glorifico a Deus, primeiramente, pela sua grande bondade e amor em permitir mais essa conquista em minha vida, dando-me sempre força e capacidade para realizar os meus objetivos, porque dEle, por Ele e para Ele são todas as coisas.

Ao meu orientador, pela ajuda desde o nascimento da ideia até o desenvolvimento desse trabalho da melhor forma possível, com o seu profundo domínio e conhecimento dos temas, e as suas dicas, sugestões e auxílio diretivo, fizeram com que esse projeto fosse realizável.

À minha família que esteve sempre me apoiando e incentivando, meus pais que transmitiram em suas palavras de sabedoria o conforto e atenção, e acompanharam esse processo ao longo do tempo.

À minha linda e amada noiva Thaís que desde o começo me apoiou com o seu amor e paciência, e esteve comigo enfrentando todas as dificuldades encontradas pelo caminho, incentivando-me a cada etapa concluída, e fez o necessário para que essa conquista acontecesse, amo você! E aproveito para saudar minha filha que está chegando ao mundo em alguns dias, já te amamos, minha princesa, e esperamos ansiosos a sua chegada, essa conquista é para você também.

RESUMO

PITANGA DOS SANTOS, Daniel. A Engenharia Social no Brasil e seus riscos. 2016. x f. Monografia (Especialização em Gestão da Tecnologia da Informação e Comunicação) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2016.

Este projeto tem como ideal a busca de conhecimento em engenharia social, alertando sobre seus riscos, técnicas comumente utilizadas e formas de prevenção. O tema em questão, muitas vezes mitigado, é fundamental para o desenvolvimento de um sistema de segurança da informação útil e eficaz para pequenas, médias e grandes empresas. Atualmente pessoas mal-intencionadas utilizam técnicas de engenharia social ocasionando grandes prejuízos às organizações, as quais necessitam de maior aprofundamento sobre o tema e sua prevenção. A pesquisa realizada apresenta indícios que a maioria dos brasileiros necessita de melhores informações sobre o tema e de que forma se prevenir. Assim como, a necessidade de que as organizações estejam atentas a gravidade do impacto que as fraudes criadas, através do uso da engenharia social, podem causar em seus negócios e consequentemente aprimorar as políticas de segurança por elas utilizadas.

PALAVRAS CHAVE: Engenharia social, cultura organizacional, fraude, phishing, pharming, skimming, vishing, smishing, tailgating, shoulder surfer, clone, manipulação, segurança da informação, espionagem.

ABSTRACT

PITANGA, Daniel. A Engenharia Social no Brasil e seus riscos. 2016. x f. Monografia (Especialização em Gestão da Tecnologia da Informação e Comunicação) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2016.

This paper proposal has the ideal to aprimorate knowledgement in social engineering, alerting about the risks, showing used techniques and forms of prevention. The theme in question, sometimes mitigated, it is essential for developing an useful and efficient information security system been applied in small, medium or big organizations. Nowadays, people are using social engineering techniques causing hugest damages to organizations, making them search for more knowledgement and how to prevent themselves. This research presents that many of the Brazilian people needs to acquire better information about social engineering and how to prevent themselves. As well as, the necessity that the organizations must be alert to the impact that the frauds, created by using social engineering, may cause in their business and consequently to aprimorate the political of security.

Key words: Social Engineer, organizational culture, fraud, phishing, pharming, skimming, vishing, smishing, tailgating, shoulder surfer, clone, manipulation, security information, spy.

LISTA DE SIGLAS

TI – Tecnologia da Informação

PNL – Programação Neurolinguística

SMS – Short Message Service

URL – Uniform Resource Locator

CPF – Cadastro de Pessoa Física

RG – Registro Geral

RFID – Radio-Frequency IDentification

HTTPS – Hyper Text Transfer Protocol Secure

DNS – Domain Name Server

IP – Internet Protocol

ISP – Internet Server Provider

SET – Social Engineering Toolkit

DoS – Denial of Service

DNS – Domain Name Server

.txt – Formato de arquivos do tipo texto

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE GRÁFICOS

SUMÁRIO

1. INTRODUÇÃO

A engenharia social é uma crucial área tratada pela segurança da informação. Com o grande advento da tecnologia em praticamente todos os setores, pessoas mal-intencionadas buscam atingir o elo mais fraco na informática, em termos de segurança, o ser humano.

Informações são cruciais para o desenvolvimento dos negócios das mais diversas áreas das ciências, ocasionando, assim, uma supervalorização dessas informações que muitas vezes valem milhares de reais. Nessa grande luta estratégica das empresas pelo domínio do mercado e do poder, as informações podem gerar grandes negócios ou destruí-los totalmente.

Com essa explosão da informação, muitos foram as formas de prevenção dos setores de TI das empresas em proteger os seus dados mais importantes, as quais obtiveram uma estabilidade operacional, investindo milhões de reais na área de segurança com a compra de diversos dispositivos e na contratação de pessoas especializadas, mas o fenômeno que está gerando cada vez mais ruído é o da engenharia social, aonde o alvo não são sistemas da informação e sim seres humanos.

Com a grande importância desse assunto posta em situação, é necessário o conhecimento dos principais tipos de métodos de ataque para que seja possível a defesa e a prevenção. Tendo analisado cada ponto disposto em suas magnitudes de importância e impacto no negócio, far-se-á essencial o seu cuidado por todas as pessoas envolvidas, em todos os processos e áreas da empresa.

Independentemente da forma de ataque que exista futuramente, o ser humano continuará sendo o elo mais fraco em toda essa disputa entre pessoas mal-intencionadas e as empresas. Ao contrário de um caso de ataque virtual, feito do modo zero-day, onde um cracker busca uma vulnerabilidade desconhecida num software e executa o ataque e posteriormente sofre uma defesa, as pessoas sempre terão vulnerabilidades as quais são insanáveis com softwares antivírus ou um potente firewall, a única arma e defesa é a prevenção e o cuidado.

Com a diferença de se atacar seres humanos ao invés de sistemas, o engenheiro social consegue aplicar golpes com muita eficiência, utilizando de artifícios do próprio modelo de pensamento e do psicológico destreinado dos usuários. E essa situação ocorre, muitas das vezes, simplesmente pelo usuário, bem-intencionado

tentar ajudar ou ser útil de alguma forma. São características psicológicas humanas que ao serem exploradas podem causar um grande rompimento de barreiras antes intransponíveis virtualmente.

Dentre essas características psicológicas os atacantes abusam de determinadas táticas com o uso de micro-expressões e sutis técnicas de *rapport*. E a programação neuroinguística (PNL) também é usada pelos atacantes que treinam arduamente para conseguir alcançar a excelência na persuasão, dentre outras diversas táticas mentais.

Por muitas vezes o engenheiro social não necessita pular um muro para conseguir informações vitais, por vezes ele as encontra no lixo, em sites de buscas, e até mesmo em redes sociais públicas. E com um telefonema e uma boa história, o atacante consegue o seu objetivo, e a vítima sequer toma consciência disso.

Atualmente são vários os ataques condicionados os quais enganam milhares de pessoas diariamente, gerando enormes prejuízos. Fraudes por telefone, por SMS, sites clonados, clone de cartões, roubo de informações privadas, e outras ofensas que podem ser prevenidas com o conhecimento desses ataques e formas de evitá-los.

A prevenção é a maior defesa do usuário e das empresas, e o ser humano deve ser treinado e capacitado antes mesmo de iniciar as suas atividades na empresa, e estar pronto para os desafios de um ataque sem software contra a sua mente e seus instintos.

1.1 PROBLEMA DE PESQUISA

A engenharia social é importante e pode gerar um grande prejuízo se executa contra uma empresa? Será que existe um conhecimento adequado sobre as técnicas e ameaças? O usuário tem agido de maneira correta? Essas são perguntas respondidas na pesquisa realizada, as quais nos proveem indícios que os usuários tratam a engenharia social como algo ficcional e existe somente em filmes ou novelas.

A prevenção e o conhecimento da engenharia social são fundamentais para a base da segurança da informação das organizações, pois sem essa o uso de softwares mais avançados tornar-se-ão totalmente inúteis.

Estudar qual é a atitude atual do usuário, como ele trata as informações sigilosas, ou o que faz em situações de ataques sutis os quais nem estão preparados ou sabem como agir.

Provar e constatar o conhecimento sobre os principais tipos de ataques de engenharia social, e qual seria o percentual de treinamento realizado pelas organizações para preparar os seus colaboradores de possíveis ataques de engenharia social

Estudar a necessidade da aplicação de seminários, palestras ou instruções sobre os ataques e sua utilidade para as organizações e usuários.

1.2 DELIMITAÇÃO DO PROBLEMA

O objeto deste trabalho é constatar a falta de instrução da população brasileira sobre as ameaças da engenharia social, e seus métodos de prevenção. Os usuários pesquisados são de diversas áreas e idades, ocasionando uma maior granularidade e alcance da pesquisa, pois a engenharia social pode ser aplicada em todas as áreas de atuação da empresa e em todas as empresas.

Espera-se com a pesquisa a elucidação do nível de conhecimento dos usuários e quais são seus hábitos e visões em situações de ataques propostos.

1.3 JUSTIFICATIVA

Justifica-se pela importância da proteção das informações das organizações, sendo estratégico e de essencial forma de manter o negócio em si. Assim se faz necessária uma conscientização das táticas mentais e técnicas utilizadas por pessoas má intencionadas que buscam determinados objetivos.

Para construir um nível suficiente de conhecimento e alcançar o amadurecimento da política de segurança no quesito engenharia social, faz-se necessária a explicação das principais táticas e também as defesas as quais prevenirão futuros ataques.

A cada dia são inventadas novas formas de ludibriar os usuários, mas os mecanismos utilizados normalmente são os mesmos, assim sendo que conhecendo o "*modus operandis*", pode-se tomar as devidas providências preventivas.

1.4 OBJETIVOS

1.4.1 OBJETIVO GERAL

- Estudar a importância do tema engenharia social na segurança da informação de empresas e na vida das pessoas;

1.4.2 OBJETIVOS ESPECÍFICOS

- Desenvolver uma pesquisa sobre engenharia social no ambiente coorporativo brasileiro.
- Analisar e evidenciar a importância da engenharia social no contexto empresarial e também no cotidiano das pessoas;
- Avaliar a efetividade da prevenção contragolpes de engenharia social;
- Criar um conjunto de instruções para prevenir os ataques.
- Propor às empresas a inclusão do tema em políticas de segurança, e na realização de treinamentos aos usuários.

2. FUNDAMENTAÇÃO TEÓRICA

2.1 CONCEITOS DA ENGENHARIA SOCIAL

A melhor definição para engenharia é: “Engenharia Social é a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de Engenharia Social são amplamente utilizadas por detetives (para obter informação) e magistrados (para comprovar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos.” (KONSULTEX, 2004 apud PEIXOTO, 2006, p. 4)

Todos os anos as corporações despendem de milhões de reais em alta tecnologia de segurança da informação, mas falham em não dar a atenção necessária aos mais triviais itens da segurança. E na pressa em deixar as políticas de segurança da informação prontas o mais rápido possível, muitos gerentes de TI deixam para trás erros simples que podem gerar enormes prejuízos. A engenharia social cuida do fator pessoa, aonde é considerado o elo mais fraco e de menor resistência em todo o sistema de uma empresa. Com isso em vista o engenheiro social buscará métodos de persuasão, e táticas que tratam de enganar para conseguir “hackear” uma pessoa ao invés de um sistema altamente protegido.

A engenharia social vem de duas palavras, segundo Patel, a engenharia significa um caminho definido para alcançar uma tarefa seguindo determinados passos para atingir um objetivo, e social refere-se ao nosso cotidiano, seja vida pessoal ou profissional.

E pode ser definido, segundo Hadnagy, como: *“Um ato que influencie uma pessoa a tomar uma ação que pode ou não ter seus melhores interesses ou intenções”* (tradução livre). Ou seja, a engenharia social não trata apenas de casos negativos, de invasões, de golpes, mas também dos métodos de como trabalhamos a comunicação com nossos familiares, filhos, e no dia a dia.

Para conseguir uma comunicação eficaz e de influência a engenharia social utiliza de métodos e artimanhas psicológicas eficazes num todo, com uma intenção direcionada oculta a conquistar um objetivo em específico. Dentre esses objetivos, denotam-se golpistas que buscam acessos às informações sensíveis de empresa, e que podem gerar milhares de reais em prejuízos.

2.1.1 A IMPORTÂNCIA DA ENGENHARIA SOCIAL

Com a geração cada vez mais abundante de dados em todas as empresas, sejam dados cruciais ou não, atacantes veem brechas espalhadas através das grandes fortalezas da segurança da informação, o elo mais fraco: o ser humano. Com a perda de informações, empresas podem literalmente entregar, sistematicamente, todas as suas estratégias de negócio e seu poderio aos concorrentes, ocasionando a sua queda.

A engenharia social, com toda essa massificação de dados, criou uma grande preocupação às empresas pela sua importância, atualmente existem sistemas dos mais avançados de segurança da informação, com a preocupação exclusiva de proteger os dados e o sistema, mas ainda o maior investimento dos atacantes está no elo mais fraco que é o ser humano.

2.1.2 O CAMINHO MAIS FRACO E VULNERÁVEL DO SISTEMA

Em sua maioria, os sistemas de informações das empresas são controlados por pessoas, especializadas ou não. Com isso, existe um fácil acesso que pode ser estrategicamente traçado pelo atacante que utilizará de várias técnicas para influenciar e manipular a vítima para atingir determinado objetivo.

Os alvos são, praticamente, todos os funcionários da empresa, pois desde o acesso às instalações pelos recepcionistas, e áreas restritas pelos trabalhadores de chão de fábrica, até a gerência ou diretoria, são facilmente ludibriadas a agirem de determinada forma em prol, mesmo que não intencionalmente, a um ataque.

2.1.3 CONSEQUÊNCIAS DOS ATAQUES

As consequências dos ataques bem-sucedidos são devastadoras às empresas. Desde a perda de informações sigilosas ou triviais, até mesmo no roubo de informações pessoais dos funcionários, podem ocasionar um grande dano, muitas das vezes irreparáveis.

Um exemplo desse ataque ocorreu no dia 06 de outubro, deste ano, quando foi descoberto uma central de atendimentos fraudulenta na Índia que capturava informações bancárias de usuários nos Estados Unidos, quando os funcionários se

passavam por funcionários da Receita Federal. O prejuízo foi de cerca de quatrocentos e oitenta e três mil reais por dia, segundo informações da redação (REVISTA VEJA, 2016) daquele dia.

2.1.4 DIFERENÇAS ENTRE ATAQUES SOCIAIS E ATAQUES TÉCNICOS

Os ataques realizados pelos engenheiros sociais podem ser divididos em duas grandes frentes, os ataques diretos, aonde o engenheiro social atacará a vítima diretamente por um telefonema ou pessoalmente, necessitando do atacante muita perspicácia e criatividade para planos alternativos. E os ataques indiretos, ocasionados pelos *malwares*, sites falsos ou e-mails com golpes em seus links.

Os ataques sociais são caracterizados pelos ataques diretos, aonde a vítima tem um contato direto com o atacante, muitas vezes disfarçado e com informações antecipadas para um ataque mais eficiente.

Os ataques técnicos caracterizados pelos tipos indiretos, dão-se por vias virtuais, como e-mail, SMS, sites clonados, dentre outras técnicas que podem enganar o usuário e possibilitar que um atacante consiga êxito em suas investidas.

2.2 ATAQUES SOCIAIS

Os ataques realizados pelos engenheiros sociais podem ser divididos em duas grandes frentes, os ataques diretos, aonde o engenheiro social atacará a vítima diretamente por um telefonema ou pessoalmente, necessitando do atacante muita perspicácia e criatividade para planos alternativos, o qual estará muitas das vezes disfarçado e com informações antecipadas para um eficaz ataque. E os ataques indiretos ou técnicos, ocasionados pelos *malwares*, sites falsos ou e-mails com links falsos, entre outras categorias.

2.2.1 PRINCÍPIOS PSICOLÓGICOS

Dentre as diversas formas de persuasão e manipulação usados pelos atacantes, os princípios psicológicos são estudados profundamente para que os ataques sejam eficazes e alcancem os objetivos propostos.

2.2.1.1 MODELOS DE COMUNICAÇÃO

Um modelo de comunicação é um processo para transferir informação de uma entidade para outra. A comunicação envolve dois elementos, pelo menos, aonde há uma troca de informações e uma progressão de pensamentos, ideias para mutuamente aceitar uma direção ou objetivo proposto.

Para a aplicação de modelos de comunicação na engenharia social a diferença está no objetivo da pessoa que está transmitindo a informação e no receptor, aonde a engenharia social é usada para criar um objetivo em comum.

A comunicação é um processo aonde a informação é empacotada e transmitida por um canal, conhecida como meio de transmissão, o receptor então decodifica a mensagem e fornece um feedback. Esse processo é comumente chamado como "*Shannon-Weaver*" ou "a mão de todos os modelos", demonstrado na figura 1.

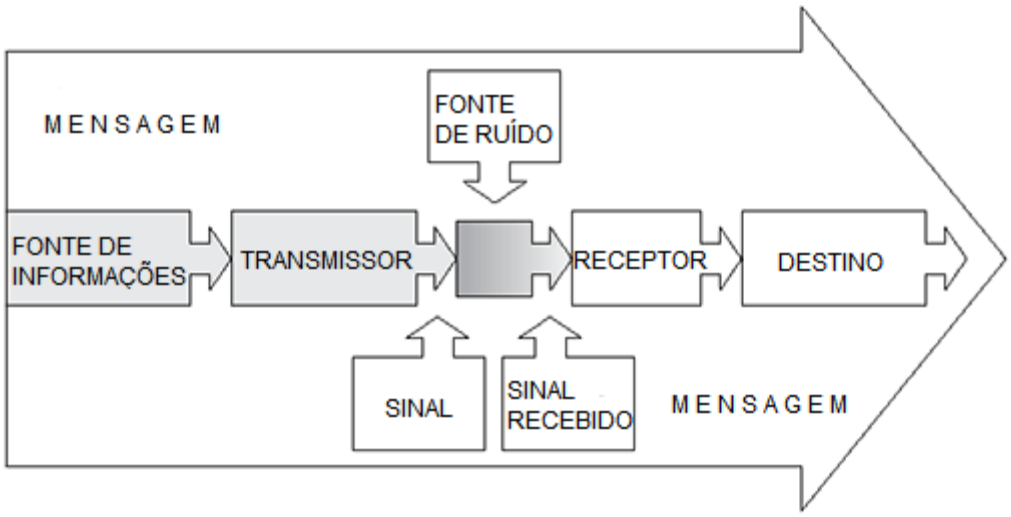

FIGURA 1: MODELO SHANNON-WEAVER

Para melhor entendimento do processo da figura 1: Uma fonte de informação produz a mensagem. Um transmissor codifica a mensagem em sinais. Um canal é aonde os sinais são adaptados para a transmissão. Um receptor que decodifica ou reconstrói a mensagem pelos sinais. O destino é aonde a mensagem chega.

Após quinze anos, David Berlo expandiu o modelo supracitado, originando o modelo de Berlo demonstrado na figura 2.

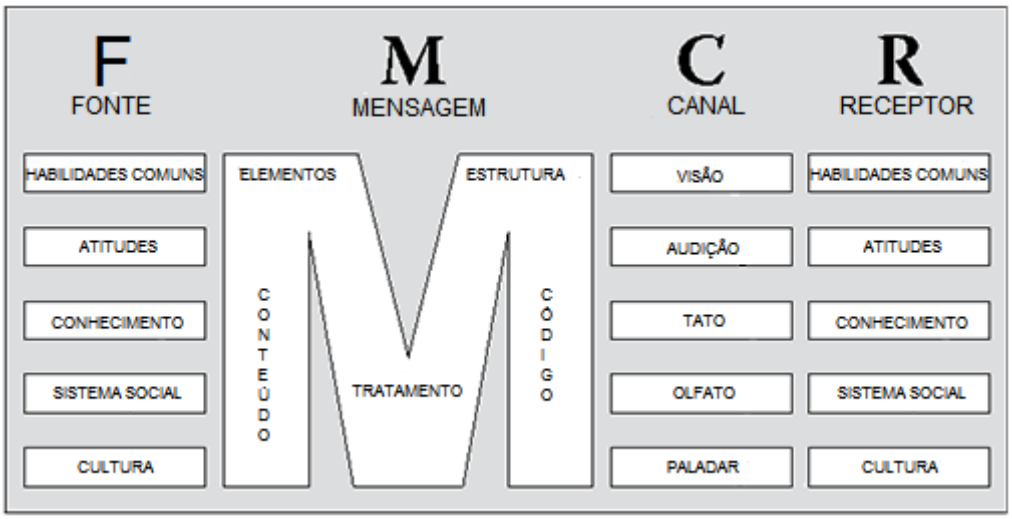

FIGURA 2: MODELO DE BERLO

No modelo de Berlo, houve uma incrementação na forma de visualizar como a comunicação é realizada. Nota-se uma divisão entre áreas, as quais: Fonte, Mensagem, Canal e Receptor. Nesse estudo a fonte possui habilidades comuns, atitudes, conhecimentos, sistema social, cultura, o mesmo ocorrido com o receptor. A diferença é visualizada pelo caminho da informação, aonde a mensagem possui

elementos, estrutura, conteúdo, códigos e tratamentos, e o canal são os sentidos donde a mensagem chega, seja pela visão, audição, toque, cheiro ou sabor.

No processo de ludibriar a vítima, o atacante buscará utilizar de todo o processo de comunicação da melhor forma possível. O ser humano, naturalmente, é disposto a ajudar quem está necessitando e será nesse momento aonde o atacante conseguirá obter o êxito, ligando todos os elementos necessários, utilizando-se de uma comunicação simples e clara, mas com um objetivo oculto.

2.2.1.2 MICRO-EXPRESSÕES

As micro-expressões são formas faciais e de expressão que dificilmente são controladas pelo corpo humano devido a uma reação de uma emoção em específico. Em oposição a isso as macro-expressões destacam-se, por exemplo, quando se dá um sorriso simpático ao cumprimentar um vizinho mesmo estando irado.

Então são movimentos musculares involuntários, geralmente imperceptíveis pela pessoa, mas demonstram toda a situação emocional do momento. Segundo Dr. Ekman, em 1972, são seis os tipos de expressões: raiva, desgosto, medo, alegria, tristeza e surpresa.

Essas expressões quase ocultas denotam quando uma pessoa pode estar mentindo, falando a verdade, estressada, e de modo geral o seu quadro emocional real e em constante alternância.

Portanto as micro-expressões são fundamentais para identificar como a vítima está reagindo a um ataque, e se aquela ofensiva está sendo bem-sucedida ou não. Um simples gesto com os olhos, com a boca, ou com o corpo, podem denotar maiores respostas e uma análise profunda da situação pelo atacante. Dentre esses sinais o atacante perceberá que a vítima está percebendo o golpe com contradições, hesitações, mudanças de comportamento e o simples gesto das mãos, motivos pelos quais o atacante mudaria a sua estratégia inicial.

2.2.1.3 RAPPORT INSTANTÂNEO

Traduzido livremente como harmonia, o *rapport* é uma fundamental ferramenta e um dos pilares na engenharia social. Com o *rapport* é possível conseguir uma harmonia entre as partes com uma sincronia muito grande na comunicação. Além de

alcançar uma maior interatividade, confiança e conseguir a conquista da vítima em prol do objetivo inicial.

Alguns tópicos são importantes no estudo do *rapport*, dentre eles:

- Seja genuíno sobre querer conhecer a pessoa.
- Tome cuidado com a aparência.
- Seja um bom ouvinte.
- Esteja atento de como afeta as pessoas com as palavras e atitudes.
- Mantenha a conversa fora de si mesmo.
- Empatia sempre.
- Tenha um bom conhecimento sobre assuntos em geral.
- Desenvolva seu lado curioso.
- Procure caminhos para conhecer as necessidades das pessoas.
- Respire na mesma frequência da outra pessoa.
- Fale no mesmo tom e altura.
- Imite a linguagem corporal.

Dentre todos esses tópicos, o atacante utilizará de caminhos após uma análise inicial das microexpressões, do *feedback* da vítima sobre os ataques e conseguirá distinguir se a situação será favorável ou necessitará de um plano diferente.

Muitos desses ataques podem ser realizados também por meios virtuais, por exemplo quando há um grande desastre ou abalo, o atacante utilizará da empatia para enviar um e-mail emotivo e conseguir êxito que a vítima clique em um *link* ou imagem.

2.2.1.4 O *BUFFER OVER FLOW* HUMANO

Assim como um copo de água que transborda após o líquido passar dos limites, assim também o cérebro humano pode ser transbordado.

Um hacker pode trabalhar num programa afim de conseguir um *buffer over flow* no qual corresponde a um estouro do tamanho de uma determinada variável dentro do espaço alocado. Isso corresponde, por exemplo, a um desenvolvedor alocar vinte *bytes* para determinada variável e o *hacker* forçar trinta *bytes*, ocasionando um *crash* do programa, no qual poderá se aproveitar para inserir um código malicioso exatamente naquele espaço com a falha intencional.

