UNIVERSIDADE DO SUL DE SANTA CATARINA

NORMANDO FERREIRA GUSMÃO

ENGENHARIA SOCIAL: O COMPORTAMENTO HUMANO COMO ELO MAIS FRÁGIL DA SEGURANÇA DA INFORMAÇÃO

VITÓRIA DA CONQUISTA - BAHIA

2019

NORMANDO FERREIRA GUSMÃO

ENGENHARIA SOCIAL: O COMPORTAMENTO HUMANO COMO ELO MAIS FRÁGIL DA SEGURANÇA DA INFORMAÇÃO

Relatório apresentado ao Curso **Tecnólogo em