O cérebro também trabalha como se fosse um software, com suas instruções, *buffer*, memória, dentre outras características homogênea. Nesse escopo mental, é possível ocorrer um *buffer over flow* através de técnicas específicas.

Dentre essas técnicas existe o *fuzzing* aonde o hacker manda dados aleatórios e de tamanhos diversos até que o programa pare de funcionar e ali consiga inserir o código malicioso. No cérebro, de forma similar, isso ocorre quando o engenheiro social manda presunções ao invés de dados. Funcionará melhor quando pergunta algo com as palavras certas, com a linguagem corporal adequada e expressão facial que indica que você está sempre em condição de aceitação ou se mostre amigável.

Dentro da técnica de *fuzzing*, é aplicado a regra de comandos embarcados, ou seja, dentro das frases são incluídos comandos sutis para fazer com que a vítima execute uma ação ou aja de determinada maneira. Frases como: "compre agora", "aja agora", "siga-me", "quando você...", "como você se sentiria...", as quais denotam um querer que a vítima sequer perceberá, mas que seu subconsciente assimilará imediatamente e seu lado emocional também será ativado.

2.2.1.5 PROGRAMAÇÃO NEUROLINGUÍSTICA (PNL)

A programação neurolinguística refere-se à capacidade de usar a linguagem e como determinadas frases e palavras refletem sobre a mente e sua programação interna. Linguística denota-se da capacidade de linguagem entendível pela mente, e neuro é referenciado pelo sistema nervoso, e aos cinco sentidos humanos: audição, visão, paladar, tato e olfato, com sua percepção do mundo.

Esse estudo se iniciou nos anos 70 por Richard Bandler e John Grinder, orientados por Gregory Bateson, aonde criaram um meta-modelo que reconhecia o uso de padrões de linguagens para influenciar mudanças.

Na origem da PNL, Grinder desenhou um código no qual a linguagem corporal era o principal objetivo, sendo que posteriormente foi criado o novo código PNL aonde é focado mais nos pensamentos ou crenças de acontecimentos futuros e na mudança de comportamentos negativos.

Na engenharia social a PNL é muito utilizada sendo uma ciência riquíssima para alcançar grandes resultados aos atacantes. Para chegar nos objetivos propostos do ataque, o golpista utilizará de scripts dentro do código novo da PNL. Dentre as técnicas utilizadas estão a voz, a sentença estruturada e a voz incrementada.

A voz é um elemento essencial na PNL quando o assunto é engenharia social, aonde o atacante usa a voz para inserir comandos nas entrelinhas e conseguir o êxito. Assim a usará para dar ordens e direcionar um comportamento em específico.

A sentença estruturada tem o seu significado pela ênfase que é dada uma palavra dentro da frase. Isso alterará o sentido, e o comando estará incluso no meio dela. Por exemplo: "Lembra-se de quando você limpa seu quarto quando a visita vem?", o destaque da frase é dado pela entonação vocal, aonde o comando é inserido e o receptor o capta pelo seu subconsciente sem perceber conscientemente.

A voz incrementada é uma técnica avançada para inserir comandos numa conversa habitual sem que o receptor a perceba. Essa técnica exige muita prática e dedicação, mas têm um grande poderio se bem aplicada.

Entre todas as técnicas e formas de utilizar a PNL num ataque de engenharia social, destacam-se três cuidados importantes: o tom vocal, escolher as palavras cuidadosamente, criar uma lista de comandos para serem usados. O tom vocal é importante para enfatizar uma palavra ou comando dentro do subconsciente. A escolha das palavras deve ser feita com critério e utilizando palavras que tragam máximo impacto. E a lista de comandos é feita para ajudar a relembrar e usá-las assim que possível.

2.3 PONTOS FRACOS HUMANOS

O ser humano é o elo mais fraco do sistema, e existem vários métodos e técnicas aonde os atacantes, com objetivo de ludibriar as suas vítimas, utilizam, dentre elas existem táticas de influências, o pretexto, a elicitação e a manipulação em diversas vertentes.

2.3.1 TÁTICAS DE INFLUÊNCIA

Um engenheiro social utiliza de diversas táticas de influência para conseguir lograr êxito em seus objetivos. Seis são as táticas de influência principais que mais alcançam um resultado eficaz, quais são: reciprocidade, escassez, autoridade, gentileza, concessão, afinidade. Além de outras táticas estudadas posteriormente, como pretexto, elicitação e a manipulação.

A reciprocidade está atrelada ao sentimento do ser humano em retribuir por um favor, uma boa ação ou algo dado, por outrem. Essa tática é muito utilizada, por exemplo, na área política, aonde quem ajuda na campanha acabará por se beneficiar após o candidato conseguir a vitória nas urnas. Existem empresas, das mais diversas áreas, que tratam os seus clientes com jantares, presentes, dentre outros modos para conseguir a renovação dos contratos e outras vantagens. Em “A norma da reciprocidade”, escrita pelo sociólogo Alvin Gouldner, relata que existem duas demandas na reciprocidade, que as pessoas deveriam ajudar aquelas que as ajudaram, e não machucar aquelas que as ajudaram. Gouldner definiu um ciclo da reciprocidade, aonde existe o seguinte caminho da figura 3:

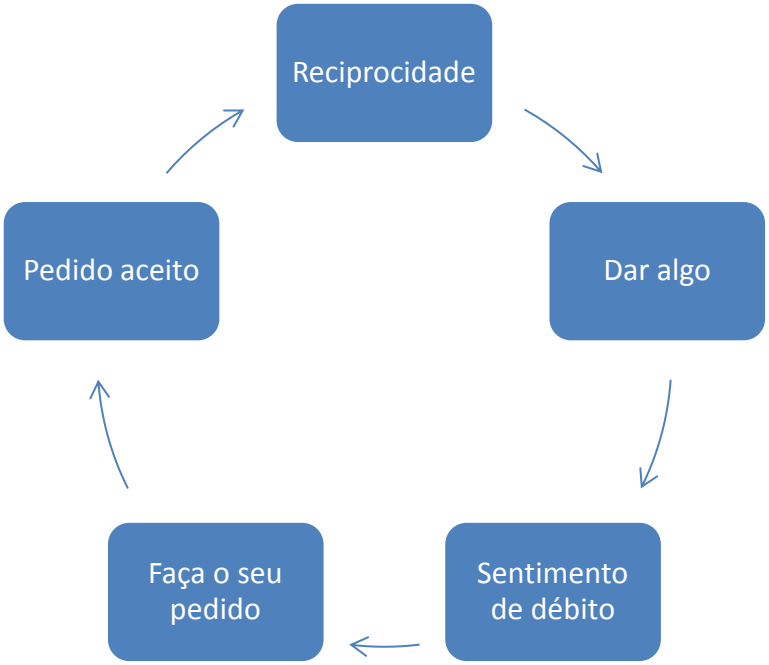

FIGURA 3: CICLO DA RECIPROCIDADE DE ALVIN GOULDNER

No ciclo o “dar algo” significa conceder algo de valor ao receptor. Pode ser um serviço, uma informação valiosa, ou algo valioso. No momento em que é concedido, a pessoa irá se aproveitar da situação e oferecer algo, como se fosse uma armadilha aonde é ofertado um bem ou serviço. A criação de um sentimento de débito será iniciada no momento do passo anterior, quando o receptor irá perceber que existe um sentimento de débito ao ter recebido determinada vantagem ou bem de valor. É quando o pedido será feito pela parte autora, a qual fará seu pedido ou proposta, aproveitando-se da situação. E o pedido, finalmente, terá grandes chances de ser aceito pelo receptor.

A escassez é outra forma de influência, e essa tática é fundamentada pelo sentimento de supervalorização que o ser humano possui ao ver que algo é escasso ou muito raro. Propostas como “últimos dias”, “urgente”, “somente hoje” ou “você nunca terá mais essa chance novamente”, são incrivelmente chamativas e eficazes para conseguir a atenção e ao seu utilizar essa tática com outras já vistas, o engenheiro social conseguirá obter êxito em suas investidas.

A autoridade é uma tática de influência muito eficaz. E essa tática trata-se de que o ser humano é levado a obedecer às autoridades ou os personagens que ajam como tal. E isso se inicia desde os primeiros anos de vida, quando as crianças obedecem aos professores, conselheiros, padres ou pastores, e outros que imponham forte autoridade em suas ações. Max Weber, um sociólogo e economista político

alemão, demonstrou que existem três categorias da autoridade: autoridade legal, autoridade organizacional e autoridade social. O engenheiro social irá utilizar de todas as suas ferramentas para conseguir se disfarçar de alguma autoridade ou tomar o papel de uma para conseguir lograr êxito.

A gentileza é uma tática muito similar à reciprocidade. No caso da gentileza é criado um sentimento após uma breve conversa ou gentileza, aonde as partes trocam gentileza após uma boa atitude de uma das partes. O atacante irá utilizar dessa técnica ao conversar com a vítima e conseguir um contato, utilizando evidentemente as técnicas anteriores, como *rapport*. Desse modo conseguirá um acesso ou uma informação pertinente.

A concessão é outra forma de influência, aonde uma das partes irá fazer uma proposta e a outra tornará com uma nova proposta. A reciprocidade é percebida nessa tática, como percebida na negociação de um automóvel, aonde o preço inicial é vinte mil, e o comprador oferece quinze mil, então o vendedor irá declinar de sua ideia inicial e conceder um desconto para que a venda seja efetuada. No contexto da engenharia social aonde o atacante perguntará por algo grande e por vezes impossível, concedendo habilmente à proposta de seu objetivo inicial, conseguindo a informação ou ação necessária de sua vítima.

A afinidade não é somente no quesito de parecer ou ser igual a outra pessoa, mas também na questão de ela ser bem vista socialmente pelas outras, isso inspira confiança. De acordo com o estudo “What is beautiful is good” (O que é bonito é bom) de Karen Dion, Ellen Berscheid e Elaine Hatfield, afirma que a aparência física positiva da pessoa influencia para que seja mais aceita e acessível em interações sociais. Na engenharia social o atacante pode utilizar a tática para começar uma conversa com um elogio breve, aonde reforçará a autoimagem positiva da vítima, fazendo aumentar a sua vulnerabilidade a um golpe ao ter mais afinidade com a vítima.

2.3.2 PRETEXTO

O pretexto é a ciência de ser quem você desejar ou precisar ser. Segundo Hadnagy, o pretexto é o ato de criar um cenário para persuadir uma vítima para conseguir uma informação ou fazer uma ação. E isso pode envolver a criação de um personagem totalmente novo ou a cópia fiel de uma outra pessoa, em suas atitudes, palavras e manias.

Isso necessitará de uma pesquisa mais apurada para saber a atual posição do personagem, e um estudo avançado de como o cenário criado poderá influenciar na decisão da vítima. Envolver a vítima nos seus próprios interesses podem aumentar as chances de conquista, e a prática de expressões corretas também. A simplificação, de forma igual as outras características, é muito importante no pretexto, pois quanto mais simples e inesperado é a situação criada mais eficiente será.

O engenheiro social conseguirá obter o sucesso em sua investida com o pretexto ao criar um cenário adequado, envolvendo a vítima em seus próprios interesses, alcançando o objetivo proposto inicialmente no golpe.

2.3.3 ELICITAÇÃO

Elicitação é uma forma de obter informações amigavelmente. Significa coletar o necessário através de uma conclusão pela lógica ao estimular a pessoa numa direção. Ao engenheiro social significa ser eficaz com as palavras e questões para construir um caminho e elevar o seu nível de afinidade com a vítima ao alcançar um novo nível de confiança.

A elicitação é utilizada nas conversas habituais, do dia a dia, sem pretensões, aonde será possível conseguir informações as quais dificilmente seriam alcançadas de forma direta e abrupta.

Essa técnica funciona bem por algumas razões em especial, como que muitas pessoas desejam ser educadas, profissionais querem parecer bem informados e inteligentes, a maioria das pessoas não mentiria, e respondem gentilmente a pessoas que aparentam se preocupar com elas.

Dentre todas as técnicas, a elicitação é uma das principais, aonde o engenheiro social que a dominar estará a um passo de obter informações privilegiadas ou conseguir que a vítima execute determinadas ações. O engenheiro social deve atender a ser o mais natural possível, muito educado e não ser apressado para conseguir os objetivos primários.

2.3.4 MANIPULAÇÃO

A manipulação em engenharia social é um assunto extremamente importante, tendo em conta o seu efeito na vítima. Assim como na arte da persuasão, a

manipulação é usada para a vítima querer agir, pensar ou acreditar em determinado caminho que o golpista deseje.

Um dos objetivos da manipulação é criar um sentimento de ansiedade, estresse e uma pressão ou responsabilização social. Quando a vítima sente que o melhor caminho a seguir é da sugestão do golpista, então ela está sendo efetivamente manipulada.

A PNL ajudará nesse processo de manipulação e será uma das vertentes principais ao causar a sugestividade no sujeito. E dentro disso há toda uma situação para envolver a vítima, a roupa usada, as frases ditas, a forma das palavras que serão pintadas em uma figura. E ao conhecer melhor a vítima, como o que ela gosta ou não, o nome das crianças, seu time do coração e as comidas favoritas, criará um ambiente emocional favorável e também uma atmosfera favorável ao atacante.

Conhecer o ambiente da vítima é algo essencial para um processo de manipulação ocorrer de modo efetivo. Atualmente os atacantes buscam usar as redes sociais para investigar mais sobre as vítimas, o que eles gostam, o que conquistaram, entre outras informações divulgadas publicamente. Com isso em mãos, os atacantes possuem grande quantidade de informações para poder criar um ambiente favorável, aonde ganharão a confiança da vítima pela afinidade de assuntos e possuirão um controle muito maior sobre a situação em caso de planos alternativos.

Fazer com que a vítima se sinta sem poder ou sem o controle é também uma das formas de manipulação muito utilizada. Aonde o atacante se passará por alguém importante e aja de maneira na qual a vítima se sinta intimidada ou reprimida pela imposição de ordens e na urgência do assunto. A vítima não terá tempo para pensar sobre o problema e agir, então permitirá que o atacante tome conta da situação e consiga o seu objetivo.

A punição mental é ligada ao item anterior em tornar a vítima intimidada, aonde terá um sentimento de culpa, humilhação, ansiedade ou perda do privilégio com a situação urgente. Com o conjunto dessas fortes emoções, a vítima não terá muitas reações sobre a situação e sentir-se-á com a sensação de que a estão fazendo um favor.

A intimidação é uma forma de manipulação muito utilizada pelos governos em tempos de crise, aonde mostram à população que se não forem feitas certas medidas trarão outras consequências drásticas no futuro. Com isso, o engenheiro social conseguirá reagir intimidando a sua vítima até mesmo pela aparência, pela entonação

vocal, olhar ocupado e preocupado, e dentro de uma importantíssima tarefa, farão com o que a vítima se sinta intimidada e pronta para ajudá-lo.

2.4 BUSCA POR INFORMAÇÕES

Um engenheiro social necessitará de abundante conteúdo de informações sobre a vítima ou organização a ser atacada. Desse modo, existem algumas maneiras de coletar esses dados.

2.4.1 TELEFONEMAS

Uma das formas é por telefonemas. O golpista vai disfarçar-se, muitas das vezes, como alguém desinformado, atrás de uma informação inocente, e se a vítima não estiver preparada, poderá sucumbir e fornecer importantes dados ao atacante. Pode-se, por exemplo, ao querer entrar em contato com um consultório odontológico, em busca de informações sobre as credenciais, o atacante fazer o seguinte. Ligar primeira vez se passando por um inocente vendedor de um software inovador para o setor, querendo falar com o médico responsável e o pessoal de TI. Nesse momento a vítima repassará, muito provavelmente, informações necessárias como os nomes dos responsáveis pelas áreas, o telefone e outras informações suscetíveis. Noutro dia o atacante pode retornar a ligação, falar com outra pessoa e se passar por alguém da TI que cuida do sistema atual e está necessitando fazer uma atualização crítica no servidor, fornecendo as informações repassadas pela primeira vítima e dando extrema urgência a situação, criando assim um senso de credibilidade, e fazendo com que a segunda vítima acredite na história. Tendo aceito a história, o atacante poderá solicitar as credenciais, e poderá obter êxito em sua investida. O exemplo demonstra o uso de truques mentais para que a vítima pense que está fazendo um favor, ou se sinta na obrigação de fazer algo em prol da organização para ajudar.

2.4.2 BUSCAS ONLINE

Outra forma utilizada pelos atacantes são as buscas online, aonde podem buscar informações triviais sobre as vítimas e organizações em sistemas de pesquisa, como o Google. Existe atualmente um termo utilizado, que é o Google Hacking, aonde

os engenheiros sociais buscam termos específicos nas pesquisas, como "*site*: ", que corresponde ao site em específico, "*intitle*:" que buscará tudo que estiver no título, ou até "*inurl*:" que buscará determinadas palavras na URL de um determinado site, "*filetype*:" que serve para buscar um tipo de arquivo específico dentro de um site. Esse assunto é muito vasto, e possui muitas vertentes para serem mostradas, e é uma ferramenta muito poderosa na mão dos golpistas. Por exemplo, quando poderão fazer pesquisas relacionando o nome da empresa com o tipo de arquivo e achar um arquivo sigiloso que foi descuidadamente deixado de forma pública, dentre outros diversos tipos de situações.

2.4.3 REDES SOCIAIS

Outra forma utilizada com muita frequência e com um grau de fidelidade de informações muito grande é o das redes sociais. Atualmente existe uma situação aonde as pessoas estão a cada dia mais publicando suas vidas privadas nas redes sociais, sem nenhum controle ou noção sobre o perigo, seja Facebook, Google+ ou outra. Os atacantes sociais conseguem informações privadas, como a hora que as vítimas saem para trabalhar, o local do trabalho, os seus colegas de trabalho, o dia a dia na empresa, e informações pessoais como o nome dos filhos, como eles se parecem ou a sua programação semanal, sem esforço algum. Além de informações como o que gostam, o que odeiam, quem são os seus vizinhos, e até mesmo fotos de seus cômodos dentro de casa ou da situação conjugal. Essas informações serão reunidas pelos atacantes que buscarão, por vezes, clonar um perfil de um conhecido ainda não adicionado à rede da pessoa para se passar por ela e ser incluído, coletando um número ainda maior de dados.

Esses dados, por vezes, são utilizados de igual modo por ladrões, que reúnem informações fundamentais sobre as vítimas para realizarem assaltos, além de sequestros e diversas outras formas de crimes.

2.5 ATAQUES DE ENGENHARIA SOCIAL

Após o estudo preliminar sobre as formas de ataques psicológicos e da coleta de informações, o atacante necessitará de ferramentas e formas efetivas de chegar às vítimas e lograr o sucesso do golpe.

2.5.1 VISHING

O termo *vishing* é uma combinação de *voice* (voz) e *phishing* (pescaria – fraude virtual). Nesse ataque o engenheiro social utilizará de vias telefônicas para entrar em contato com a vítima. O atacante poderá utilizar de artimanhas como alterar a identificação do número que está ligando. Esse ataque está mais relacionado para o alvo fornecer credenciais ou informações de contas bancárias, dentre outras. No Brasil esse ataque é feito geralmente por presos, dentro de presídios, aonde ligam aleatoriamente e informam que a vítima ganhou um grande prêmio, e para isso deve creditar um valor em um número para a confirmação do ganhador. Além de outros golpes conhecidos aonde muitas pessoas são ludibriadas.

2.5.2 SMISHING

Essa é uma forma muito tradicional de golpe, o uso de SMS em celulares. Nesse ataque o golpista se faz passar por uma organização ou pessoa, muitas das vezes informando que a conta bancária foi bloqueada ou o cartão foi clonado, então fornecem um link para um arquivo ou página maliciosos, aonde poderá ser efetivado o golpe quando a vítima clicar e ser direcionada a um *malware* ou fornecer informações numa página falsa, inclusive com sua senha.

2.5.3 DUMPSTER DIVING

A tática de ataque *dumpster diving*, ou xeretando no lixo, é uma forma muito usada em casos aonde são necessárias a coleta de maiores informações das vítimas. Nesse método o hacker não precisa sequer tocar na rede corporativa, ou realizar um ataque contra seus poderosos firewalls. Quando a organização não possui um método eficaz para eliminar os documentos, picando-os em máquinas específicas, o hacker conseguirá informações valiosas apenas vasculhando o lixo.

No lixo são encontradas muitas informações, como a conta do banco, informações de cartões de créditos, até mesmo credenciais de sistemas, ou dados de holerites que são descartados sem a sua destruição completa. Além de quando a organização descarta ou doa computadores sem destruir os dados efetivamente, podendo haver recuperação por pessoas más intencionadas.

Com esses dados em mãos, os engenheiros sociais conseguem traçar estratégias de ataque muito mais eficientes e fidedignas, por possuírem informações particulares.

Há também golpes de falsidade ideológica, aonde as pessoas descartam documentos com o seu CPF ou RG, os quais bandidos utilizarão para fazer cadastros em lojas, pedir cartões de créditos, dentre outras formas, e gerar um grande prejuízo aos reais proprietários.

2.5.4 SKIMMING

Skimming é uma técnica utilizada para clonar cartões de acesso RFID (rádio frequência). Muitas empresas utilizam essa forma para fornecer acesso a áreas restritas da organização pelos seus colaboradores, aonde basta o funcionário aproximar o cartão para conseguir o acesso. No *skimming* o atacante utilizará de um sistema próprio para clonar esse cartão com um cartão virgem, apenas o aproximando do equipamento.

Com o cartão clonado, o golpista conseguirá acesso em várias áreas restritas da empresa, ocasionando um enorme desmantelamento em sua área de segurança, além de poder replicar o cartão diversas vezes.

2.5.5 TAILGATING OU PIGGYBACKING

Tailgating é o método utilizado quando um atacante resolve seguir de perto a vítima quando ela estiver entrando no prédio ou organização, dessa forma, muito provavelmente, ela segurará a porta ou deixará alguma brecha aonde o golpista aproveitará. Essa é considerada uma das melhores táticas para conseguir acesso restrito nas organizações. Nessa técnica poderá ser usado um disfarce ou um estereótipo adequado à situação que favorecerá o sucesso da operação.

Piggybacking, de forma muito semelhante ao *tailgating*, é quando o golpista utilizará de informações, por exemplo de uma empresa terceirizada, aonde o atacante irá se vestir com a mesma roupa, com um crachá idêntico, e se passará por um funcionário legítimo realizando algum serviço. Dificilmente alguém desconfiará e tentará o barrar e nesse acesso em locais restritos, assim pode conseguir muitas informações relevantes aos seus objetivos dentro de áreas restritas.

2.5.6 ESPIONAGEM

A espionagem é uma antiga forma de coletar informações. É frequentemente usada quando o engenheiro social necessita de uma coleta maior de informações sem ser percebido. Com isso há uma averiguação do dia a dia da vítima, com um acompanhamento de perto dos seus passos. Dentre as formas utilizadas pelos engenheiros sociais está o *dumpster diving*, aonde conseguirão coletar informações sensíveis apenas vasculhando o lixo da vítima. Além de fotografias, filmagens e uma investigação cautelosa e sigilosa sobre o cotidiano das vítimas para a preparação estratégica de um ataque.

2.5.7 ENGENHARIA SOCIAL REVERSA

A engenharia social reversa ocorre quando o fraudador cria um personagem fictício chamativo ou que aparenta ter uma posição de autoridade e assim conseguir intimidar ou ludibriar a vítima.

Ocorre também em redes sociais, como o Facebook, aonde o engenheiro social irá se disfarçar e infiltrar dentre os amigos de seu alvo com um perfil falso e com muitas semelhanças de interesses da vítima e vários amigos em comum, e o mecanismo da rede social o identificará como alguém interessante para se adicionar. Tendo a vítima o adicionado, criará assim, um laço muito mais forte, pois o interesse partiu da vítima. Segundo Danesh Irani, a vítima é levada a entrar em contato com o fraudador e adicioná-lo como amigo e com isso o fraudador poderá atacar com uma vasta quantidade de métodos de ataques, persuadindo a vítima a clicar em links maliciosos, roubando a identidade e levando-a a entrar em páginas falsas.

A engenharia social reversa é aplicável, de igual modo, quando o engenheiro social se disfarçar por uma autoridade, como por exemplo, vestindo-se de policial ou fiscal da Receita, e com a sua autoridade aparente, vestindo o mesmo uniforme, conseguirá realizar os seus intuitos.

2.5.8 SHOULDER SURFING

Técnica conhecida e costumeiramente utilizada. *Shoulder surfing* significa olhar sobre os ombros, em sua tradução livre, e é uma das formas mais sutis que os engenheiros sociais usam para coletar informações de seus alvos.

Esse método apresenta uma grande efetividade na coleta de dados. Um clássico uso é quando a pessoa está digitando a sua senha em terminais de caixas eletrônicos, aonde mostra a posição das teclas, auxiliando o atacante. Ou quando está num aeroporto, ou local público, utilizando o notebook da empresa, aonde exibe adesivos com a marca, logotipo da empresa, e demais informações.

Apenas com uma observação atenta e algumas fotos tiradas em momentos oportunos, o engenheiro social conseguirá a empresa que a vítima trabalha, quais os programas estão instalados e o sistema operacional. Inclusive se a vítima estiver trabalhando em algum projeto secreto ou confidencial, o atacante acompanhará disfarçadamente toda a movimentação, e pacientemente aguardará um dado relevante.

2.5.9 HOAX

Hoax (boato) é uma tática muito usada virtualmente, aonde os golpistas se aproveitam de situações que geram grande comoção geral. É também classificado como um SPAM em redes sociais, mensagens telefônicas, ou alastradas em grupos de conversas virtuais, como o Whatsapp.

A grande jogada do *hoax* está em mover emocionalmente a vítima numa história triste ou grave. E quando a vítima aceitar, inocentemente, a mensagem e clicar em seu link, um *malware* poderá ser instalado e todos os seus contatos receberão a mesma mensagem.

E não só de boatos alarmantes o *hoax* é constituído, mas também de mensagens de empresas informando que a vítima é ganhadora de um prêmio ou sorteio, ou o mais famigerado golpe do e-mail de um príncipe nigeriano que precisa de alguém para cuidar dos seus milhões de dólares, mas para isso deve-se depositar uma quantia em determinada conta.

Os engenheiros sociais conseguem êxito nessas investidas pois conhecem previamente algumas particularidades e afinidades da vítima, utilizando dos truques psicológicos para convencer e influenciar, alcançam o resultado pretendido.

2.6 ATAQUES TÉCNICOS

2.6.1 TÉCNICAS DE ATAQUES

Algumas formas de ataques técnicos são muito utilizadas pelos engenheiros sociais, os quais buscam o objetivo de ludibriar ou achar uma brecha na segurança.

2.6.1.1 PHISHING

Phishing é uma forma de obtenção de dados sigilosos por meio de sites falsos ou clonados. Geralmente o caminho para a aplicação deste método é por um e-mail, no qual o atacante descreverá uma situação emergencial, geralmente, para atingir o emocional da vítima e atiçar a sua curiosidade. Ao clicar no *link*, a vítima será direcionada a um site malicioso aonde algumas informações secretas poderão ser coletadas. Outra forma é enviar um *malware* pelo e-mail e a vítima será infectada ao clicar.

Para exemplificar essa fraude, toma-se por exemplo a figura 4 a qual corresponde a um site idêntico à rede social Facebook. A semelhança é tamanha ao site oficial na figura 5 que os mais experientes usuários não perceberiam a fraude num primeiro momento. A única mudança visível aonde o usuário poderá atentar é quanto ao endereço do site que é alterado para um servidor do atacante (destaque na figura 4) no qual aguarda a vítima digitar seu *e-mail* e senha, assim concluindo a fraude ao clicar em “Entrar”. No mesmo destaque da figura 4, nota-se que há a ausência do HTTP Secure (HTTPS), que corresponde a uma conexão em uma camada segura aonde é essencial em sites que necessitem de credenciais e tenham sigilo e confiabilidade do domínio aonde se está conectando.

FIGURA 4: PHISHING - SITE CLONADO DO FACEBOOK

FIGURA 5: PHISHING – SITE ORIGINAL DO FACEBOOK

A figura 6 corresponde a um e-mail recebido, supostamente pela Microsoft, cujo conteúdo descreve que a conta da vítima foi bloqueada por motivos de fraude. Então

o fraudador fornece a opção de a vítima clicar no link para desbloqueá-la, que aparenta ser legítimo visualmente, mas ao passar o mouse logo em cima a fraude é revelada. O endereço visual na imagem indica “https://account.live.com” e na realidade ao clicar a vítima seria direcionada para “http://hotmail.com.br.log-live.com/” aonde poderá fazer automaticamente o download e instalação de um *malware* ou seguir para a página clonada do Hotmail para a obtenção das credenciais da vítima.

FIGURA 6: PHISHING – ATAQUE DA CONTA BLOQUEADA

2.6.1.2 PHARMING

Pharming é um vetor de ataque muito sofisticado, cujo objetivo é alterar o *Domain Name Server* (DNS) da vítima ou o arquivo *hosts* da máquina, ou ainda o *IPTABLE*, e quando a pessoa entrar em um site específico será direcionada automaticamente a um site clonado pelo golpista. O site será idêntico ao original, e a vítima dificilmente perceberá que ao digitar suas credenciais, as informações serão imediatamente repassadas ao hacker.

O ataque consiste em uma dupla frente, a primeira é o envenenamento do DNS e a segunda frente é em relação à página falsa. O DNS é o servidor que resolve o

nome dos sites, de uma linguagem do usuário em “www.exemplo.com” para um endereço IP, por exemplo 200.255.255.17, o qual o servidor web o reconhecerá como uma requisição válida. Quando esse tradutor de endereços é adulterado, faz com que o endereço de exemplo acima passe a traduzir para um destino malicioso, como exemplo 200.254.125.17. A vítima será direcionada sem perceber para o site clonado, na qual até mesmo a URL estará ainda original, mas somente o endereço IP do site que estará falsificado. A segunda frente do ataque consistirá no *phishing*, no qual o fraudador criará uma página falsa, idêntica a original, e conseguirá em seguida as credenciais da vítima quando ela as inserir e enviar no site clonado.

Outro modo de ataque *pharming* consiste na alteração do arquivo que traduz os endereços internamente nas máquinas, chamado de hosts, localizado no Windows em “\Windows\System32\drivers\etc\”. A alteração em sistemas Unix, como o Linux e suas distribuições, consiste em modificar o arquivo, normalmente localizado em “/etc/hosts”. Essa alteração é efetuada criando uma linha com o nome do site e em seguida o seu endereço IP, por exemplo: www.facebook.com 192.168.10.10. Quando a vítima solicitar no navegador o endereço “www.facebook.com”, ela será direcionada para 192.168.10.10 e não o IP original: 185.60.216.35. Usualmente as organizações possuem seus próprios servidores DNS e com uma invasão, o atacante irá alterar arquivos de configurações destes servidores tradutores, e farão o desvio adequado ao site malicioso.

Pharming é um ataque muito sofisticado e por esse motivo, tem um alto grau de dificuldade para ser detectado a tempo pelo usuário.

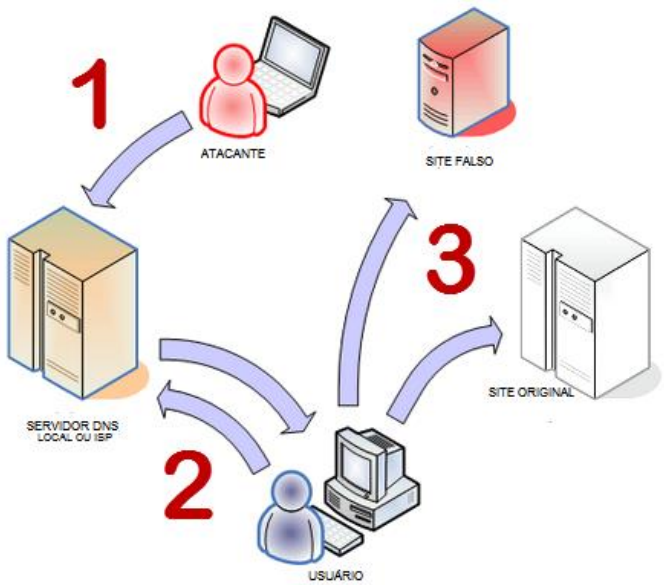

FIGURA 7: PHARMING – ENVENENAMENTO DE DNS

Na figura 7 é demonstrado o ataque *pharming*, aonde no primeiro passo o atacante irá modificar o servidor DNS, seja local ou externo (*Internet Server Provider* – ISP), no segundo passo o usuário requisitará um site e o servidor já modificado irá retornar ao invés do site original, o site falso, como mostra a terceira e última etapa.

2.6.1.3 POP-UPS

Muitos *websites* utilizam a forma de *pop-ups* para anunciar seus produtos e serviços, em estilo propaganda, em uma pequena janela externa ligada ao site. Mas os hackers utilizarão essa forma para conseguir um clique despercebido da vítima, e quando isso ocorrer ela fará automaticamente o download de um *malware* ou será direcionada a uma página falsa, cuja intenção será a coleta de informações sigilosas.

2.6.1.4 DEMITIDOS

Atualmente existe uma preocupação cada vez maior por parte das organizações quando demitem seus colaboradores. Caso o funcionário seja alguém com má índole ou revoltado com a decisão da demissão, muito provavelmente buscará prejudicar a empresa de alguma forma, seja derrubando serviços da informática, apagando arquivos, ou copiando para divulgar a quem interessar.

As organizações têm agido de modo diferente quando decidem pelo desligamento de seus colaboradores, e determinadas empresas ao chamarem o funcionário para comunicar a sua dispensa, já o acompanham para fora do local e não permitem que ele volte ou tenha acesso ao sistema de informações novamente, desativando todos as suas credenciais no sistema e acessos físicos.

2.6.2 FERRAMENTAS ESPECÍFICAS

Uma ferramenta muito utilizada por hackers para executar ataques técnicas é o *Social Engineering Toolkit* (SET), que é um conjunto de ferramentas criadas por David Kennedy, na linguagem Python, disponível para usuários de Unix.

Na figura 8, pode-se ver as opções dadas por esse verdadeiro canivete suíço que auxilia os engenheiros sociais em seus objetivos.

FIGURA 8: MENU PRINCIPAL DO SET

Com essa poderosa ferramenta é possível fazer clone de sites, testes instantâneos, criação de *payloads* e *malwares*, envio de SMS em massa, ataques em Android, infectar arquivos de mídia, e diversos outros usos necessários para um ataque eficiente.

2.6.3 SEGURANÇA FÍSICA

A segurança física em organizações é um assunto muito sério e deve ser tratado com prioridade quando o assunto é engenharia social. Existem diversas técnicas para burlar esquemas de segurança ou itens de segurança de um local.

A técnica *Lock Bumping*, que é o conhecimento e prática que uma pessoa possui para conseguir abrir cadeados e portas, com uma ferramenta específica, podendo ser um simples clipe de cabelo.

Existem cadeados mais sofisticados em forma de roda, lembrando os grandes cofres de bancos, aonde existe uma combinação para conseguir abri-los. Posteriormente houve uma evolução nos cadeados, devido às falhas detectadas nos primeiros modelos, e foi desenvolvido o modelo chamado *Master Lock*, que é um cadeado que busca eliminar brechas de segurança, como consta na figura 9.

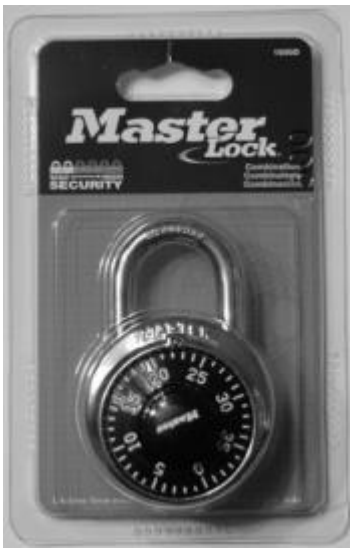

FIGURA 9: CADEADO MASTER LOCK

Mesmo com a inovação, o cadeado *Master Lock* também é vulnerável a ataques. Existe também cadeados para notebooks, aonde fixam-se cordas de metal ao equipamento e em locais fixos para evitar furtos. Esses cadeados de notebooks são de igual modo vulneráveis a ataques, então foi desenvolvido um cadeado com uma chave com numeração rolante para destravar, aumentando o nível de segurança.

Além dos cadeados, existem sensores infravermelho para detecção de intrusos em locais restritos, e que se ativam ao detectar um movimento.

As câmeras são a cada dia mais usadas e podem evitar que um engenheiro social tenha livre acesso a um local, mas para isso ocorrer, elas devem ter uma boa tecnologia e serem instaladas em locais estratégicos.

2.7 SITUAÇÃO DA ENGENHERIA SOCIAL NO BRASIL

Segundo Dmitry Bestuzhev, pesquisador da empresa de segurança da informação Kaspersky Lab, informa que 57% das fraudes on-line na América Latina ocorrem no Brasil e esse número tende de aumentar. Ainda segundo Bestuzhev, em entrevista à Globo, debate que o brasileiro para compensar seu pouco nível técnico na criação de sofisticadas armas técnicas virtuais, são mestres na engenharia social.

Essa análise de Bestuzhev explica que o brasileiro gosta de enganar, e prefere o modo amigável de conquistar os seus objetivos com suas vítimas a criar um software avançado ou ultrapassar grandes fortalezas digitais.

2.7.1 PERSPECTIVAS FUTURAS E CONSEQUÊNCIAS DA ENGENHARIA SOCIAL

Em pesquisa realizada pela Hewlett Packard (HP) em conjunto com o Instituto Ponemon, no ano de 2015, demonstra que o custo no combato a crime cibernéticos aumentou 20% naquele ano para quinze milhões de dólares anualmente. Os dados são que o uso de malwares estão em 40% dos ataques, 16% em ataques *denial of service* (DoS), 14% de engenharia social, 12% de ataques via *web*, 10% combatendo invasores internos e 7% a dispositivos roubados.

Nessa pesquisa pode-se inferir que apesar de somente 14% do total para ataques de engenharia social, somam-se também aos 40% dos *malwares*, pois um ataque de *phishing* com um arquivo malicioso é considerado um ataque da engenharia social.

Esses números tendem a crescer e futuramente, se não houver uma conscientização dos usuários que correspondem ao elo mais fraco do sistema, para impedir os ataques da engenharia social, as estatísticas tornar-se-ão em números mais graves e preocupantes.

2.8 PREVENÇÃO DOS ATAQUES DE ENGENHARIA SOCIAL

Muitas são as formas de um engenheiro social obter sucesso contra uma vítima, mas pode haver formas eficientes para evitar isso. Em cada situação há uma maneira de se prevenir de ataques de pessoas más intencionadas.

Manter o silêncio sobre situações especiais e confidenciais, e a discricionariedade é uma das primeiras formas para evitar bisbilhoteiros. Evitar publicar atos particulares ou da empresa em redes sociais também é uma forma de dificultar as ações de um engenheiro social. Evitar utilizar a camiseta da empresa, ou o crachá publicamente, desnecessariamente, para chamar a atenção e fomentar uma ação criminosa. No expediente de serviço evitar escrever senhas ou credenciais em papéis, ou manter *post-its* visíveis com informações sensíveis. E ao jogar fora papéis com determinada informação, checar se há a necessidade de trituração total para determinados documentos. Jogar no lixo somente quando tiver a certeza que nada é relevante. E quando o setor de TI desejar descartar aquela máquina velha, checar se ela foi devidamente apagada de forma a tornar irreversível a recuperação daqueles dados. Algumas dicas de discrição são importantes, como não sair para almoçar e começar a contar a rotina da empresa, ou situações confidenciais com o colega, evitar ao máximo tirar informações de dentro dos portões da empresa, sempre pode haver alguém por perto interessado em ouvir. Cuidado também com os *shoulder surfer* que estarão atentos ao que a vítima fizer, precavendo-se em não utilizar o notebook ou celular em lugares públicos, ou ao digitar senhas em terminais eletrônicos, aonde se suspeita uma movimentação estranha ou de ameaças à espreita.

A pessoa deve estar atenta em perceber se há alguém o seguindo ou querendo entrar na empresa sem a credencial para realizar um *tailgating*. E se houver, a pessoa deve impedir o acesso daquela, avisar a segurança ou a portaria e tentar identificar o invasor imediatamente. E atenção às saídas de fumar, ou conversas em grupos muito grandes, aonde um engenheiro pode se aproximar para fazer amizade com intenções de invadir os perímetros restritos da organização.

A compra de cadeados e portas seguras, com sistemas avançados e testados contra invasões é um item importante para evitar invasões indesejadas. Assim como a instalação de câmeras bem posicionadas para perceber movimentações suspeitas e na implantação de sensores infravermelho para detectar a movimentação de indivíduos não identificados em áreas seguras.

A pessoa deve ter consciência em evitar colar adesivos de identificação em carros, notebooks, celulares, entre outros, e assim dificultar a sua identificação.

No bate papo online ou em conversas em grupo pela internet, a pessoa deve estar sempre suspeitando de falsificadores de identidade, que buscarão se passar por quem não são. E sempre desconfiar de e-mails aonde passam uma sensação de urgência, ou que buscam enganar pelo aguçamento da curiosidade. Nunca clicar em links ou abrir anexos de remetentes desconhecidos e evitar se comunicar com os mesmos.

São infinitas as dicas aplicáveis de prevenir a engenharia social, mas todas não seriam úteis se o usuário não tiver a consciência de que os ataques existem e que existem pessoas más intencionadas em fazer o necessário para cumprir seus objetivos maliciosos.

2.8.1 NECESSIDADES BÁSICAS DAS EMPRESAS CONTRA OS ATAQUES

A conscientização de todos os usuários e de todas as áreas da corporação são fundamentais para prevenir possíveis ataques de engenharia social. As empresas devem manter uma política de segurança da informação sempre atualizada, com todos os itens previstos no estudo de engenharia social, inclusive no quesito de credenciais, tendo o acesso justo e necessário para a função exercida e quando houver desligamento agir de forma eficaz para cortar todos os acessos e impedir que a pessoa volte ao seu equipamento. E a gestão da empresa deve estar sempre alinhada com a segurança, tendo em mente as normas mais atuais e possuir uma equipe especializada e consciente para prevenir prováveis ataques, e poder treinar a empresa. O treinamento pode ser de forma a conscientizar por meio de folhetos, em treinamentos, palestras, vídeos, dentre outros modos para mostrar o que acontece geralmente num ataque e de como eles poderiam ser evitados, assim como na tabela 1.

Fraude	Prevenção
VISHING	• **No celular:** Desconfie de números desconhecidos ou privados e nunca acredite

	totalmente nas instruções ou ordens estranhas. • **No telefone sem identificação:** Sempre desconfie se alguém perguntar nomes, datas ou perguntas genéricas, esteja atento. • **Falso sequestro:** Caso seja informado que existe um sequestro, mantenha a calma, e verifique se a pessoa realmente está segura por outro meio de comunicação, ligando para o serviço ou conhecidos. Comunique as autoridades.
SMISHING	• **Prêmios**: Se você não participou de algum sorteio, ou não se lembra, esteja atento, nada é de graça. • **Recarga**: Se alguém oferecer dinheiro em troca de apenas uma recarga, esteja atento, certamente é uma fraude. • **Falsa identidade**: Se percebe algo estranho na mensagem, ignore ou busque encontrar a pessoa por outro meio de comunicação.
DUMPSTER DIVING	• **Descarte**: Faça o descarte de papéis importante de um modo que os deixe totalmente ilegíveis. • **Armazenamento**: Se gostaria de guardar documentos recebidos, certifique que é um local seguro e

	confidencial, sem acesso a desconhecidos.
SKIMMING	• **Lugares conhecidos**: Prefira lugares conhecidos para fazer compras com cartão, os clones e fraudes geralmente são em lugares afastados e remotos. • **Use dinheiro**: Caso o local seja suspeito, prefira usar dinheiro a cartão, a prevenção pode ajudar.
TAILGATING	• **Trabalho**: Quando entrar em lugares restritos, garanta que ninguém o seguiu ou se aproveitou de sua gentileza para invadir um local de acesso fechado. • **Casa**: Esteja atento quando entrar em sua garagem de casa, muitos ladrões estão à espreita e sabem, muitas vezes, o horário de sua rotina. Pare o carro a uma distância segura, preste atenção em movimentações estranhas, abra o portão e entre diretamente na garagem, e em seguida feche o portão imediatamente.
PIGGYBACKING	• **Desconfie:** Vigie quando alguém que aparenta ter autoridade em sua voz ou atitude e tentar convencê-lo que necessita de algo urgente, será que realmente ele é um funcionário? • **Verifique:** Questione a pessoa e verifique com outros se de fato

	aquela pessoa é conhecida e possui tais atribuições ou está habilitado para tais ações.
ENGENHARIA SOCIAL REVERSA	• **Perfil falso**: Será que realmente aquela pessoa é confiável? Desconfie de pessoas novas que estejam com fotos suspeitas ou que estejam com amigos comuns adicionados em redes sociais, garanta sua privacidade acima de tudo, alguns dos seus amigos podem adicionar qualquer pessoa e o fraudador usará disso para criar uma falsa confiança. • **Em bate-papos**: Se alguém adicioná-lo em aplicativos mensageiros, como o *Whatsapp*, desconfie de suas intenções e busque maiores informações sobre quem realmente é antes de qualquer envolvimento maior. • **Carteirada**: O clássico golpe da carteirada ainda é muito utilizado, preste atenção se alguém solicitar seus documentos ou informações pessoais, garanta que é de fato uma autoridade legítima.
ESPIONAGEM	• **Esteja atento**: Se perceber que todos os dias um determinado carro está o seguindo de longe, anote a placa e se persistir comunique as autoridades policiais.

	• **No trabalho**: Se notar que existe sempre uma pessoa o observando quando, por exemplo, sair para almoçar, questione, pode ser um admirador ou alguém buscando informações sobre a sua rotina. • **Crachá guardado**: Prefira deixar o seu crachá escondido quando sair das dependências da empresa, fraudadores estão aguardando informações sobre seu nome, função ou algum outro dado relevante. • **Sem post-its**: Abandone a ideia de grudar post-it em seu computador com dados relevantes, se algum fraudador conseguir acesso à empresa, com certeza, coletará esses dados. Ou se não for um fraudador, poderá ser um colega buscando uma oportunidade para prejudicar você. • **Cuide com as palavras**: Quando estiver almoçando em um local público, com colegas, evite conversar de assuntos corporativos e de relevância estratégica.
SHOULDER SURFING	• **Em locais públicos**: Quando utilizar notebook ou celular em público, certifique de que ninguém observa a sua tela diretamente, e

	se acontecer, mude de local e de preferência perto de uma parede. • **Remova etiquetas**: Tire as etiquetas ou adesivos as quais identificam a sua corporação, tipo de sistema operacional, alertas de confidencialidade, dentre outras notas relevantes. • **Papel de parede limpo**: Evite muitos ícones no papel de parede, são informações estratégicas para hackers descobrirem vulnerabilidades em seus aplicativos e sistemas.
HOAX	• **Verifique**: Se realmente alguém famoso faleceu, ou se houve uma grande tragédia, verifique antes de clicar no link que diz trazer fotos e vídeos, sites de notícias de confiança, e se a notícia for verdadeira, supere a tentação de clicar no link que pode ser um *malware*. • **Por e-mail**: Se um príncipe nigeriano está oferecendo milhões de dólares a você do nada, certamente você está diante de uma fraude para coleta de suas informações pessoais. Sempre atente para ofertas extraordinárias ou promoções impossíveis, normalmente são armadilhas para persuadir suas emoções.

	• **Em redes sociais**: Existem correntes de campanhas diariamente divulgadas, trazendo grande comoção com fotos emocionantes que trazem um link malicioso, evite participar ou verifique antes a sua autenticidade, na maioria das vezes é uma cilada.
PHISHING	• **Certifique**: Evite digitar parte do site e apertar ENTER para o Google buscar, por vezes ele exibirá por primeiro páginas maliciosas. Prefira digitar diretamente o endereço completo na barra de endereços. • **SPAM**: A grande maioria das pessoas já recebeu um e-mail de “lojas” com promoções inacreditáveis, da Receita Federal, dos Correios, do Banco do Brasil, dentre outros. Na maioria das vezes são armadilhas bem preparadas que direcionam para uma página falsa. Entre no site original antes e busque a oferta, e se for de algum órgão oficial, normalmente ignore ou se houver conhecimento, entre em contato por outro meio de comunicação. • **Passe o cursor do mouse**: Ao passar o mouse em cima de uma imagem, ou algo que aparenta ser

	um link, a URL real aparecerá embaixo, se não for a mesma, desconfie. Se for a mesma, desconfie de nomes longos ou que não condizem com a realidade quando você entra nesses domínios. • **Ransomware**: Seria uma grande infelicidade caso, por acidente, você clique em um link de um e-mail ou site que instale um *malware* do tipo *Ransomware*, que é um sequestro de dados virtuais. Seus dados criptografados estão perdidos, de fato, por isso mantenha SEMPRE backup atualizado de dados importantes em outros lugares, com isso a chantagem do fraudador de nada valerá, caso contrário a sua empresa ou você terão que desembolsar um grande valor para reaver seus dados.
PHARMING	• **O lugar conectado**: Evite conectar-se em Wi-Fi pública o máximo que puder. Podem ocorrer fraudes nesses lugares, aonde coletarão com páginas falsas as suas informações. • **O dispositivo certo**: Evite sempre que possível entrar em sites críticos, como bancos, em lugares desconhecidos, como *lan*

	houses, pode ocorrer que o arquivo *hosts* do computador esteja alterado ou o DNS adulterado.
DEMITIDOS	• **Desative antes**: Quando o setor de RH decidir demitir o colaborador, providenciem imediatamente a sua desativação total do sistema, sejam acessos físicos ou nos sistemas. Incluindo VPNs, e outras formas. • **Acompanhe à saída**: Se o funcionário foi demitido, ele estará, muitas das vezes, furioso e poderá se vingar na hora de buscar suas coisas em sua mesa ou quando for salvar “algumas fotos” no *pendrive*. Sempre atente e mantenha alguém junto para observar e questionar, e se possível, evite que ele mexa novamente no equipamento. • **Política de segurança**: Inclua cláusulas no contrato de trabalho que indiquem a responsabilidade dos colaboradores sobre o uso de dados e informações, e suas responsabilidades civis e criminais sobre tais. E mencione sobre o momento da demissão para que esteja ciente de que não poderá mexer mais no equipamento ou ter qualquer tipo de acesso à sistemas.

SEGURANÇA FÍSICA	• **Cadeados**: Se tiver portas ou janelas que permitam acessos restritos, invista em cadeados de boa qualidade e certificados, o preço será justificado pelo valor de suas informações. • **Câmeras**: Instale um sistema eficiente de câmeras de alta tecnologia, em lugares estratégicos, e que não permitam que um *tailgating*, por exemplo, seja executado sem que seja percebido. • **Sensores de presença**: Instale sensores de presença em lugares que evitem o "sombreamento", aonde o fraudador pode se livrar do alcance. • **Portas seguras**: O alto investimento na forma em como o colaborador entra em lugares restritos é justificável e esperado. Prefira sensores biométricos, e com senhas particulares, com identificação da hora e dia da entrada e saída.

TABELA 1: BOAS PRÁTICAS
FONTE: AUTORIA PRÓPRIA

2.9 A CULTURA ORGANIZACIONAL

Dentre todos os aspectos anteriores estudados, a cultura organizacional acaba se destacando pela razão de afetar diretamente as políticas de segurança da empresa e ocasionando a facilitação das fraudes ocorrerem.

A cultura organizacional constitui-se de crenças comuns que se refletem nas tradições e nos hábitos, em manifestações mais ou menos tangíveis (Mintzberg et al, 2000). E essa cultura é fundamental para o desenvolvimento organizacional e dos indivíduos que a compõe, assim como no envolvimento destes.

Segundo Sampaio, aonde descreve a cultura sendo formada por um conjunto de características típicas como as normas, crenças e valores, e as estratégias e que são formadas com base nos recursos disponíveis na organização de acordo com a realidade do mercado e de concorrência.

No aspecto da engenharia social, é necessária uma adaptação de estratégias na criação e manutenção das políticas de segurança da informação das organizações. Faz-se necessária uma maior flexibilização e constante mudança nos aspectos abrangidos e que podem estar sendo subestimados pelas empresas.

A cultura organizacional, inclusive, pode engessar em aspectos gerais as políticas de segurança, ocasionando uma facilitação na prática das fraudes pelos engenheiros sociais. Exemplo disso seria uma empresa utilizar um sistema de criptografia ultrapassado, ou obsoleto, ou mesmo armazenar arquivos importantes em papéis, nos antigos arquivos ao invés de um sofisticado sistema de informação com *backup*.

Uma gestão preocupada com a segurança de sua organização, ousará ultrapassar as barreiras culturais e de crenças encrustadas em suas antigas políticas. Com essa flexibilização, os gestores buscarão cobrir todas as áreas da empresa com uma política de segurança ampla e abrangente, mitigando os riscos e danos dos ataques da engenharia social.

3. METODOLOGIA

A pesquisa trata-se do estudo dos danos e do alcance da engenharia social num grupo aleatório da sociedade brasileira. E visa estudar a relação dos crimes cometidos, muitas das vezes despercebidos, e também das atitudes dos usuários em detrimento de algumas situações de risco. O embasamento teórico foi buscado em literaturas sobre Tecnologia da Informação e materiais derivados da segurança destas informações criadas, armazenadas e apagadas pelas organizações.

Os métodos utilizados pela pesquisa são: observacional, comparativo, experimental e estatístico. A escolha de diversos métodos fundamenta-se pela abrangência psicológica, técnica e social envolvida no tema. Segundo Gil, (2008, p.15), o método observacional é um dos mais utilizados nas ciências sociais, sendo que neste estudo apenas observa algo que acontece ou já aconteceu, sendo melhor aproveitado com outros métodos em conjunto. O método comparativo, segundo Gil, (2008, p.15), “procede pela investigação de indivíduos, classes, fenômenos ou fatos, com vistas a ressaltar as diferenças e similaridades entre eles”. Conforme Gil, (2008, p.16), o método experimental se trata “essencialmente em submeter os objetos de estudo à influência de certas variáveis, em condições controladas e conhecidas pelo investigador, para observar os resultados que a variável produz no objeto. ”. E por fim, conforme Gil, (2008, p.17), o método estatístico “fundamenta-se na aplicação da teoria estatística da probabilidade e constitui importante auxílio para a investigação em ciências sociais... Mediante a utilização de testes estatísticos, torna-se possível determinar, em termos numéricos, a probabilidade de acerto de determinada conclusão, bem como a margem de erro de um valor obtido... Os procedimentos estatísticos fornecem considerável reforço às conclusões obtidas, sobretudo mediante a experimentação e a observação.”.

A coleta de dados foi realizada por meio de questionário disponibilizado virtualmente, contendo a maioria das questões fechadas e algumas alternativas abertas para aferir o máximo possível de informações dos entrevistados. Segundo Gil, (2008, p.121), o questionário “é a técnica de investigação composta por um conjunto de questões que são submetidas a pessoas com o propósito de obter informações sobre conhecimentos, crenças, sentimentos, valores, interesses, expectativas, aspirações, temores, comportamento presente ou passado etc. Construir um questionário consiste basicamente em traduzir objetivos da pesquisa em questões

específicas. As respostas a essas questões é que irão proporcionar os dados requeridos para descrever as características da população pesquisada ou testar as hipóteses que forma construídas durante o planejamento da pesquisa.”. A pesquisa é quantitativa, conforme Fonseca (2002, p.20), “a pesquisa quantitativa se centra na objetividade. Influenciada pelo positivismo, considera que a realidade só pode ser compreendida com base na análise de dados brutos, recolhidos com o auxílio de instrumentos padronizados e neutros. A pesquisa quantitativa recorre à linguagem matemática para descrever as causas de um fenômeno, as relações entre variáveis etc.” O objetivo da pesquisa é explicativa e exploratória, segundo Gil (2008), a pesquisa exploratória “tem como objetivo proporcionar maior familiaridade com o problema, com vistas a torna-lo mais explícito ou a construir hipóteses” e sobre a pesquisa explicativa “preocupa-se em identificar os fatores que determinam ou que contribuem para a ocorrência dos fenômenos”.

4. LEVANTAMENTO DE DADOS E ANÁLISE DOS RESULTADOS

4.1 NÍVEL DE CONHECIMENTO DO ASSUNTO

Com a intenção de saber o nível de conhecimento dos participantes, quatro perguntas foram feitas.

A primeira pergunta, com o resultado demonstrado na tabela 2 e gráfico 1, questiona o nível de conhecimento prévio do assunto, sendo essa a primeira pergunta do questionário.

QUAL É O SEU NÍVEL DE CONHECIMENTO SOBRE O TEMA "ENGENHARIA SOCIAL"?	FREQUÊNCIA	PERCENTUAL
Total conhecimento e domínio do assunto	2	1,8%
Possuo algum conhecimento	51	44,7%
Indiferente	6	5,3%
Já ouvi falar pela mídia	28	24,6%
Nenhum	27	23,7%
Total	114	100%

TABELA 2: PESQUISA - NÍVEL DE CONHECIMENTO
FONTE: PESQUISA DESTE TRABALHO

Infere-se que 48,3% não tem nenhum conhecimento ou apenas já ouviu falar pela mídia quando há alguma notícia muito relevante. Apenas 1,8% têm um profundo conhecimento do assunto, e a maioria absoluta com 44,7% possui algum conhecimento.

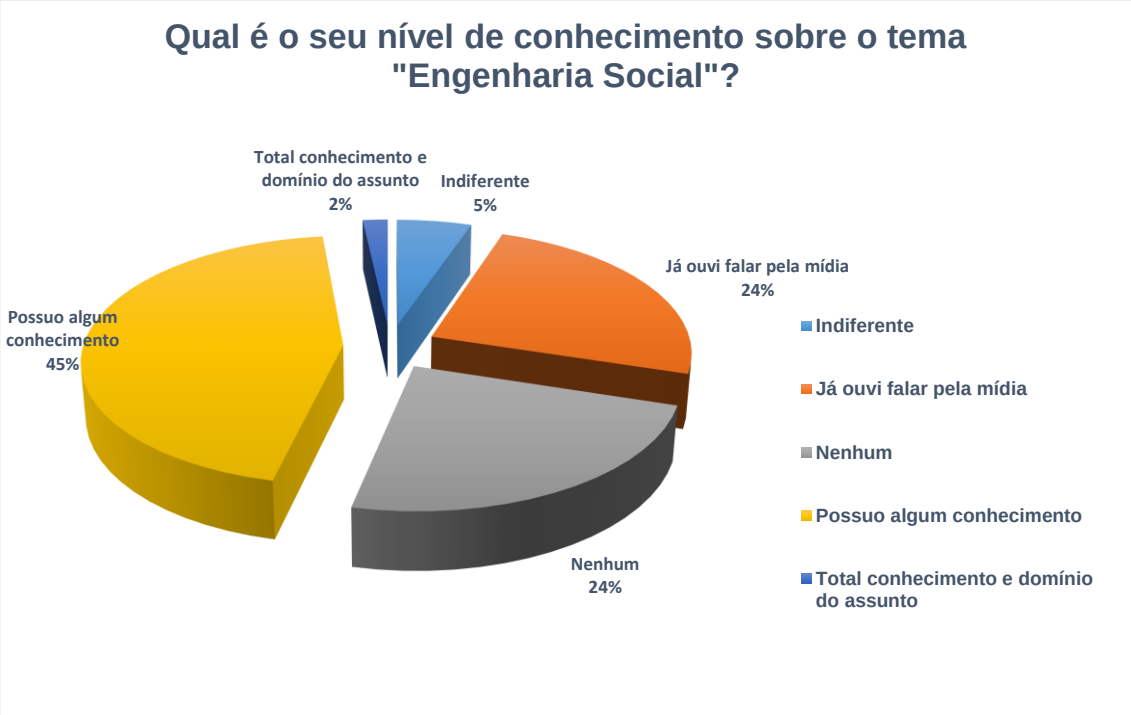

GRÁFICO 1: PESQUISA - NÍVEL DE CONHECIMENTO
FONTE: PESQUISA DESTE TRABALHO

A próxima pergunta questiona a gravidade para a organização se informações fossem perdidas. A tabela 3 e o gráfico 2 demonstram a situação.

SE HOUVESSE A PERDA DE SIGILO DE INFORMAÇÕES CRUCIAIS E ESTRATÉGICAS DE SUA ORGANIZAÇÃO, ISSO PODERIA SER GRAVE AOS NEGÓCIOS?	FREQUÊNCIA	PERCENTUAL
Sim	97	85,1%
Não	4	3,5%
Talvez	13	11,4%
Total	114	100%

TABELA 3: PESQUISA - PERDA DE SIGILO
FONTE: PESQUISA DESTE TRABALHO

Com a esmagadora maioria de 85,1%, ou noventa e sete participantes, demonstraram que as informações para as suas organizações são importantes e gerariam grandes danos aos negócios se perdidas. Os 11,4% respondendo “Talvez” pode ser atrelado à classificação da informação na organização e isso dependeria do volume de informações furtado ou a determinadas áreas da empresa.

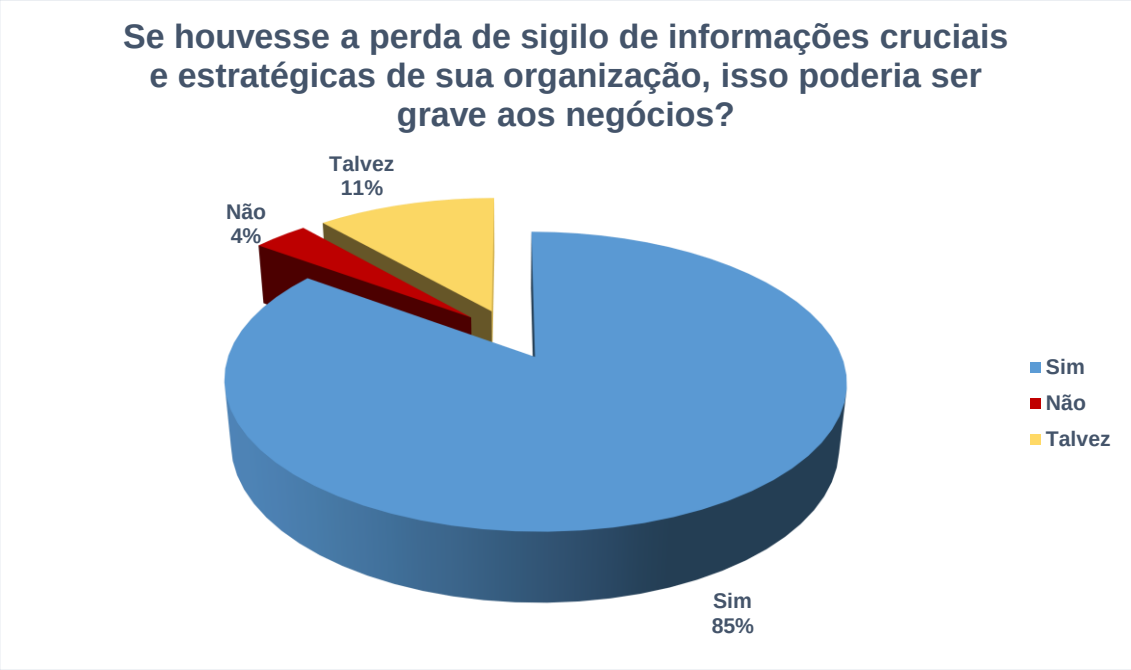

GRÁFICO 2: PESQUISA - PERDA DE SIGILO
FONTE: PESQUISA DESTE TRABALHO

A próxima pergunta buscou aferir se o participante tem algum conhecimento da aplicação de vários tipos de fraudes na engenharia social, a tabela 4 e gráfico 3, demonstram o resultado.

QUAIS DOS SEGUINTES GOLPES DE ENGENHARIA SOCIAL VOCÊ TEM ALGUM CONHECIMENTO DE SUA APLICAÇÃO:	FREQUÊNCIA SIM (PERCENTUAL)	FREQUÊNCIA NÃO (PERCENTUAL)
Phishing	89 (78,1%)	25 (21,9%)
Vishing	88 (77,2%)	26 (22,8%)
Espionagem	85 (74,6%)	29 (25,4%)
Skimming	81 (71,7%)	33 (28,9%)
Tombstone Theft	73 (64%)	41 (36%)
Piggybacking	72 (63,2%)	42 (36,8%)
SMiShing	68 (59,6%)	46 (40,4%)
Engenharia Social Reversa	66 (57,9%)	48 (42,1%)
Dumpster Diving	62 (54,4%)	52 (45,6%)
Pharming	50 (43,9%)	64 (56,1%)

Shoulder Surfing	43 (37,7%)	71 (62,3%)
Tailgating	41 (36%)	73 (64%)
Total	818 (59,7%)	550 (40,3%)

TABELA 4: PESQUISA - GOLPES DA ENGENHARIA
FONTE: PESQUISA DESTE TRABALHO

A tabela 4 foi classificada apenas para fins demonstrativos neste trabalho, o questionário era aleatoriamente mudado a cada novo participante, mas com as mesmas fraudes descritas. Ao lado de cada fraude, foi feita uma breve descrição de seu significado.

Phishing e *Vishing* tiveram as maiores porcentagens para quem conhece essas fraudes, dentre todas, com 78,1% e 77,2%, respectivamente, e *Tailgating* teve a maior porcentagem para quem não conhece o golpe com 64% dos participantes. Assim como *Shoulder Surfing* que ficou logo em seguida com 62,3% de desconhecimento. De modo geral, 59,7% dos participantes afirmaram conhecer alguma das doze fraudes propostas, e 40,3% responderam negativamente.

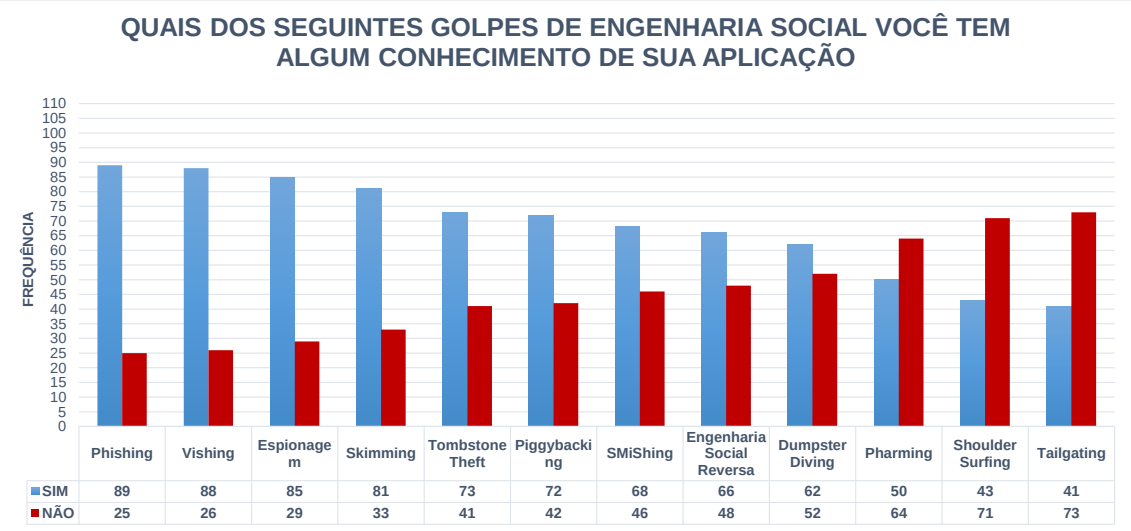

GRÁFICO 3: PESQUISA - GOLPES DA ENGENHARIA
FONTE: PESQUISA DESTE TRABALHO

A última pergunta relacionada ao nível de conhecimento do participante, tem como objetivo saber se a organização já forneceu treinamento ou algum tipo de instrução aos seus colaboradores, em algum tempo. O resultado demonstrado na tabela 5 e gráfico 4 dá argumentos para uma melhor discussão sobre o tema.

A SUA EMPRESA JÁ OFERECEU ALGUM TREINAMENTO OU FORNECEU INSTRUÇÕES	FREQUÊNCIA	PERCENTUAL

DE PREVENÇÃO SOBRE O TEMA EM QUESTÃO?		
Sim	36	31,6%
Não	78	68,4%
Total	114	100%

TABELA 5: PESQUISA - TREINAMENTO
FONTE: PESQUISA DESTE TRABALHO

Fica nítida a despreocupação da maioria das empresas em treinar os seus colaboradores em relação ao tema estudado, de fato uma preocupante informação, com 68,4% respondendo que nunca receberam nenhum tipo de treinamento ou instrução.

GRÁFICO 4: PESQUISA - TREINAMENTO
FONTE: PESQUISA DESTE TRABALHO

4.2 OS DANOS DA ENGENHARIA SOCIAL

Essa parte da pesquisa está relacionada a todos os danos, ou ao alcance em que as fraudes da engenharia social atingiram, de alguma maneira, os participantes da pesquisa.

4.2.1 SPAM

O recebimento de SPAM é uma antiga, e ainda muito utilizada, forma de atingir o público, e estão relacionados a espalhar *malwares, phishing, pharming*, e gerar prejuízos financeiros e de roubo de informações. Assim como no uso do espaço reservado nas caixas de mensagens dos usuários. A tabela 6 e gráfico 5 mostra como a situação está atualmente no recebimento de um e-mail falso.

JÁ RECEBEU UM E-MAIL FALSO?	FREQUÊNCIA	PERCENTUAL
Sim	109	95,6%
Não	5	4,4%
Total	114	100%

TABELA 6: PESQUISA - E-MAIL FALSO
FONTE: PESQUISA DESTE TRABALHO

Quase a totalidade dos participantes, com 95,6%, respondeu que já recebeu um e-mail falso, alguma vez. Apenas 4,4% nunca recebeu. Infere-se que essa prática é vastamente utilizada.

GRÁFICO 5: PESQUISA - E-MAIL FALSO
FONTE: PESQUISA DESTE TRABALHO

Para ter o conhecimento necessário se o usuário clica ou não no link ou anexo contido, a próxima pesquisa, demonstrada na tabela 7 e gráfico 6 a seguir, prova que a maioria nunca caiu na armadilha proposta.

SE JÁ RECEBEU UM E-MAIL FALSO: CHEGOU A CLICAR NO LINK OU NO ANEXO NELE CONTIDO, EM SEU DISPOSITIVO, POR CURIOSIDADE?	FREQUÊNCIA	PERCENTUAL
Sim	27	23,7%
Não	84	73,7%
Nunca recebi	3	2,6%
Total	114	100%

TABELA 7: PESQUISA - RECEBEU E-MAIL FALSO
FONTE: PESQUISA DESTE TRABALHO

Com 73,7%, apesar de receberem os e-mails falsos, não clicam no link ou anexo contidos, pode-se concluir que a maioria da população tem a consciência dos riscos ao receber um e-mail suspeito.

GRÁFICO 6: PESQUISA - RECEBEU E-MAIL FALSO
FONTE: PESQUISA DESTE TRABALHO

4.2.2 CLIQUE ENGANOSO

O clique enganoso ocorre enquanto o usuário navega em um site, e sem querer acaba clicando em uma propaganda ou link, ou levado a clicar em algum local obrigatório para prosseguir. A tabela 8 e gráfico 7, demonstram os resultados.

JÁ CLICOU EM UM LINK DE FORMA ENGANOSA ENQUANTO NAVEGAVA EM ALGUM SITE	FREQUÊNCIA	PERCENTUAL
Sim	94	82,5%
Não	20	17,5%
Total	114	100%

TABELA 8: PESQUISA - ENGANO AO CLICAR
FONTE: PESQUISA DESTE TRABALHO

Com a grande maioria, com 82,5% dos participantes, afirmaram já terem clicado de forma enganosa em algum link enquanto navegavam. Um resultado preocupante que demonstra como os websites têm se especializado em ocultar propagandas, e consequentemente, inerente ao assunto, links maliciosos.

GRÁFICO 7: PESQUISA - ENGANO AO CLICAR
FONTE: PESQUISA DESTE TRABALHO

4.2.3 PHISHING OU PHARMING

Essa questão é relacionada diretamente às práticas de *phishing* ou *pharming*, quando o usuário é levado a entrar em determinado endereço, e se ao entrar nesse endereço malicioso digitará informações confidenciais, causando danos de alguma forma. A tabela 9 e gráfico 8 demonstram os resultados.

JÁ DIGITOU INFORMAÇÕES CONFIDENCIAIS EM SITES NÃO SEGUROS QUE CAUSARAM DANOS DE ALGUMA FORMA?	FREQUÊNCIA	PERCENTUAL
Sim	11	9,6%
Não	103	90,4%
Total	114	100%

TABELA 9: PESQUISA - DIGITAR INFORMAÇÕES CONFIDENCIAIS
FONTE: PESQUISA DESTE TRABALHO

A maioria, com 90,4%, dos usuários pesquisados respondeu que nunca digitou informações confidenciais em sites não seguros causando algum dano. Apenas 9,6% dos usuários efetivamente sofreu as consequências de uma fraude desse tipo. Infere-se a maior consciência dos usuários em se prevenir desses conhecidos golpes.

GRÁFICO 8: PESQUISA - DIGITAR INFORMAÇÕES CONFIDENCIAIS
FONTE: PESQUISA DESTE TRABALHO

4.2.4 TELEFONEMAS (VISHING)

Uma das mais antigas formas de fraude, que é a fraude telefônica, foi alvo de questionamento. O gráfico 9 e tabela 10 demonstram o resultado.

ALGUMA VEZ VOCÊ JÁ RECEBEU UM TELEFONEMA COM UMA TENTATIVA DE FRAUDE? SOBRE SEQUESTRO, UM PRÊMIO, BANCO...	FREQUÊNCIA	PERCENTUAL
Sim	73	64%
Não	37	32,5%
Talvez	4	3,5%
Total	114	100%

TABELA 10: PESQUISA - RECEBEU TELEFONEMA
FONTE: PESQUISA DESTE TRABALHO

A maioria das pessoas já recebeu uma ligação de um fraudador, com 64%, e curiosamente 3,5% não sabem se efetivamente era uma fraude, e 32,5% nunca receberam um telefonema desse tipo.

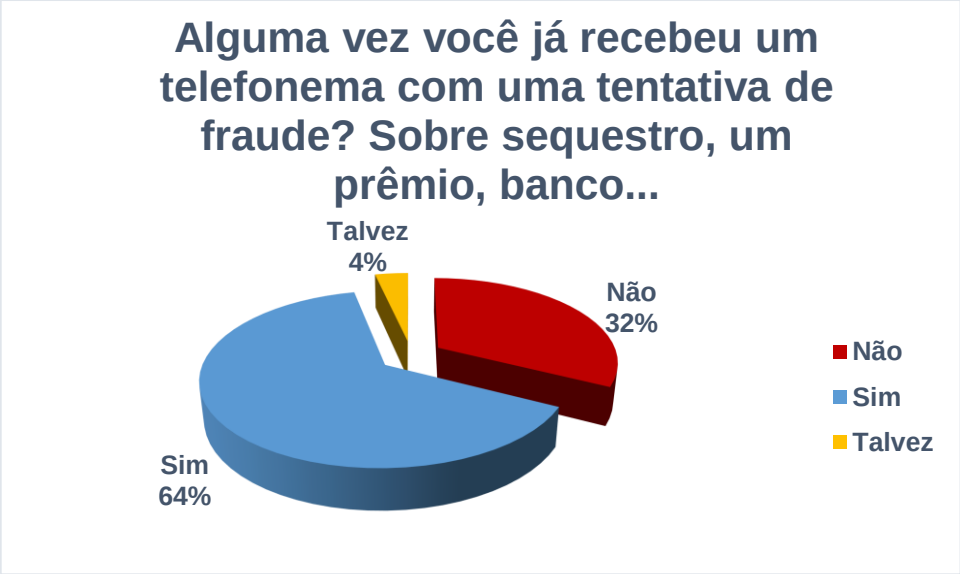

GRÁFICO 9: PESQUISA - RECEBEU TELEFONEMA
FONTE: PESQUISA DESTE TRABALHO

Para saber se após receber a ligação do fraudador, o participante foi perguntado se ao receber a ligação do fraudador, chegou a realizar o pedido e concluiu efetivamente o golpe. A tabela 11 e gráfico 10 mostram o resultado.

SE JÁ RECEBEU A LIGAÇÃO DE UM FRAUDADOR, CHEGOU A REALIZAR O QUE FOI PEDIDO?	FREQUÊNCIA	PERCENTUAL
Sim	6	5,3%
Não	75	65,8%
Nunca me ligaram	33	28,9%
Total	114	100%

TABELA 11: PESQUISA - FEZ O QUE FOI PEDIDO NO VISHING
FONTE: PESQUISA DESTE TRABALHO

Como esperado, pelo maior nível de conscientização e também por ser uma forma muito antiga de engenharia social, apenas 5,3% já realizaram o pedido do fraudador. 65,8% não realizaram o pedido, frustrando os objetivos do golpista.

GRÁFICO 10: PESQUISA - FEZ O QUE FOI PEDIDO NO VISHING
FONTE: PESQUISA DESTE TRABALHO

4.2.5 SMISHING

O ataque por SMS, quando o atacante envia uma mensagem de texto curta à vítima, dizendo que ela ganhou um sorteio, um prêmio, ou similar, possuindo um link para clicar, foi alvo de pesquisa. A tabela 12 e gráfico 11 demonstram o resultado.

JÁ RECEBEU UM SMS FALSO DE UM SORTEIO QUE TENHA GANHO UM PRÊMIO, OU CRÉDITOS ADICIONAIS, NO QUAL TENHA QUE CLICAR NUM LINK OU LIGAR PARA ALGUM NÚMERO?	FREQUÊNCIA	PERCENTUAL
Sim	107	93,9%
Não	7	6,1%
Total	114	100%

TABELA 12: PESQUISA - RECEBEU SMISHING
FONTE: PESQUISA DESTE TRABALHO

93,9% dos participantes responderam que já receberam um SMS falso, e apenas 6,1% responderam nunca ter recebido. Demonstra que esse é uma fraude muito utilizada e de vasto alcance.

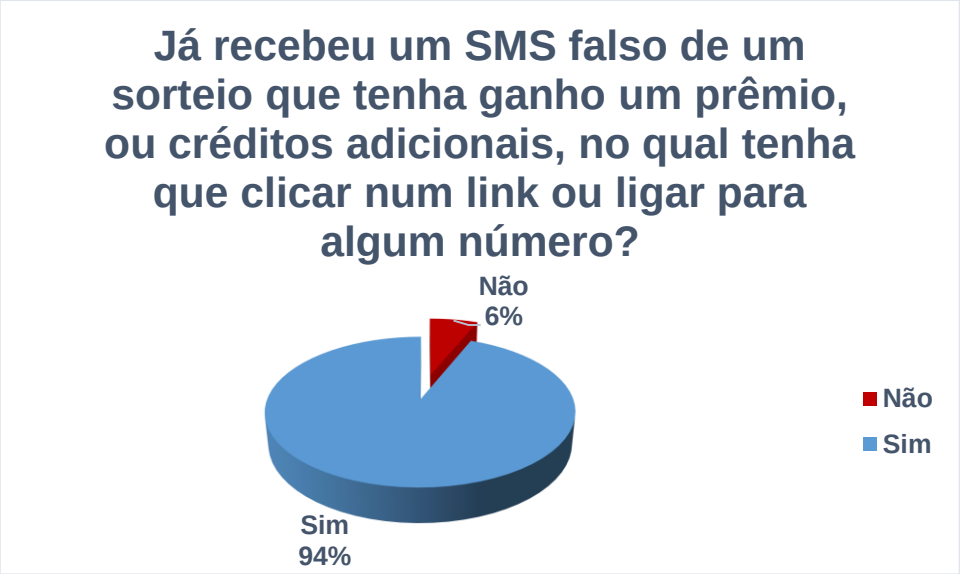

GRÁFICO 11: PESQUISA - RECEBEU SMISHING
FONTE: PESQUISA DESTE TRABALHO

Para saber se o golpe foi efetivamente concluído, a próxima pergunta foi para revelar quantas pessoas chegar a concluir a fraude. Demonstradas na tabela 13 e gráfico 12.

SE RECEBEU O SMS FALSO, CHEGOU A CLICAR NO LINK OU LIGAR PARA O NÚMERO?	FREQUÊNCIA	PERCENTUAL
Sim	4	3,5%
Não	104	91,2%
Nunca recebi	6	5,3%
Total	114	100%

TABELA 13: PESQUISA - GOLPE SMISHING
FONTE: PESQUISA DESTE TRABALHO

91,2% dos participantes não caíram na fraude, e apenas 3,5% concluíram o golpe. Afere-se uma grande conscientização dos usuários em se prevenir e que essa fraude antiga, é muito bem conhecida e dificilmente terá sucesso.

GRÁFICO 12: PESQUISA - GOLPE SMISHING
FONTE: PESQUISA DESTE TRABALHO

4.2.6 HOAX

Hoax, que é um boato divulgado em redes socais, e-mail, e nessa pergunta foi inquerido se o participante já clicou em algum *link* ou imagem por curiosidade ou desconhecimento. A tabela 14 e gráfico 13 demonstram o resultado.

JÁ CLICOU NA IMAGEM OU LINK DE UM BOATO NUM SITE, OU REDE SOCIAL, POR CURIOSIDADE OU DESCONHECIMENTO?	FREQUÊNCIA	PERCENTUAL
Sim	75	65,8%
Não	39	34,2%
Total	114	100%

TABELA 14: PESQUISA - HOAX
FONTE: PESQUISA DESTE TRABALHO

A grande maioria dos pesquisados afirmou que já clicou no link ou imagem, com 65,8%. 34,2% afirmaram nunca clicar. De fato essa fraude é muito utilizada e tem, de fato, efetividade em seu propósito. Ao clicar no link o usuário poderá instalar um *malware*, ser direcionado a uma página falsa ou outra consequência. O sucesso dessa fraude está relacionada diretamente ao grau de emotividade e apresentação da notícia ou boato, tendo um amplo alcance.

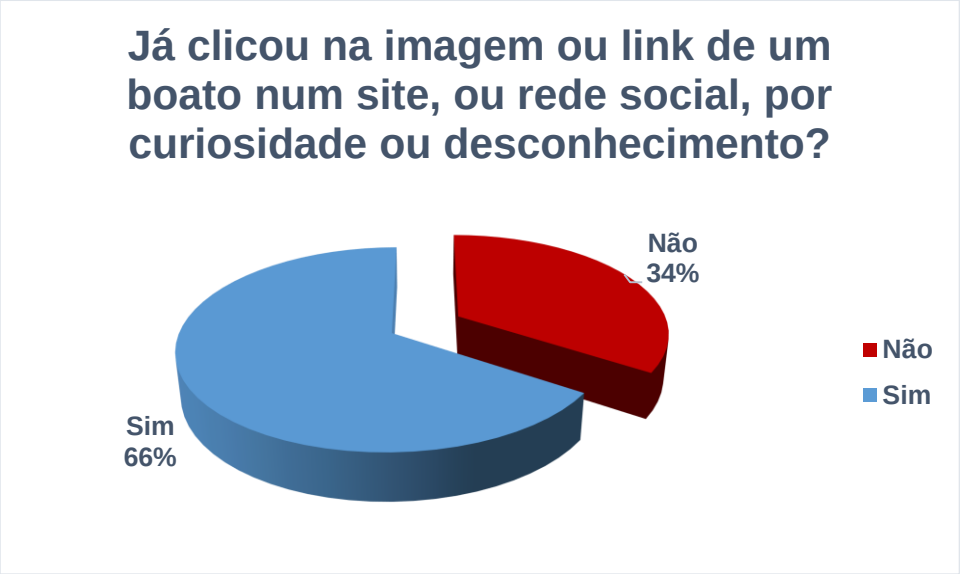

GRÁFICO 13: PESQUISA - HOAX
FONTE: PESQUISA DESTE TRABALHO

4.2.7 RANSOMWARE

Um perigoso *malware* difundido nos últimos anos, aonde informações são sequestradas ao serem criptografadas no próprio dispositivo do usuário, aonde o hacker solicita dinheiro para a liberação da chave. A tabela 15 e gráfico 14 revelam quantos participantes já sofreram ou conheceram alguém que já sofreu essa fraude.

JÁ SOFREU UM ATAQUE DE RANSOMWARE (SEQUESTRO DE DADOS VIRTUAIS) OU CONHECE ALGUÉM QUE TENHA SOFRIDO?	FREQUÊNCIA	PERCENTUAL
Sim	34	29,8%
Não	80	70,2%
Total	114	100%

TABELA 15: PESQUISA - RANSOMWARE
FONTE: PESQUISA DESTE TRABALHO

A maioria dos participantes respondeu que nunca sofreu esse tipo de ataque, com 70,2% e 29,8% respondeu que já sofreu ou conheceu alguém que sofreu esse novo tipo de fraude online. É um número preocupante de respostas positivas, de quase um terço, pelo dano causado ao usuário ou organização, caso a vítima não possua um backup em seu ambiente, terá que arcar com valores determinados pelo fraudador, e submeter-se a perder os dados para sempre. A origem dessa fraude geralmente é por meio de um e-mail falso.

GRÁFICO 14: PESQUISA - RANSOMWARE
FONTE: PESQUISA DESTE TRABALHO

4.2.8 SHOULDER SURFING

Shoulder surfing é a atitude de estar sendo espionado enquanto utiliza um notebook ou outro dispositivo, em público, e o fraudador observar tudo que é escrito ou o que possui de programas no equipamento. A próxima pergunta questiona se o participante já notou estar sendo espionado nessa situação, na tabela 16 e gráfico 15.

ALGUMA VEZ JÁ NOTOU ESTAR SENDO ESPIONADO (SHOULDER SURFER) ENQUANTO UTILIZAVA O NOTEBOOK OU CELULAR AO ACESSAR INFORMAÇÕES SIGILOSAS EM LOCAIS PÚBLICOS?	FREQUÊNCIA	PERCENTUAL
Sim	22	19,3%
Não	80	70,2%
Talvez	12	10,5%
Total	114	100%

TABELA 16: PESQUISA - SHOULDER SURFING
FONTE: PESQUISA DESTE TRABALHO

70,2% nunca perceberam alguém tentando observar o que estava sendo escrito, e 10,5% já desconfiaram estarem sendo observados. 19,3% já teve a certeza de que alguém observa o seu equipamento enquanto usava em público. Essa fraude

é a segunda mais desconhecida nessa pesquisa e possui um grau relevante de resposta positiva, pois somando a resposta positiva com a desconfiança, dá-se 29,8%.

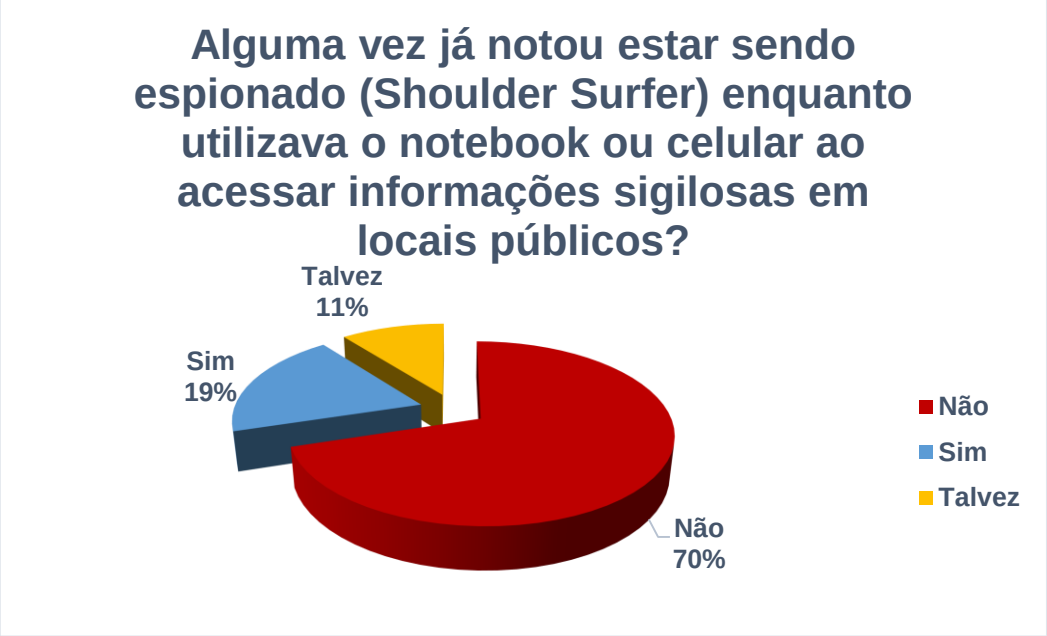

GRÁFICO 15: PESQUISA - SHOULDER SURFING
FONTE: PESQUISA DESTE TRABALHO

4.2.9 PIGGYBACKING

O questionário questionou o participante sobre a fraude de piggybacking, aonde alguém tenta se passar por quem não era para conseguir acesso físico à organização ou acessos ao sistema e informações privilegiadas. Na tabela 17 e gráfico 16, os resultados são demonstrados.

ALGUÉM, EM SEU CONHECIMENTO, JÁ TENTOU SE PASSAR POR QUEM NÃO ERA, POR TELEFONE, E-MAIL OU FISICAMENTE, PARA CONSEGUIR VANTAGENS DE ACESSO FÍSICO, AO SISTEMA OU INFORMAÇÕES PRIVILEGIADAS?	FREQUÊNCIA	PERCENTUAL
Sim	31	27,2%
Não	79	69,3%
Talvez	4	3,5%
Total	114	100%

TABELA 17: PESQUISA - PIGGYBACKING
FONTE: PESQUISA DESTE TRABALHO

A grande maioria dos participantes respondeu que não sofreu essa fraude, com 69,3%, e 27,2% já sofreu. 3,5% não souberam dizer se sim, e pode-se aferir que muitas das vezes o fraudador pode ter desistido da fraude, ou alguma parte do seu propósito foi mal sucedida.

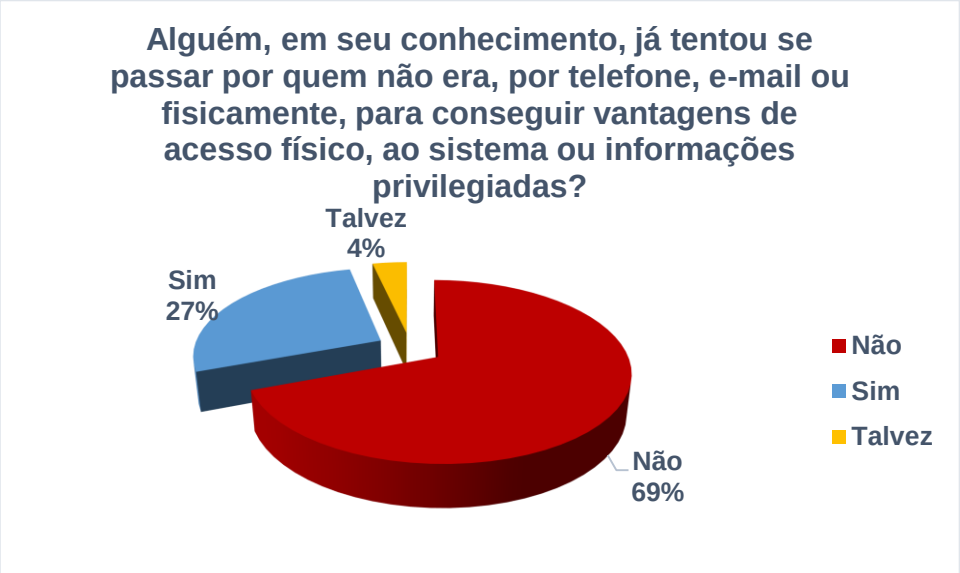

GRÁFICO 16: PESQUISA - PIGGYBACKING
FONTE: PESQUISA DESTE TRABALHO

4.2.10 DOS DEMITIDOS

Após a demissão, ex-colaboradores podem se vingar de suas empresas antigas. Esse assunto foi alvo de questionamento na pesquisa, demonstrada na tabela 18 e gráfico 17.

CONHECE ALGUÉM QUE TENHA SE VINGADO (PELO SISTEMA DE INFORMAÇÕES) DE SUA EMPRESA POR MOTIVO DE DEMISSÃO?	FREQUÊNCIA	PERCENTUAL
Sim	18	15,8%
Não	96	84,2%
Total	114	100%

TABELA 18: PESQUISA - DOS DEMITIDOS
FONTE: PESQUISA DESTE TRABALHO

Apenas 15,8% dos participantes informaram que conhece alguém que tenha se vingado de sua empresa por motivo de demissão, e esse é um número preocupante tendo em conta ao alto grau de danos possíveis que esses ex-funcionários podem causar. E 84,2% responderam que não souberam ainda de alguém que tenha se vingado. É notória a necessidade de uma política específica às empresas para prevenir tais casos e mitigar o máximo possível os danos.

GRÁFICO 17: PESQUISA - DOS DEMITIDOS
FONTE: PESQUISA DESTE TRABALHO

4.2.11 SKIMMING

A fraude de clone de cartões foi motivo de questionamento na pesquisa. A tabela 19 e gráfico 18 revelam o resultado de quantas pessoas já passaram por isso, ou se conhecem alguém que tenha passado.

JÁ SOUBE DE ALGUM CONHECIDO, OU VOCÊ JÁ PASSOU PELA SITUAÇÃO, NA QUAL O CARTÃO DE CRÉDITO TENHA SIDO CLONADO?	FREQUÊNCIA	PERCENTUAL
Sim	40	35,1%
Sim, um conhecido já passou por isso	57	50%
Não	17	14,9%
Total	114	100%

TABELA 19: PESQUISA - SKIMMING
FONTE: PESQUISA DESTE TRABALHO

O número positivo surpreende, são 35,1% que já teve o seu cartão clonado e 50% informou que conhece alguém que tenha sofrido esse golpe. Apenas 14,9% informou não ter passado ou conhecido alguém que tenha passado por essa frustrante situação. O número de participantes que respondeu positivamente, provavelmente passou por locais não confiáveis para inserir o cartão, ou até mesmo em agências bancárias nos fins de semana, aonde os fraudadores alteram as máquinas com dispositivos chamados “chupa-cabra” na qual clonam os cartões inseridos e coletam a senha. Além de outras fraudes conhecidas com os cartões de crédito.

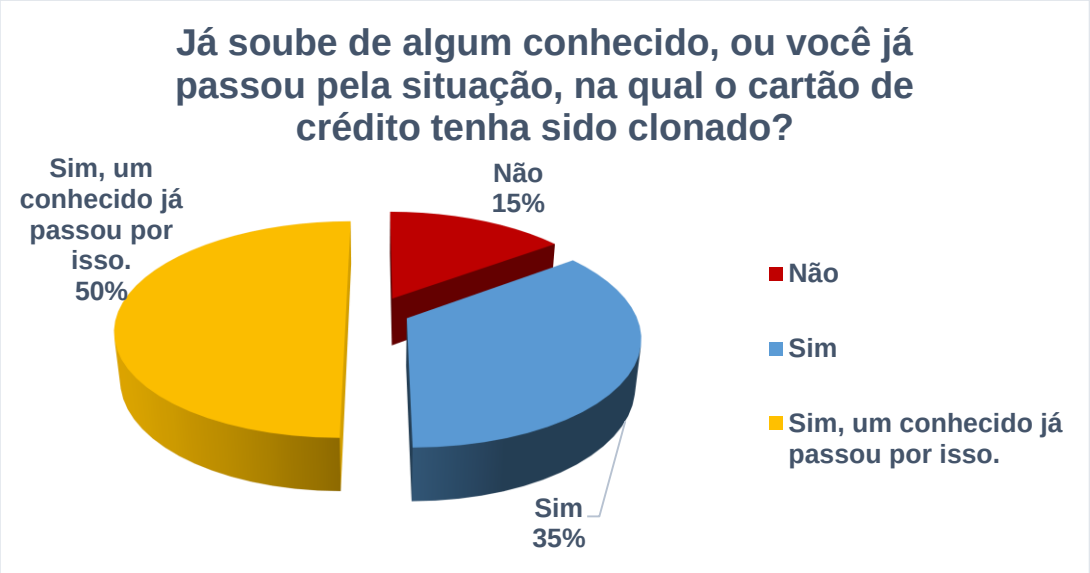

GRÁFICO 18: PESQUISA - SKIMMING
FONTE: PESQUISA DESTE TRABALHO

4.2.12 FRAUDE EM BANCOS

A pesquisa questionou os participantes sobre as fraudes online em bancos, se já passaram por essa situação ou conhecem alguém que já passou por isso. A tabela 20 e gráfico 19 mostram o resultado.

JÁ SOFREU UMA FRAUDE ONLINE NUM BANCO? COM PREJUÍZOS FINANCEIROS? OU CONHECE ALGUÉM QUE TENHA SOFRIDO...	FREQUÊNCIA	PERCENTUAL
Sim	19	19,7%
Sim, um conhecido já passou por isso	42	36,8%
Não	53	46,5%

Total	114	100%

TABELA 20: PESQUISA - FRAUDE EM BANCOS
FONTE: PESQUISA DESTE TRABALHO

Novamente é um número expressivo de respostas positivas, com 19,7% para sim, e 36,8% para que um conhecido já passou por isso, totalizando 56,5% de respostas positivas contra 46,5% negativas. Essa fraude pode ter sido causada por um *malware*, por um *phishing* ou *pharming*, ou por alguma outra forma que gerou prejuízo ao usuário. Geralmente a origem desses ataques é por um e-mail falso.

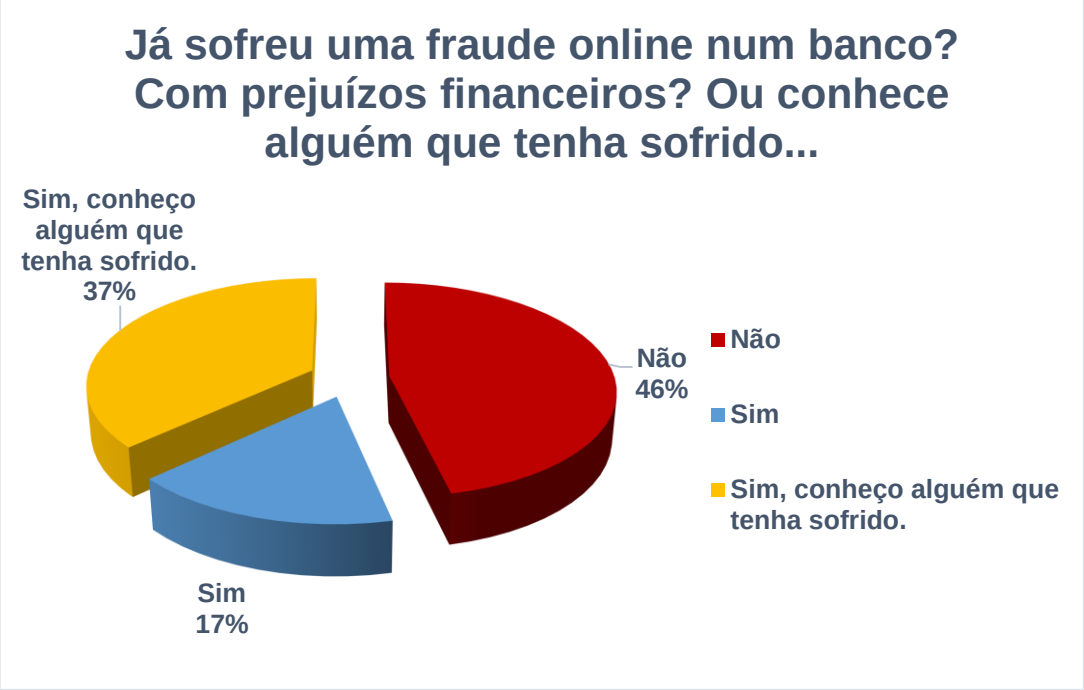

GRÁFICO 19: PESQUISA - FRAUDE EM BANCOS
FONTE: PESQUISA DESTE TRABALHO

4.2.13 TOMBSTONE THEFT

A fraude conhecida como *tombstone theft*, na qual o fraudador se passa pela vítima e realiza clones, fraudes, uso de documentos, também foi motivo de questionamento. A tabela 21 e gráfico 20 revelam o resultado dessa conhecida fraude.

JÁ TEVE PROBLEMAS POR UM FRAUDADOR ESTAR SE PASSANDO POR VOCÊ? (CLONE, FRAUDES, USO DE DOCUMENTOS). OU CONHECE ALGUÉM QUE TENHA PASSADO PELA SITUAÇÃO...	FREQUÊNCIA	PERCENTUAL
Sim	16	14%

Sim, um conhecido já passou por isso	32	28,1%
Não	66	57,9%
Total	114	100%

TABELA 21: PESQUISA - TOMBSTONE THEFT
FONTE: PESQUISA DESTE TRABALHO

14% dos pesquisados respondeu que já sofreu essa fraude, e 28,1% informa que algum conhecido já passou por isso. E 57,9% respondeu negativamente. Além de ser uma fraude muito frustrante para aquele que o sofre, o roubo de identidade é muito danosa à vítima que necessitará procurar as autoridades policiais e a justiça para conseguir reaver sua real identidade.

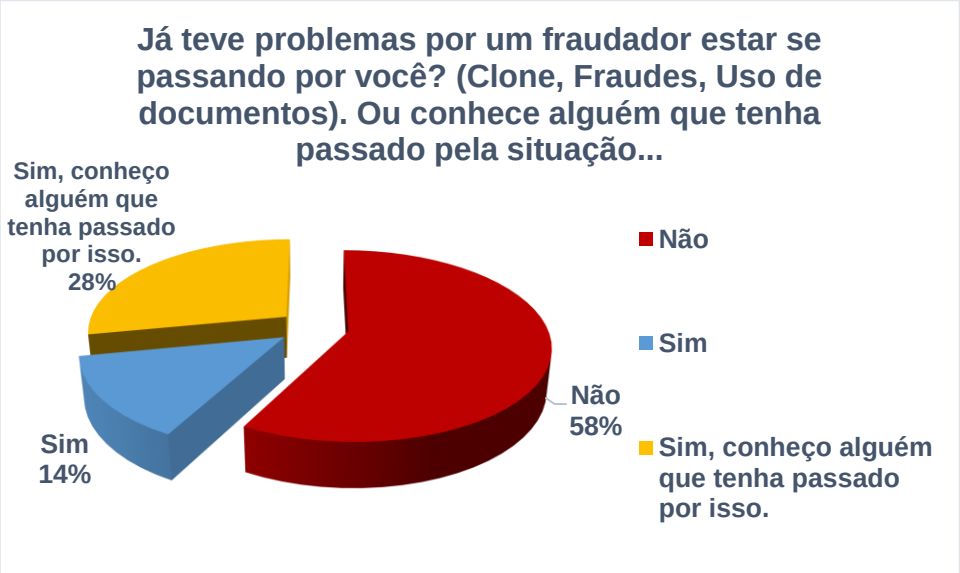

GRÁFICO 20: PESQUISA - TOMBSTONE THEFT
FONTE: PESQUISA DESTE TRABALHO

4.2.14 PERDA DE DADOS OU PREJUÍZO FINANCEIRO

A pesquisa também buscou conhecer se o participante já sofreu algum a perda de informações ou prejuízo financeiro envolvendo as fraudes da engenharia social. A tabela 22 e gráfico 21 revelam o resultado.

HOUVE ALGUMA PERDA DE INFORMAÇÕES (CONFIDENCIALIDADE / INTEGRIDADE / DISPONIBILIDADE) OU PREJUÍZO FINANCEIRO EM ALGUM GOLPE DE ENGENHARIA SOCIAL DESCRITOS NESSA PESQUISA NA QUAL TENHA CONHECIMENTO?	FREQUÊNCIA	PERCENTUAL

Sim	47	41,2%
Não	67	58,8%
Total	114	100%

TABELA 22: PESQUISA - PERDA DE DADOS OU FINANCEIRA
FONTE: PESQUISA DESTE TRABALHO

58,8% informou que não houve nenhuma perda de dados ou prejuízo financeiro relacionado à fraudes da engenharia social. Mas 41,2%, um número expressivo, informa que já houve algum prejuízo relacionado ao tema, de alguma forma.

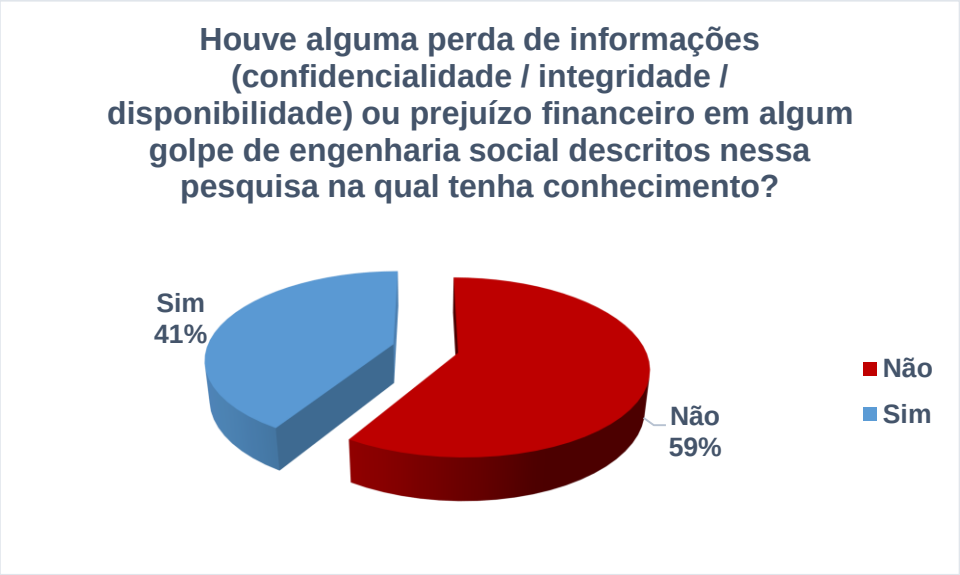

GRÁFICO 21: PESQUISA - PERDA DE DADOS OU FINANCEIRA
FONTE: PESQUISA DESTE TRABALHO

4.3 UMA QUESTÃO DE ATITUDE

Nessa seção perguntas foram realizadas para determinar como os participantes agem a determinadas situações cotidianas.

4.3.1 POST-IT

O ato de deixar post-its espalhados pela máquina, com informações sensíveis, foi motivo de questionamento. A tabela 23 e gráfico 22 mostram o resultado,

VOCÊ COSTUMA DEIXAR POST-ITS COLADOS COM INFORMAÇÕES CONSIDERADAS SENSÍVEIS NA SUA	FREQUÊNCIA	PERCENTUAL

MESA OU NO COMPUTADOR DA EMPRESA?		
Sim	15	13,2%
Não	99	86,8%
Total	114	100%

TABELA 23: PESQUISA - POST-IT
FONTE: PESQUISA DESTE TRABALHO

Costumeiramente os usuários estão deixando para trás a prática de usar post-it, inclusive com informações sensíveis, como provado nos 86,8% que afirmaram não usar esse artifício. E 13,2% indicam que costumam colar informações sensíveis e visíveis. Pode-se inferir que há também uma mudança na atitude por existir atualmente post-it virtuais, aonde os sistemas operacionais oferecem esse recurso nativamente, como o Windows 8.1 da Microsoft.

GRÁFICO 22: PESQUISA - POST-IT
FONTE: PESQUISA DESTE TRABALHO

4.3.2 INFORMAR A SENHA

A situação de informar a senha para um colega ou para a equipe de TI foi alvo de questionamento na pesquisa, revelada na tabela 24 e gráfico 23.

INFORMOU, EM ALGUM MOMENTO, A SUA SENHA DO SISTEMA A UM COLEGA OU A EQUIPE DE TI?	FREQUÊNCIA	PERCENTUAL
Sim	26	22,8%

Não	88	77,2%
Total	114	100%

TABELA 24: PESQUISA - INFORMAR A SENHA
FONTE: PESQUISA DESTE TRABALHO

A maioria dos pesquisados respondeu que não forneceu a senha, com 77,2%. É um número expressivo, mas ainda assim quase um quarto dos participantes informaram que já forneceram a senha, com 22,8%. Isso pode ser causado pela equipe de TI ter em sua cultura fazer tal procedimento, ou quando a pessoa necessita de algum favor de seu colega no sistema, e pede para que o mesmo faça em seu nome.

GRÁFICO 23: PESQUISA - INFORMAR A SENHA
FONTE: PESQUISA DESTE TRABALHO

4.3.3 ESCREVER LOGINS COM SENHA

A atitude de escrever credenciais com senha e posteriormente descartar, foi motivo de questionamento. Demonstrado na tabela 25 e gráfico 24.

JÁ ESCREVEU LOGINS DE ACESSO, COM SENHA, EM UM PAPEL E O DESCARTOU NUMA LIXEIRA, EM ALGUM MOMENTO?	FREQUÊNCIA	PERCENTUAL
Sim	24	29,8%
Não	80	70,2%

Total	114	100%

TABELA 25: PESQUISA - ESCREVER LOGINS COM SENHA
FONTE: PESQUISA DESTE TRABALHO

70,2% nunca realizou esse procedimento, e 29,8% respondeu que já escreveu. Os números positivos são expressivos e podem preocupar uma equipe de TI ou a organização, que deve se preocupar com o descarte do lixo para evitar que tais informações cheguem a fraudadores interessados em um acesso ao sistema sem esforço.

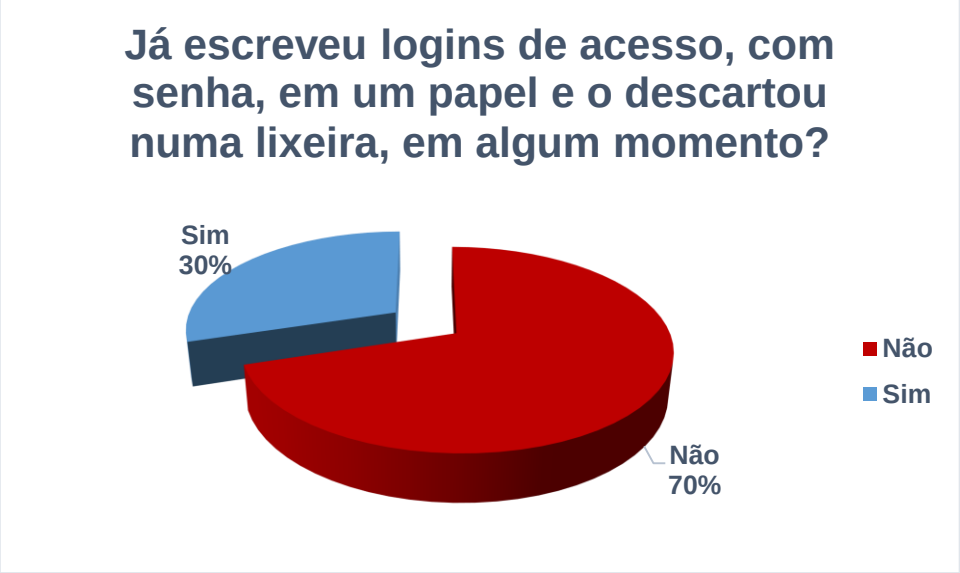

GRÁFICO 24: PESQUISA - ESCREVER LOGINS COM SENHA
FONTE: PESQUISA DESTE TRABALHO

4.3.4 RESTRINGIR ACESSO A GAVETA

A pesquisa buscou questionar também o participante pela segurança física de seus documentos em gavetas de escritório. A tabela 26 e gráfico 25 revelam o resultado.

VOCÊ FECHA A SUA GAVETA DO ESCRITÓRIO COM ALGUM TIPO DE DISPOSITIVO DE SEGURANÇA, POR EXEMPLO COM CADEADO, CHAVE ETC..?	FREQUÊNCIA	PERCENTUAL
Sim	32	28,1%
Não	82	71,9%
Total	114	100%

TABELA 26: PESQUISA - RESTRINGIR ACESSO A GAVETA

FONTE: PESQUISA DESTE TRABALHO

Apenas 28,1% dos participantes informaram que fecham suas gavetas com algum dispositivo de segurança, e 71,9% não tomam essa prevenção. O resultado expressivo para a não tomada dessa prevenção pode estar relacionada em que os usuários costumeiramente não imprimem ou armazenam documentos importantes em suas gavetas, sendo desnecessária tal prevenção. Caso não seja esse o motivo, pode-se inferir o grande perigo, tendo em vista que tais documentos podem ser gravemente prejudiciais às organizações se perdidos.

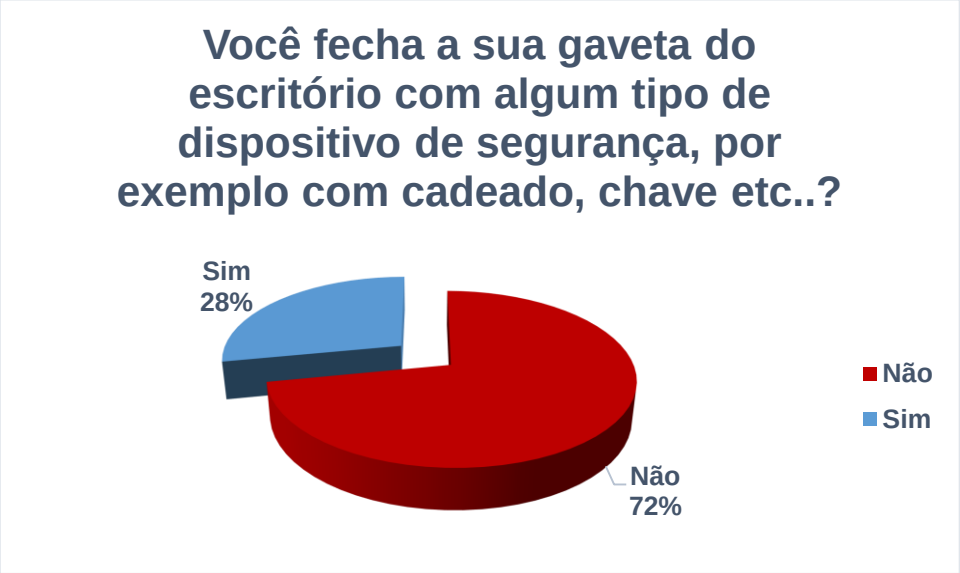

GRÁFICO 25: PESQUISA - RESTRINGIR ACESSO A GAVETA
FONTE: PESQUISA DESTE TRABALHO

4.3.5 ELIMINAR DOCUMENTOS (DUMPSTER DIVING)

A pesquisa buscou saber a opinião dos participantes quanto a eliminação de documentos importantes, de bancos, cartões de crédito etc. A tabela 27 e gráfico 26 revelam o resultado.

APÓS RECEBER UMA CARTA DO SEU BANCO OU DO CARTÃO DE CRÉDITO COM INFORMAÇÕES SIGILOSAS, QUAL É A SUA ATITUDE PARA DESCARTÁ-LA?	FREQUÊNCIA	PERCENTUAL
Rasgo-a no meio e jogo no lixo	44	38,6%
Trituro numa máquina específica ou a deixo totalmente ilegível de outra forma	39	34,2%

Sequer a amasso para descartar	1	0,9%
Guardo para eventuais necessidades futuras	24	21,1%
Outros	6	5,3%
Total	114	100%

TABELA 27: PESQUISA - ELIMINAR DOCUMENTOS
FONTE: PESQUISA DESTE TRABALHO

38,6% dos participantes informaram que apenas rasgam e jogam no lixo. 21,1% guardam para eventuais necessidades futuras, e apenas uma pessoa informou que nem amassa para descartar. 34,2% informou que deixam o documento totalmente ilegível. A fraude de roubo de identidade pode ser realizada na maioria dos casos, e aplicável em 60,6% das situações. Apenas 34,2% estão seguros de terem suas informações asseguradas contra o *dumpster diving* e espionagem, ocasionando *tombstone theft* e na coleta de informações confidenciais. Os participantes que responderam a opção outros, buscam também eliminar totalmente os documentos no fogo e outros modos, conseguindo prevenir tais fraudes.

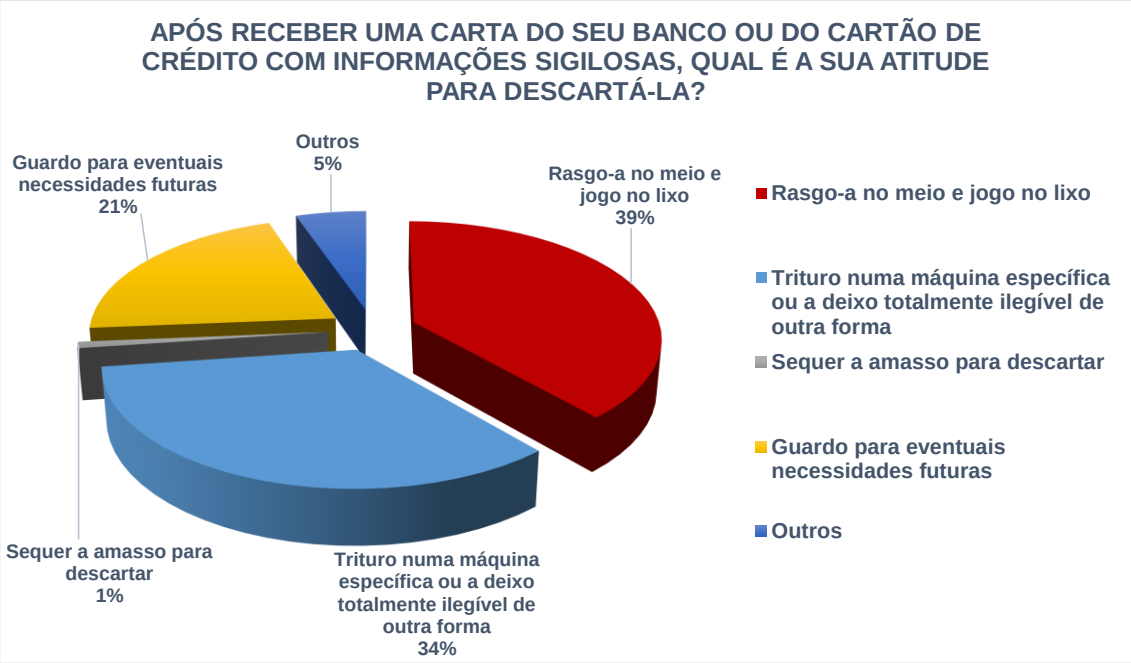

GRÁFICO 26: PESQUISA - ELIMINAR DOCUMENTOS
FONTE: PESQUISA DESTE TRABALHO

4.3.6 SOFTWARE NÃO HOMOLOGADO

A atitude de instalar um software não homologado na organização é uma atitude comum, e foi questionada na pesquisa, como demonstrado na tabela 28 e gráfico 27.

ALGUMA VEZ JÁ INSTALOU UM SOFTWARE NÃO HOMOLOGADO PELA EQUIPE DE TI NO COMPUTADOR DA EMPRESA?	FREQUÊNCIA	PERCENTUAL
Sim	38	33,3%
Não	47	41,2%
Talvez ou não saberia responder por não ter conhecimento dos softwares homologados	29	25,4%
Total	114	100%

TABELA 28: PESQUISA - SOFTWARE NÃO HOMOLOGADO
FONTE: PESQUISA DESTE TRABALHO

41,2% responderam que nunca instalaram um software não homologado nas máquinas da organização. Agora 58,7% responderam que já instalaram um software na organização, sendo que 25,4% informaram que não sabiam se os softwares eram ou não homologados, e 33,3% informou que já efetuou a instalação mesmo sabendo da homologação. A empresa deve manter um catálogo atualizado com os softwares homologados e não vulneráveis e disponíveis a todos os setores da empresa. Não sendo permitida a instalação dos demais softwares, tendo uma política de segurança atualizada e com a concordância e apoio da alta direção da organização.

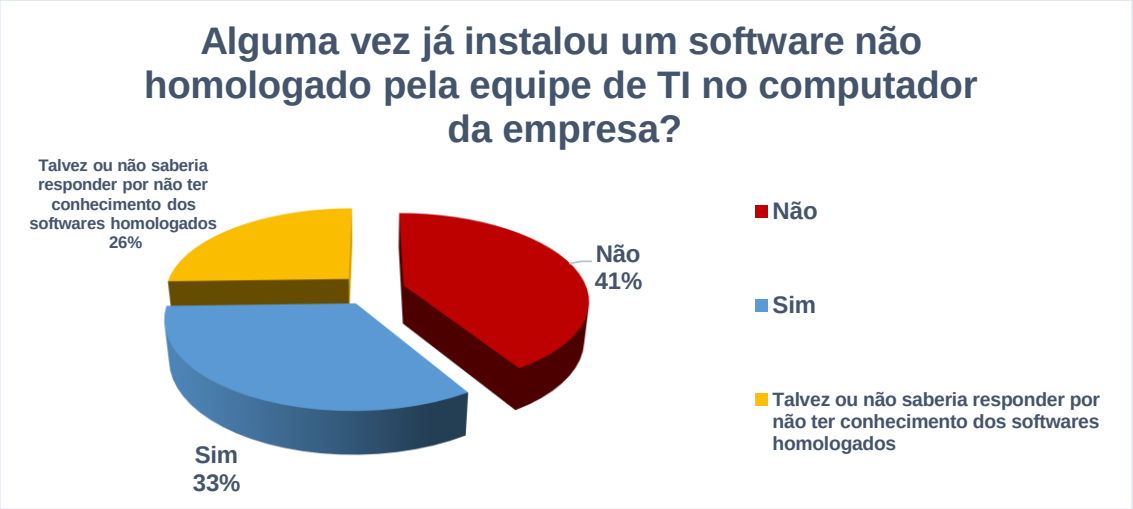

GRÁFICO 27: PESQUISA - SOFTWARE NÃO HOMOLOGADO
FONTE: PESQUISA DESTE TRABALHO

4.3.7 ATITUDE DURANTE UM SHOULDER SURFING

A pesquisa buscou saber a reação dos participantes da pesquisa durante um *shoulder surfing*, enquanto usam seu dispositivo em lugar público e são observados. A tabela 29 e gráfico 28 mostram os resultados.

AO NOTAR QUE ESTÁ SENDO ESPIONADO ENQUANTO USA O NOTEBOOK NUM LOCAL PÚBLICO, QUAL SERIA A SUA PRIMEIRA ATITUDE?	FREQUÊNCIA	PERCENTUAL
Desligo-o imediatamente	25	21,9%
Mudo de lugar e fico incomodado	48	42,1%
Acho normal olharem e continuo na mesma posição	3	2,6%
Sequer noto ou me preocupo com isso	1	0,9%
Nunca passei ou desconfiei que estava nessa situação	37	32,5%
Outros	0	0
Total	114	100%

TABELA 29: PESQUISA - ATITUDE NO SHOULDER SURFING
FONTE: PESQUISA DESTE TRABALHO

Apesar de ser a segunda mais desconhecida dentre todas as fraudes na pesquisa, os participantes informaram que se detectarem de fato um *shoulder surfing*,

em 42,1% eles mudariam de lugar e ficariam incomodados, o que é um bom sinal. E se somados com a prevenção mais primária de desligar o equipamento, em 21,9%, somasse 64% de prevenção ativa sobre essa fraude. Apesar disso 2,6% acham normal a situação, 0,9% nem se preocupa com isso. Outros 32,5% nunca passaram por isso ou imaginavam que estavam numa situação assim.

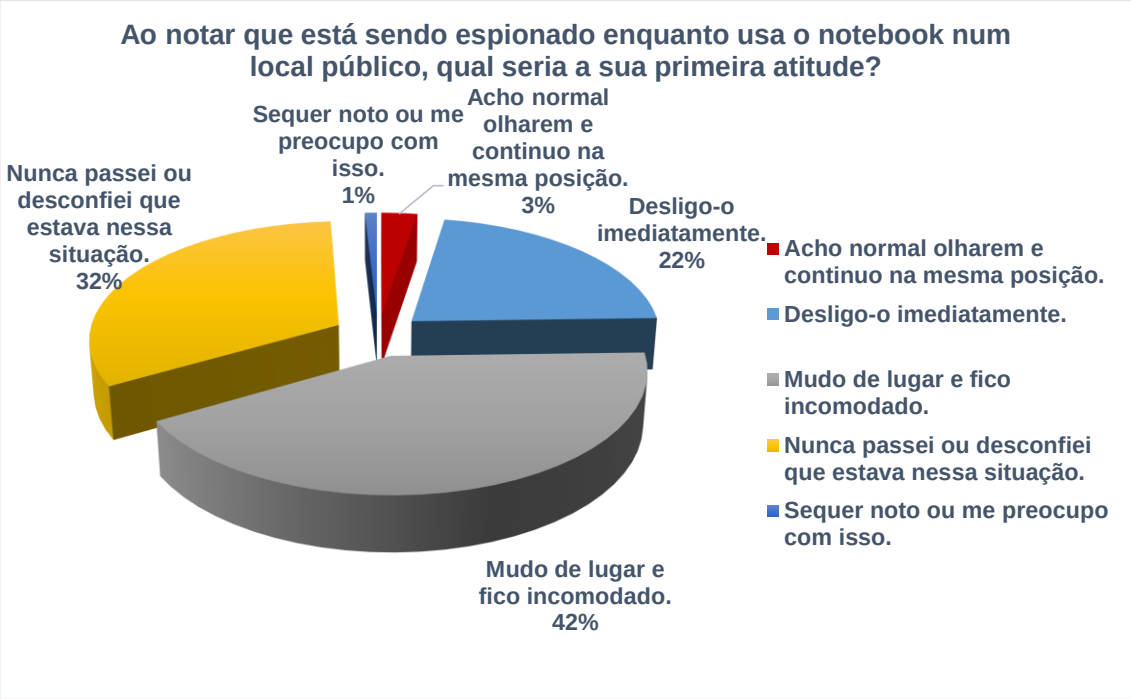

GRÁFICO 28: PESQUISA - ATITUDE NO SHOULDER SURFING
FONTE: PESQUISA DESTE TRABALHO

4.3.8 CRACHÁ EM PÚBLICO

O uso de crachá em público foi motivo de pergunta no questionário e o resultado está representado na tabela 30 e gráfico 29.

VOCÊ COSTUMA USAR O SEU CRACHÁ FUNCIONAL PUBLICAMENTE?	FREQUÊNCIA	PERCENTUAL
Sim	15	13,2%
Não	86	75,4%
Esporadicamente	13	11,4%
Total	114	100%

TABELA 30: PESQUISA - CRACHÁ EM PÚBLICO
FONTE: PESQUISA DESTE TRABALHO

O uso do crachá publicamente pode incorrer em alguns problemas a quem utiliza dessa prática. A primeira seria a identificação da vítima, com seu nome ou cargo. A segunda consequência seria a possibilidade da cópia do crachá, mesmo que visualmente, o fraudador conseguiria fazer uma cópia parecida para buscar se infiltrar na organização. Os pesquisados são prevenidos em deixar o crachá na empresa em 75,4%, e outros 11,4% usam de vez em quando e 13,2% o utilizam publicamente.

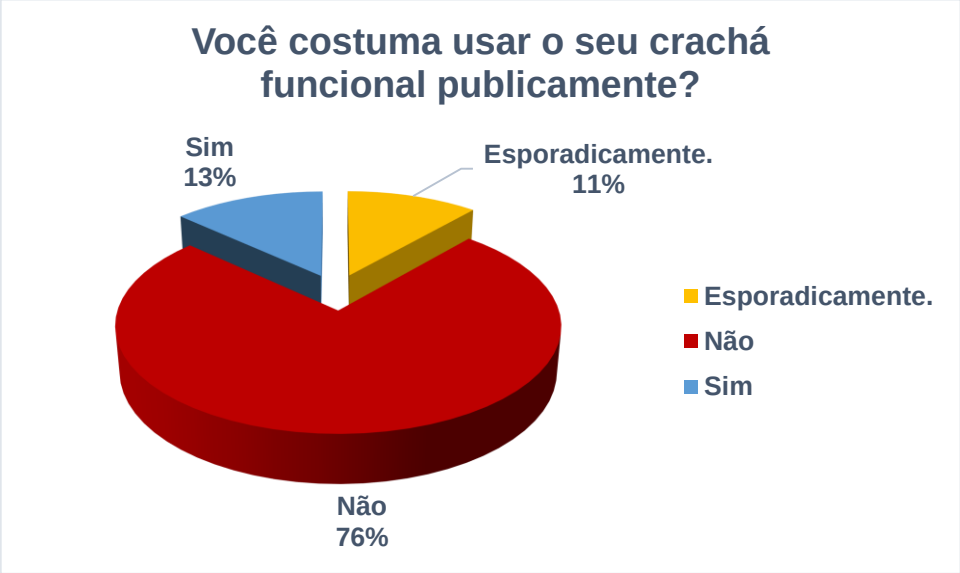

GRÁFICO 29: PESQUISA - CRACHÁ EM PÚBLICO
FONTE: PESQUISA DESTE TRABALHO

4.4 A REAÇÃO EM DETERMINADAS SITUAÇÕES

Nessa seção de perguntas, o objetivo foi criar situações em suposições para conhecer a reação dos participantes segundo o tema proposto.

4.4.1 O ARQUIVO COM SENHAS

A suposição dessa pergunta é para saber o que o participante faria caso tivesse um arquivo em texto, no formato .txt, para armazenar todas as suas senhas importantes dentro de um pendrive. A tabela 31 e gráfico 30 revelam o resultado.

SUPONHAMOS QUE VOCÊ POSSUA UM ARQUIVO EM TEXTO (.TXT) COM TODAS AS SUAS SENHAS, QUAL SERIA A SUA ATITUDE PARA O ARMAZENAMENTO DESTAS VALIOSAS INFORMAÇÕES EM UM PENDRIVE?	FREQUÊNCIA	PERCENTUAL

Salvo normalmente	30	26,3%
Troco a extensão do arquivo e salvo	5	4,4%
Oculto o arquivo no pendrive, em propriedades do arquivo	14	12,3%
Criptografo o pendrive antes de salvar	16	14%
Crio várias pastas e salvo de forma disfarçada ao meio de outros tipos de arquivos	12	10,5%
Uso de técnicas esteganográficas para esconder a informação	4	3,5%
Criptografo o arquivo	22	19,3%
Outros	11	9,6%
Total	114	100%

TABELA 31: PESQUISA - O ARQUIVO COM SENHAS
FONTE: PESQUISA DESTE TRABALHO

A maioria dos participantes informa que salvaria normalmente os arquivos no pendrive, com 26,3%. A criptografia de arquivo e de pendrive foi preferida por 33,3% dos participantes, 19,3% e 14%, respectivamente. Formas para dificultar a visualização das senhas foi preferida por 31% dos pesquisados, sendo 4,4% para trocar a extensão, 12,3% para ocultar o arquivo e 10,5% para esconder no meio de vários arquivos. O uso de técnicas esteganográfica foi preferida por 3,5% dos participantes.

Fica evidente a vontade e o querer dos pesquisados em se preocupar com as informações sigilosas, sendo 73,7% tentam de alguma forma dificultar o acesso. E infere-se que se esses outros usuários tivessem um treinamento ou instruções de como armazenar informações importantes, provavelmente agiriam da melhor forma possível.

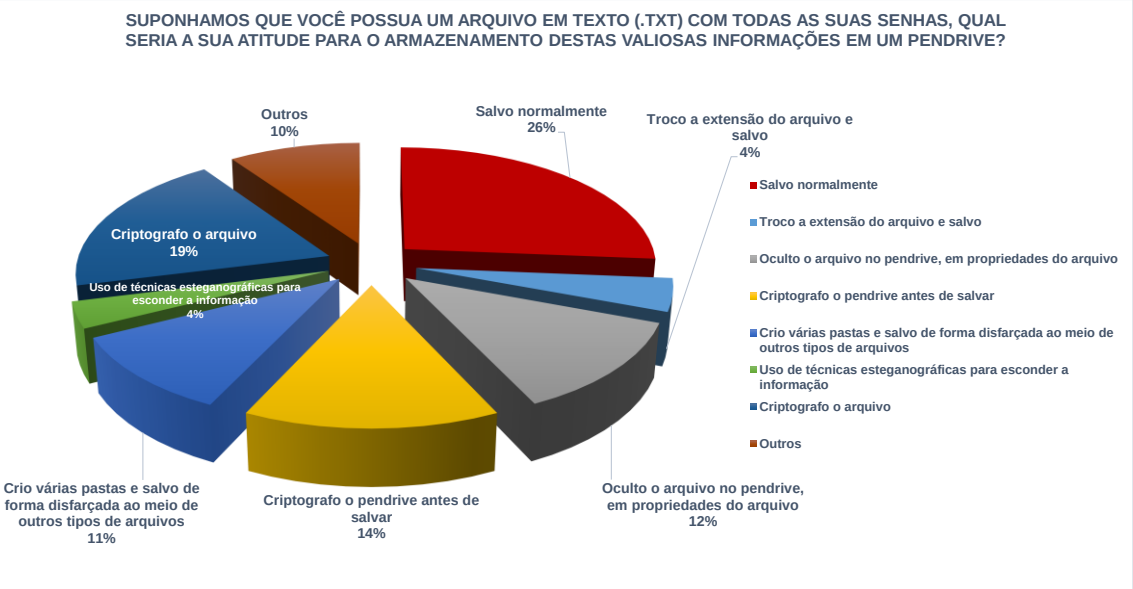

GRÁFICO 30: PESQUISA - O ARQUIVO COM SENHAS
FONTE: PESQUISA DESTE TRABALHO

4.4.2 PERDER IMPORTANTE DISPOSITIVO DE DADOS DA EMPRESA

Essa questão foi feita para saber a reação do participante caso perdesse um dispositivo de armazenamento de dados com importantes informações da empresa, num local público, e qual seria a sua reação. A tabela 32 e gráfico 31 exibem os resultados.

CASO NECESSITE LEVAR UM HD EXTERNO OU NOTEBOOK CORPORATIVO COM VÁRIAS INFORMAÇÕES RELEVANTES DA EMPRESA PARA TRABALHAR EM CASA, E O APARELHO SEJA PERDIDO NUM LOCAL PÚBLICO, QUAL SERIA A SUA ATITUDE?	FREQUÊNCIA	PERCENTUAL
Comunicaria as autoridades policiais, somente	19	16,7%
Entraria em contato com a equipe de TI e os informaria	92	80,7%
Buscaria comprar outro equipamento igual e substituir sem que ninguém notasse a perda	2	1,8%
Outros	1	0,9%
Total	114	100%

TABELA 32: PESQUISA - O EQUIPAMENTO PERDIDO
FONTE: PESQUISA DESTE TRABALHO

80,7% dos participantes responderam que entrariam em contato com a equipe de TI e os informaria, e 16,7% comunicariam às autoridades policiais. 1,8% trocaria o equipamento sem que ninguém percebesse. E apenas 0,9% escolheu “outros”. É notório que os participantes se preocupam com os dados, com 97,4% em comunicar o acontecido de alguma forma. O contato com a equipe de TI seria o ideal para saber quais seriam as consequências daquela perda e possíveis danos aos negócios e a organização, e poder mitigar os prováveis prejuízos.

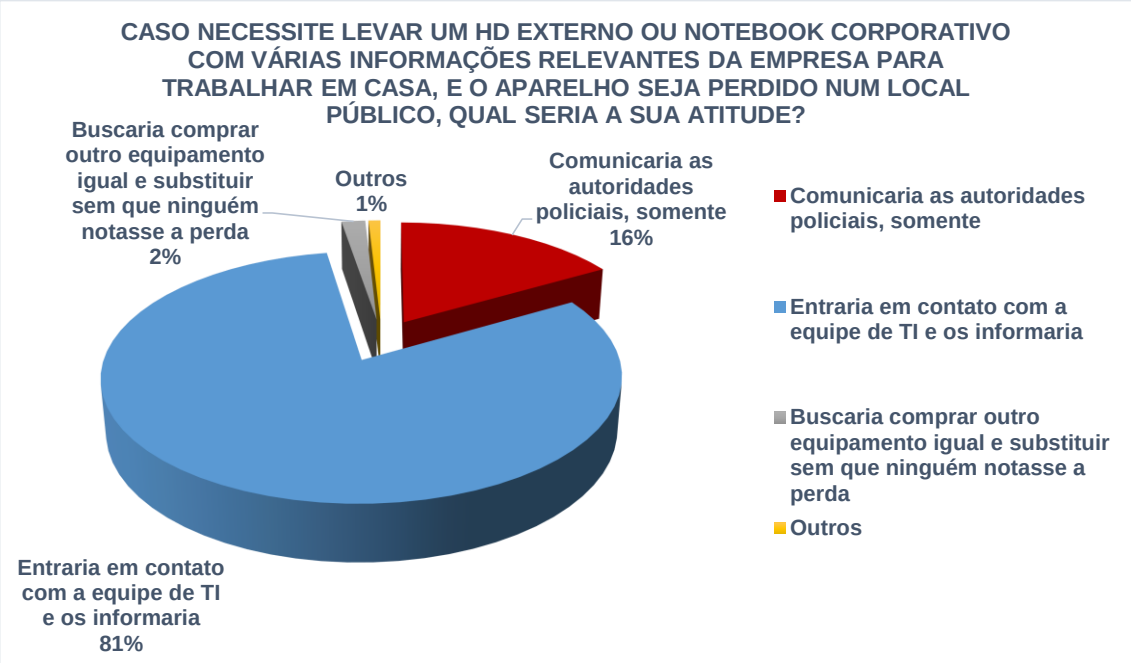

GRÁFICO 31: PESQUISA - O EQUIPAMENTO PERDIDO
FONTE: PESQUISA DESTE TRABALHO

4.4.3 O PENDRIVE ENCONTRADO

A situação hipotética proposta nessa questão foi levar o participante a pensar no que faria se encontrasse um pendrive no chão. O resultado é revelado na tabela 33 e gráfico 32.

AO ENCONTRAR UM PENDRIVE OU DISPOSITIVO DE ARMAZENAMENTO USB NO CHÃO, PRÓXIMO AO SEU TRABALHO, QUAL SERIA A SUA ATITUDE?	FREQUÊNCIA	PERCENTUAL
Conectaria no computador de casa	31	27,2%
Conectaria no computador da empresa	17	14,9%
Conectaria no celular/tablet	1	0,9%

Descartá-lo-ia imediatamente	47	41,2%
Outros	18	15,8%
Total	114	100%

TABELA 33: PESQUISA - O PENDRIVE ENCONTRADO
FONTE: PESQUISA DESTE TRABALHO

Caso encontrasse o pendrive no chão descartaria imediatamente, essa foi a opinião de 41,2% dos participantes. E outros 43% conectariam o pendrive de alguma forma para verificar seu conteúdo ou funcionamento, sendo 27,2% em casa, 14,9% na empresa e 0,9% no celular ou tablet. E 15,8% para outros, incluindo formas mais sofisticadas de abertura do pendrive, como conectar em sistemas operacionais específicos, com distribuições *lives* (sem instalação), ou sem disco rígido, ou até mesmo no computador com o melhor antivírus.

Fraudadores buscam atiçar a curiosidade de suas vítimas com pendrives espalhados nas garagens de empresas, ou estacionamentos. Quando elas conectam, acabam sendo infectadas com *malwares*, e outras formas, até mesmo para queimar o computador com pendrives que causam curtos-circuitos.

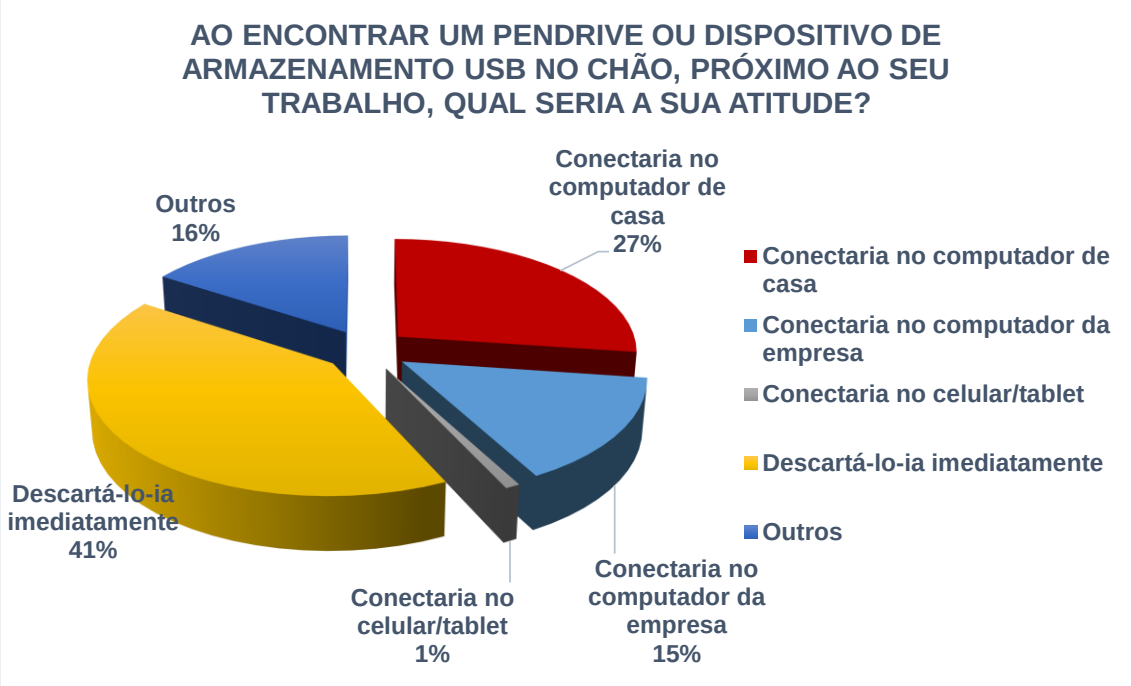

GRÁFICO 32: PESQUISA - O PENDRIVE ENCONTRADO
FONTE: PESQUISA DESTE TRABALHO

4.4.4 O VALIOSO SOFTWARE

A última pergunta do questionário teve como objetivo supor uma inusitada situação na demissão de um funcionário. A suposição é do participante da pesquisa estar no lugar do funcionário demitido e possuir um software inovador que possibilite descobrir a cura de uma rara doença. Então após a venda de sua empresa para uma concorrente no exterior, e com a demissão de todos e cancelamento do projeto, o participante tem uma única chance para salvar o arquivo antes de sair, e o resultado está na tabela 34 e gráfico 33.

SUPONDO QUE EXISTA, EM SUA EMPRESA, UM SOFTWARE INOVADOR QUE POSSIBILITE DESCOBRIR A CURA DE UMA RARA DOENÇA POR MEIO DE UM ALGORITMO INTELIGENTE QUE ANALISA OS GENES DOS PACIENTES E QUE PODE SALVAR A VIDA DE MILHARES DE PESSOAS, PORÉM A EMPRESA É VENDIDA A SUA CONCORRENTE NO EXTERIOR E O PROJETO É CANCELADO, INCLUINDO A DEMISSÃO DE TODOS. ENQUANTO OS SEGURANÇAS ESVAZIAM AS SALAS, VOCÊ TEM UM MOMENTO ÚNICO PARA SALVAR O PROGRAMA. VOCÊ FARIA ESSA CÓPIA?	FREQUÊNCIA	PERCENTUAL
Sim	60	52,6%
Não	54	47,4%
Total	114	100%

TABELA 34: PESQUISA - O VALIOSO SOFTWARE
FONTE: PESQUISA DESTE TRABALHO

Com uma acirrada disputada do começo ao fim da pesquisa, 52,6% escolheram copiar o arquivo e 47,4% não. Esse experimento teve como objetivo analisar o comportamento dos participantes em uma situação extrema e de grande responsabilidade, inclusive de questão social. Com uma diferença muito apertada, de apenas seis pessoas, a maioria absoluta copiaria o programa. O resultado pode servir de argumento para as empresas incrementarem suas políticas de segurança da informação, inclusive em situações como essa.

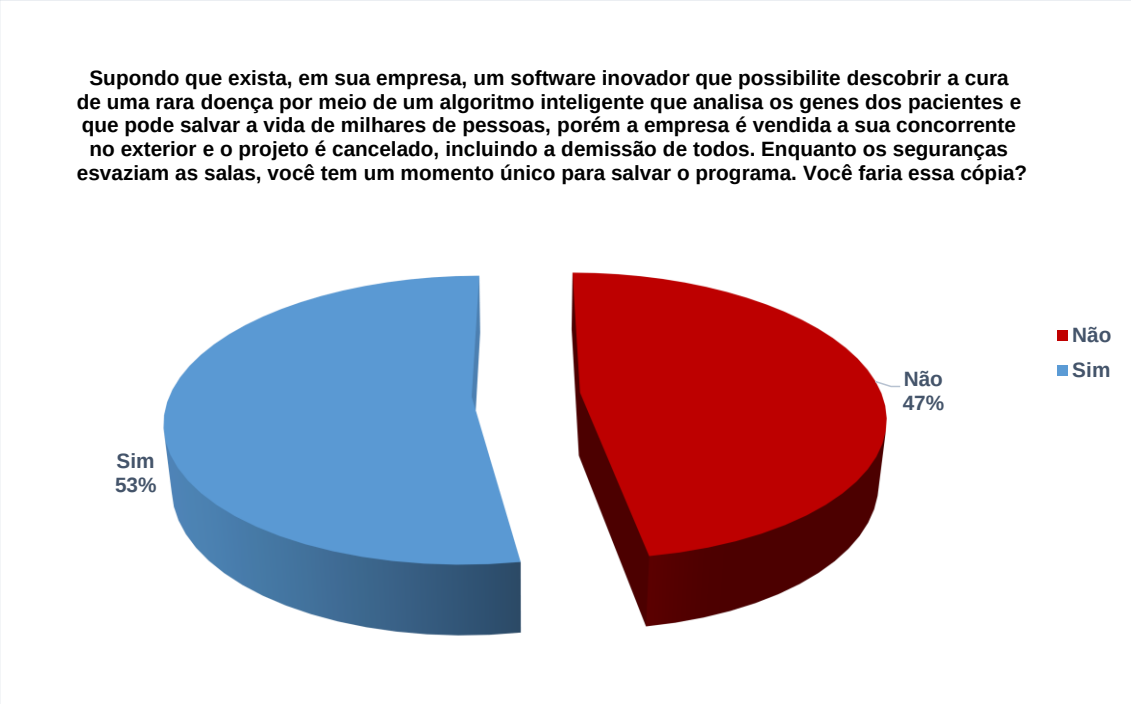

GRÁFICO 33: PESQUISA - O VALIOSO SOFTWARE
FONTE: PESQUISA DESTE TRABALHO

5. CONSIDERAÇÕES FINAIS

5.1 ESTUDOS SOBRE OS RESULTADOS DA PESQUISA

A pesquisa revelou algumas surpresas no seu resultado em determinados itens, mas também reafirmou questões críticas nas quais os gestores e principalmente os usuários devem se prevenir.

5.1.1 NÍVEL DE CONHECIMENTO DO ASSUNTO

A pesquisa demonstrou que muitos participantes sustentam o seu nível de informação em apenas conhecer alguma coisa sobre esse importante tema, e até mesmo alguns dizem sequer se importar. Apesar do resultado de conhecimento, os pesquisados têm em mente a importância no sigilo de informações de suas organizações, afirmando que é um assunto sério a ser tratado. Quanto aos tipos de fraudes conhecidas, os participantes, incentivados por uma breve descrição, revelam conhecer a maioria dos assuntos perguntados. E o dado mais alarmante foi revelando aonde os pesquisados foram questionados se já tiveram uma preparação para esse assunto dentro de suas organizações, a resposta negativa de quase 70% foi surpreendente.

Conclui-se que os participantes possuem um grau adequado de conhecimento em todas as fraudes questionadas, e consciência de sua importância para os negócios da empresa. Com isso, as organizações necessitam incentivar, por meio de treinamentos, uma cultura de segurança além de somente as políticas, mas também no modo em como os colaboradores tratam as informações e pelo intermédio de suas atitudes preventivas contra os ataques da engenharia social para mitigar seus riscos e prejuízos. Sugere-se a adequação de treinamentos para colaboradores iniciantes e antigos, por palestras, vídeos educacionais, situações simuladas, dentre outras atitudes diretas de educação sobre esse importante tema.

5.1.2 OS DANOS DA ENGENHARIA SOCIAL

Os danos causados pela engenharia social tiveram a apresentação de vários assuntos e buscaram conhecer e quantificar seus níveis de impacto. O resultado da

pesquisa trouxe à tona alguns problemas antigos, como o alto grau de e-mails falsos recebidos, apesar de que poucos tenham sido atingidos; na forma em como o desenvolvimento de técnicas de desenvolvimento web impactou na forma de navegação dos usuários, quando clicam de forma enganosa em algum link; na prática do *phishing* ou *pharming* que apesar de poucas pessoas terem sido atingidas, o prejuízo pode ter sido muito grande; a antiga prática dos trotes telefônicos com assuntos de prêmios, sequestros, aonde a grande maioria afirma ter recebido uma ligação falsa apesar de nunca, em sua maioria, terem cumprido o seu ordenado; à vasta prática de *smishing*, no envio de SMS com links de sorteios falsos, prêmios, vislumbrando o engano e curiosidade do usuário, e apesar disso também poucos foram efetivamente atingidos; à prática ostensiva do *hoax* em suas vastas vertentes que alcançaram os seus objetivos em sua grande maioria de tentativas; os perigos do *ransonware*, esse perigoso e novo método de sequestro de dados, donde muitos já foram vítimas; o *shoulder surfing*, prática pouco conhecida, mas utilizada de forma eficaz pelos engenheiros sociais em suas investidas maliciosas; ao *piggybacking* que é a prática de uma autoridade se passar por quem não é para conseguir informações privilegiadas, donde cerca de um terço respondeu positivamente; na atitudes dos demitidos em causar algum dano as suas ex-organizações quando demitidos, e apesar do baixo número de respostas positivas, seria uma fraude muito danosa à empresa; ao clone de cartões, aonde surpreendentemente apenas 15% não sofreu de alguma forma ou que conhece alguém que tenha sofrido esse perigoso golpe; pelas fraudes online em bancos, donde mais da metade afirmou conhecer alguém ou já ter sofrido por isso; ao roubo de informações, clone de documentos, prática do *tombstone theft*, aonde pouco menos da metade diz ter sofrido a fraude ou conhecido alguém que tenha a sofrido; e enfim a perda de dados ou prejuízo financeiro sofrido pela engenharia social em alguma vertente, donde quase metade dos participantes afirmaram terem sido atingidos.

Deduz-se pela pesquisa que os danos causados pela engenharia social são reais e preocupantes. Nota-se também que os ataques novos, como o *hoax*, que atiçam a curiosidade dos usuários para que cliquem em notícias e imagens, tem uma eficácia surpreendente, além de links ocultos aonde os usuários devem clicar em um link para prosseguir na página ou para visualizar tal conteúdo, abrindo outra página ou segmento. O usuário deve sempre atentar e suspeitar de quaisquer e-mails ou notícias em redes sociais que aparentam suspeita, e sempre manter seu sistema de

antivírus atualizado. O preocupante avanço do sequestro de dados via *ransomware* pode ser mitigado ao não clicar em links de e-mails ou imagens, que atiçam por várias maneiras o emocional e buscam tratar a curiosidade do usuário. Além disso, há uma conscientização dos usuários para ataques antigos como o de trotes telefônicos e mensagens sms, donde esse assunto é tratado em notícias e documentários na rede aberta de televisão, com ampla divulgação. E os ataques mais físicos, como de *shoulder surfing* e *piggybacking* são menos eficazes ou mais despercebidos pelos participantes, mas que se obtiverem os seus objetivos iniciais, trarão grandes riscos às organizações e às vítimas. O clone de cartões é de fato uma fraude antiga, mas que não depende apenas da prevenção do usuário, que por vezes é vítima dessa fraude indo em uma agência bancária conhecida, mas burlada, infere-se a importância de um seguro adicional contra essas fraudes devido a sua notória eficácia. E fraudes online dependem muito do usuário que deve atentar ao clicar em links de e-mails ou outras formas, com uma prevenção ativa e sempre em suspeição de avisos em e-mails, podendo mitigar totalmente esse apenas ligando para a sua agência e perguntando sobre tal situação. O roubo de identidade é eficaz e preocupa devido aos seus danos, o usuário deve sempre atentar quando descartar documentos importantes, não informar números de documentos em ligações telefônicas ou pesquisas de rua, e evitar ao máximo publicar tais em locais públicos.

5.1.3 UMA QUESTÃO DE ATITUDE

A atitude do participante é a forma mais simples de se prevenir, de forma primária, um ataque de engenharia social ou efetivamente ajudar a se tornar vítima de uma fraude.

Atitudes de colar adesivos post-it em monitores é mínima, e de fato os participantes informaram que não usam, em sua maioria, esse método de anotação. Método que pode ser danoso ao informar à pessoa má intencionada informações importantíssimas sem muito esforço. O ato de escrever senhas também é pouco utilizado, e apesar do seu alto grau de risco e danosidade essa atitude está sendo extinta. O ideal para não esquecer senhas ou outras informações é utilizar softwares próprios para esse propósito, e eles existem tanto no celular como em sistemas operacionais. O preocupante nesse quesito de senha é que quase um quarto dos participantes afirmou que já contou a senha para algum colega ou equipe de TI,

tornando o acesso às suas credenciais público, e podendo o participante responder por atos tomados por outros em seu nome. O ideal nesse caso é nunca informar a sua senha, que é pessoal e instransferível a qualquer pessoa. A restrição de acesso a gaveta, que pode conter documentos sigilosos e estratégicos da organização também é uma prática pouco utilizada, mas ainda assim pode-se inferir que talvez não haja a necessidade de fechamento por não conter tais documentos ou por ser uma gaveta de uso apenas particular. De qualquer modo sempre é positivo manter a gaveta trancada para evitar a ação de pessoas preparadas a roubar informações. A eliminação de documentos, prática necessária para evitar o tombstone theft, é tratada com certo descuido pelos participantes, e isso pode ser muito danoso, tanto para as organizações que não praticam esse ato, quanto para os usuários que podem ter suas informações coletadas e usadas por outrem. O ideal é deixar o documento totalmente ilegível, de forma a prevenir tais atos danosos pelos fraudadores. Outra informação relevante e preocupante foi o uso de software não homologado na empresa, o que pode trazer sérios riscos à segurança da informação e danos quanto à integridade do sistema. O ideal é a empresa manter um catálogo de homologação e informar aos seus colaboradores que nenhum software além daqueles são permitidos, incluindo tais informações na política de uso e na política de segurança, com a concordância de todos os funcionários. O uso do crachá em público, que pode trazer riscos aos participantes, é uma prática, de certo modo, pouco utilizada, e àqueles que a utilizam devem ter ciência do seu dano caso um engenheiro social consiga utilizar tais informações que constam em seus crachás, como roubo de identidade e clone do design para conseguir acesso à empresa.

5.1.4 A REAÇÃO EM DETERMINADAS SITUAÇÕES

Foram quatro situações criadas aonde os participantes precisaram escolher a resposta do que fariam. A guarda de um arquivo com senhas, se perdessem um dispositivo de armazenamento de dados da empresa, ao encontrar um pendrive, e sobre salvar um valioso software que seria descartado.

Guardar um arquivo com sigilo atualmente é algo trabalhoso, evitar que ele torne-se público ainda mais, agora guardar um arquivo com suas senhas e toda a sua privacidade. A maioria das pessoas buscou um método de salvar esse arquivo da maneira mais segura possível em seu conhecimento, e cerca de um terço não teve a

preocupação nisso. Pode-se inferir que o participante busca sigilo e a guarda da melhor forma possível, cabe a organização demonstrar os riscos inerentes de uma perda desse dispositivo e também instruir de como essa guarda deve ser realizada. Outra pesquisa interessante foi a perda do dispositivo de armazenamento de dados com dados importantes da empresa, em um local público, interessante notar que a maioria dos participantes tomaria a atitude de contar à equipe de TI o ocorrido, e de fato essa seria a melhor alternativa para mitigar os danos o máximo possível. Ao encontrar um pendrive no chão, os usuários em sua maioria não teriam uma preocupação em onde ligá-lo, por curiosidade, para saber o que se tem dentro. De fato, poderia haver um malware ou algo destrutitivo, e usuários sem o conhecimento necessário poderiam ser afetados diretamente apenas por conectarem em seus dispositivos. O ideal seria descartar ou entregar a alguém com conhecimentos de informática, e esse item é tão imprevisto que dificilmente seria incluído no conteúdo dado em palestras de segurança da informação. O software valioso que seria perdido e poderia ser salvo pelo participante traz à tona muitas questões relevantes, e de fato, a responsabilidade sob os dados é da empresa, mas se houver uma política de segurança da informação consistente e que informe do sigilo de tais informações, muitos dos usuários poderiam ter deixado de salvar essas informações mesmo com a extinção da empresa, de modo que este não poderia ser responsabilizado pela falta de diretrizes e políticas daquela.

5.1.5 A PREVENÇÃO CONTRA A ENGENHARIA SOCIAL

Após a explanificação do tema engenharia social, passando por assuntos como os princípios psicológicos, modelos de comunicação, e táticas de influência, com todas as técnicas e armas usadas pelos fraudadores, vê-se a grande necessidade de uma tomada de atitudes contra a eficácia da engenharia social aos cidadãos e organizações.

A tabela 1 exemplificou situações de prevenção que podem ser tomadas em cada tipo de fraude, e além disso a pesquisa explanatória torna a dimensão de cada fraude em aspectos concretos e atuais, demonstrando a sua efetividade.

A responsabilidade pela prevenção de ataques de engenharia social deve partir de cada colaborador da organização e a empresa deve preparar-se para todo o tipo

de situação, criando uma política e cultura apta para mitigar todas as possíveis consequências e riscos dessas graves ameaças aos negócios.

5.2 CONCLUSÂO FINAL

Por fim, o projeto concluiu seu objetivo em demonstrar através de uma consistente base teórica sobre o assunto em questão e uma abrangente e extensiva pesquisa a relação entre os problemas ocasionados pelas fraudes da engenharia social e das atitudes dos usuários frente a casos prioritários do uso da informação.

Defere-se a urgente necessidade das organizações em criar ou atualizar as suas políticas de segurança da informação, pois em muitos dos casos analisados é demonstrada uma despreocupação dos usuários e a falta de conhecimento do assunto, com a carência de instruções e treinamentos. Além de tratar a informação como algo valioso, as organizações devem atentar sobre a questão de que o ser humano é, e sempre será, o elo mais fraco do sistema, podendo tomar como referência a pesquisa deste projeto como forma para parametrizar os itens necessários em suas políticas, e no desdobramento de sua cultura em detrimento das necessidades emergentes desse importantíssimo tema. E é de responsabilidade das organizações a aplicação de treinamentos, palestras, e-mails informativos, e de caráter didáticos com exemplos, das fraudes e dos danos causados. Além de demonstrar o valor das informações para a organização e da grande responsabilidade de cada colaborador em cada área, para a formação de uma cultura organizacional consistente preocupada e atenta às necessidades atuais e que abranja todas as áreas da empresa, cobrindo-a de ponta a ponta. E nesse critério a mais alta direção e gestão devem caminhar juntas no objetivo de proteger e tomar as devidas providências para que as mudanças ocorram gradualmente e que os riscos sejam mitigados a cada decisão de negócio.

Por fim, cabe aos usuários tratarem as informações com prudência e buscar instruções atualizadas sobre formas de resguardar seus conteúdos para manter a confidencialidade, integridade e disponibilidade de seus dados e dos dados organizacionais, utilizando de eficientes sistemas de segurança e cópias das informações mais importantes. Ressalta-se, inclusive, a necessidade de aferir o valor de cada informação, atentando também pelas atitudes em situações cotidianas com o objetivo de mitigar os riscos e danos de prováveis ataques da engenharia social.

6. REFERÊNCIAS BIBLIOGRÁFICAS

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

FONSECA, J. J. S. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002. Apostila.

YEBOAH-BOATENG, E. O. ; AMANOR, P. M. **Phishing, SMiShing e Vishing: An Assessment of Threats against mobile devices.** Vol. 5. Copenhagen: CIS Journal, 2014.

SANTOS, Yuri Rafael de Lima. **A engenharia social nas redes sociais online**. Mato Grosso: Universidade do Estado de Mato Grosso, 2014.

HADNAGY, Christopher. **Unmasking the Social Engineer.** Indianapolis, IN: Wiley, 2014.

An analysis of identity theft: Motives, related frauds, techniques and prevention. Vol 4. Nanaimo: Journal of Law and Conflict Resolution, 2012.

KHIDZIR, N. Z. ; ISMAIL, A. R. ; DAUD, A. M. D ; GHANI, M. S. A. A. ; IBRAHIM, M. A. H. **Critical Cybersecurity Risk Factors in Digital Social Media:** Analysis of Information Security Requirements. Malaysia: Universiti Malaysia Kelatan, 2015.

CONTEH, Nabie Y. ; SCHMICK, Paul J. **Cybersecurity**: risks, vulnerabilities and countermeasures to prevent social engineering attacks. EUA: ACCENTS, 2016.

PATEL, Rahul Singh. **Kali Linux Social Engineering**. EUA: Packt Publishing Ltd, 2013.

BATISTA, F. L. **Métodos e práticas utilizadas em engenharia social com o intuito de obstar o roubo de informações sensíveis**. Brasília: Centro Universitário de Brasília, 2015.

LONG, Johnny. **No Tech Hacking:** A Guide To Social Engineering, Dumpster Diving, And Shoulder Surfing. Burlington: Elsevier Inc, 2008.

JAMES, Lance. **Phishing Exposed:** Uncover Secrets from the Dark Side. EUA: Syngress Publishing Inc, 2005.

SLONKA, K. J. ; SHRIFT, B. F. **Phishing our clients:** a step toward improving training via social engineering. EUA: Precision Business Solutions, 2016.

VAKNIN, S. **The big book of NLP Tecnhiques.** EUA: Book Surge, 2008.

ANDREAS, S. **PNL Programação Neurolinguística:** A nova tecnologia do sucesso. 10 ed. Editora Campus, 1995.

HANCKE, G. P. **Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens**. Londres: University of London, 2011.

PEIXOTO, Mário C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa.** Rio de Janeiro: Brasport, 2006.

IRANI, D. ; BALDUZZI, M. ; BALZAROTTI, D. ; KIRDA, E. ; PU, C. **Reverse Social Engineering Attacks in Online Social Networks.** Boston: Northeastern University, 2011.

KONTIO, M. **Social Engineering 101**. Turku: Turku University of Applied Sciences, 2016.

MOUTON, F. ; LEENEN L. ; VENTER, H. S. **Social Engineering Attack Examples, Templates and Scenarios.** África do Sul: University of Pretoria, 2016.

ENGEBRETSON, P. **The basics of hacking and penetration testing:** Ethical Hacking and Penetration Testing Made Easy. EUA: Elsevier, 2011.

HADNAGY, C. **Social Engineering:** The art of human hacking. EUA: Wiley Publishing Inc, 2011.

ALECRIM, E. **O que é phishing scam e como evitá-lo?**. INFO WESTER, 15 mar. 2013. Disponível em: <http://www.infowester.com/phishing_scam.php>. Acesso em: 19 set. 2016.

FERNANDES, J. H. C. ; SOUZA, R. C. de. **Um estudo sobre a confiança em segurança da informação focado na prevenção a ataques de engenharia social nas comunicações digitais.** Brazilian Journal of Information Studies, 2016.

HEDAYATI, A. **An analysis of identity theft:** Motives, related frauds, techniques and prevention. Vol. 4. Vancouver: Journal of Law and Conflict Resolution, 2012.

RORH, A. **Hacker brasileiro sabe compensar técnica de iniciante, diz especialista.** G1.GLOBO.COM, Rio de Janeiro, 21 set. 2009. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1303233-6174,00-HACKER+BRASILEIRO+SABE+COMPENSAR+TECNICA+DE+INICIANTE+DIZ+ESPECIALISTA.html> Acesso em: 10 out. 2016.

BERSHCEID, E. ; DION, K. ; HATFIELD, E. **What is beautiful is good**. Vol. 25. EUA: Journal of Personality and Social Psychology, 1971.

FRENZEN, J. K. ; DAVIS, H. L. **Purchasing Behavior in Embedded Markets.** Vol. 17. EUA: Oxford University Press, 1990.

GOULDNER, A. W. **The norm of reciprocity:** A preliminary statement. St. Louis: Washington University, 1960.

LICHTFUSS, M. **Cost of Cyber Crime Study: Malicious Insiders, Phishing and Social Engineering.** LINKEDIN, 09 out. 2015. Disponível em: <https://www.linkedin.com/pulse/2015-cost-cyber-crime-study-malicious-insiders-social-matt-lichtfuss>. Acesso em: 14 out. 2016.

TECHNET. **Como proteger as pessoas de dentro da empresa contra ameaças de engenharia social.** MICROSOFT, 18 ago. 2006. Disponível em: <https://technet.microsoft.com/pt-br/library/cc875841.aspx>. Acesso em 02 out. 2016.

MARTINS, R. **Engenharia Social.** Atitude Reflexiva, 26 de ago. 2014. Disponível em: <https://atitudereflexiva.wordpress.com/2014/08/26/engenharia-social/>. Acesso em: 20 out. 2016.

DA REDAÇÃO. **Call center falso na índia rouba milhões de dólares de americanos.** REVISTA VEJA, 06 out. 2016. Disponível em: <http://veja.abril.com.br/mundo/call-center-falso-na-india-rouba-milhoes-de-dolares-de-americanos/>. Acesso em: 15 out. 2016.

ALECRIM, E. **HOAX:** os perigos dos boatos na internet. INFO WESTER, 14 set. 2012. Disponível em: <http://www.infowester.com/hoax.php>. Acesso em: 01 out. 2016.

SAMPAIO, D. **O relacionamento entre estratégia e cultura organizacional em cooperativas e associações da cidade de viçosa em Minas Gerais**. Sociedade Brasileira de Economia, Administração e Sociologia Rural. 2007. Disponível em: <http://www.sober.org.br/palestra/6/427.pdf>. Acesso em 28 Nov. 2016.

APÊNDICE 1 – QUESTIONÁRIO

Engenharia Social

Essa pesquisa acadêmica tem como objetivo analisar e quantificar dados sobre o assunto "Engenharia Social no Brasil e seus riscos", para o desenvolvimento da monografia do curso de MBA em Gestão de Tecnologia da Informação e Comunicação da UTFPR, sob a orientação do Dr. Prof. Christian Mendes.

A pesquisa é totalmente anônima e sigilosa, e os dados coletados aqui são apenas e exclusivamente dos resultados dos formulários de pesquisa, sem quaisquer identificações de nome, IP, email, login, sessões, ou de outra forma.

A coleta de dados será encerrada no dia 01/11/2016.

*Obrigatório

Qual é o seu nível de conhecimento sobre o tema "Engenharia Social"? *

- ◯ Total conhecimento e domínio do assunto
- ◯ Possuo algum conhecimento
- ◯ Indiferente
- ◯ Já ouvi falar pela mídia
- ◯ Nenhum

Quais dos seguintes golpes de engenharia social você tem algum conhecimento de sua aplicação: *

	SIM	NÃO
Shoulder Surfing - Espionar sobre os ombros	◯	◯
Phishing - Site clonado, falsificado	◯	◯
Tailgating - Seguir alguém de perto para entrar em lugares restritos.	◯	◯
Espionagem	◯	◯
Dumpster Diving - Quando mexem no lixo em busca de informações	◯	◯
SMiShing - Fraude por SMS	◯	◯
Piggybacking - O golpista se disfarça para conseguir informações ou acessos.	◯	◯
Skimming - Clone de cartões (crédito e RFID)	◯	◯
Engenharia social reversa - Passar-se por um personagem de grande autoridade para conseguir informações ou acessos.	◯	◯
Vishing - Fraude por telefone	◯	◯
Tombstone Theft - Assumir a identidade de outra pessoa.	◯	◯
Pharming - Alteração do DNS ou do arquivo hosts.	◯	◯

Se houvesse a perda de sigilo de informações cruciais e estratégias de sua organização, isso poderia ser grave aos negócios? *

- ◯ Sim
- ◯ Não
- ◯ Talvez

Você costuma deixar post-its colados com informações consideradas sensíveis na sua mesa ou no computador da empresa? *

- ◯ Sim
- ◯ Não

Informou, em algum momento, a sua senha do sistema a um colega ou a equipe de TI? *

- ◯ Sim
- ◯ Não

Já escreveu logins de acesso, com senha, em um papel e o descartou numa lixeira, em algum momento? *

- ◯ Sim
- ◯ Não

Você fecha a sua gaveta do escritório com algum tipo de dispositivo de segurança, por exemplo com cadeado, chave etc..? *

- ◯ Sim
- ◯ Não

Após receber uma carta do seu banco ou do cartão de crédito com informações sigilosas, qual é a sua atitude para descartá-la? *

- ◯ Rasgo-a no meio e jogo no lixo.
- ◯ Trituro numa máquina específica ou a deixo totalmente ilegível de outra forma.
- ◯ Sequer a amasso para descartar.
- ◯ Guardo para eventuais necessidades futuras.
- ◯ Outro: _____

Já recebeu um e-mail falso? Por exemplo: *

- ◯ Sim
- ◯ Não

Se já recebeu um e-mail falso: chegou a clicar no link ou no anexo nele contido, em seu dispositivo, por curiosidade? *

- ◯ Sim
- ◯ Não
- ◯ Nunca recebi

Já clicou em um link de forma enganosa enquanto navegava em algum site? *

- ◯ Sim
- ◯ Não

Já digitou informações confidenciais em sites não seguros que causaram danos de alguma forma? *

- ◯ Sim
- ◯ Não

Alguma vez você já recebeu um telefonema com uma tentativa de fraude? Sobre sequestro, um prêmio, banco... *

- ◯ Sim
- ◯ Não
- ◯ Talvez

Se já recebeu a ligação de um fraudador, chegou a realizar o que foi pedido? *

- ◯ Sim
- ◯ Não
- ◯ Nunca me ligaram

Já recebeu um SMS falso de um sorteio que tenha ganho um prêmio, ou créditos adicionais, no qual tenha que clicar num link ou ligar para algum número? Por exemplo: *

- ◯ Sim
- ◯ Não

Se recebeu o SMS falso, chegou a clicar no link ou ligar para o número? *

- ◯ Sim
- ◯ Não
- ◯ Nunca recebi

Já clicou na imagem ou link de um boato num site, ou rede social, por curiosidade ou desconhecimento? *

- ◯ Sim
- ◯ Não

Já sofreu um ataque de RansomWare (sequestro de dados virtuais) ou conhece alguém que tenha sofrido? *

- ◯ Sim
- ◯ Não

Alguma vez já instalou um software não homologado pela equipe de TI no computador da empresa? *

- ◯ Sim
- ◯ Não
- ◯ Talvez ou não saberia responder por não ter conhecimento dos softwares homologados

Alguma vez já notou estar sendo espionado (Shoulder Surfer) enquanto utilizava o notebook ou celular ao acessar informações sigilosas em locais públicos? *

- ◯ Sim
- ◯ Não
- ◯ Talvez

Ao notar que está sendo espionado enquanto usa o notebook num local público, qual seria a sua primeira atitude? *

- ◯ Desligo-o imediatamente.
- ◯ Mudo de lugar e fico incomodado.
- ◯ Acho normal olharem e continuo na mesma posição.
- ◯ Sequer noto ou me preocupo com isso.
- ◯ Nunca passei ou desconfiei que estava nessa situação.
- ◯ Outro:

Você costuma usar o seu crachá funcional publicamente? *

- ◯ Sim
- ◯ Não
- ◯ Esporadicamente.

Suponhamos que você possua um arquivo em texto (.txt) com todas as suas senhas, qual seria a sua atitude para o armazenamento destas valiosas informações em um pendrive? *

- ◯ Salvo normalmente.
- ◯ Troco a extensão do arquivo e salvo.
- ◯ Oculto o arquivo no pendrive, em propriedades do arquivo.
- ◯ Criptografo o pendrive antes de salvar.
- ◯ Crio várias pastas e salvo de forma disfarçada ao meio de outros tipos de arquivos.
- ◯ Uso de técnicas esteganográficas para esconder a informação.
- ◯ Criptografo o arquivo.
- ◯ Outro: _____

Caso necessite levar um HD externo ou notebook corporativo com várias informações relevantes da empresa para trabalhar em casa, e o aparelho seja perdido num local público, qual seria a sua atitude? *

- ◯ Comunicaria as autoridades policiais, somente.
- ◯ Entraria em contato com a equipe de TI e os informaria.
- ◯ Buscaria comprar outro equipamento igual e substituir sem que ninguém notasse a perda.
- ◯ Outro: _____

Ao encontrar um pendrive ou dispositivo de armazenamento USB no chão, próximo ao seu trabalho, qual seria a sua atitude? *

- ◯ Conectaria no computador de casa.
- ◯ Conectaria no computador da empresa.
- ◯ Conectaria no celular/tablet.
- ◯ Descartaria-o imediatamente.
- ◯ Outro: _____

Alguém, em seu conhecimento, já tentou se passar por quem não era, por telefone, e-mail ou fisicamente, para conseguir vantagens de acesso físico, ao sistema ou informações privilegiadas? *

- ◯ Sim
- ◯ Não
- ◯ Talvez

Conhece alguém que tenha se vingado (pelo sistema de informações) de sua empresa por motivo de demissão? *

- ◯ Sim
- ◯ Não

Já soube de algum conhecido, ou você já passou pela situação, na qual o cartão de crédito tenha sido clonado? *

- ◯ Sim
- ◯ Sim, um conhecido já passou por isso.
- ◯ Não

Já sofreu uma fraude online num banco? Com prejuízos financeiros? Ou conhece alguém que tenha sofrido... *

- ◯ Sim
- ◯ Sim, conheço alguém que tenha sofrido.
- ◯ Não

Já teve problemas por um fraudador estar se passando por você? (Clone, Fraudes, Uso de documentos). Ou conhece alguém que tenha passado pela situação... *

- ◯ Sim
- ◯ Sim, conheço alguém que tenha passado por isso.
- ◯ Não

Supondo que exista, em sua empresa, um software inovador que possibilite descobrir a cura de uma rara doença por meio de um algoritmo inteligente que analisa os genes dos pacientes e que pode salvar a vida de milhares de pessoas, porém a empresa é vendida a sua concorrente no exterior e o projeto é cancelado, incluindo a demissão de todos. Enquanto os seguranças esvaziam as salas, você tem um momento único para salvar o programa. Você faria essa cópia? *

- ◯ Sim
- ◯ Não

Houve alguma perda de informações (confidencialidade / integridade / disponibilidade) ou prejuízo financeiro em algum golpe de engenharia social descritos nessa pesquisa na qual tenha conhecimento? *

- ◯ Sim
- ◯ Não

A sua empresa já ofereceu algum treinamento ou forneceu instruções de prevenção sobre o tema em questão? *

- ◯ Sim
- ◯ Não

ENVIAR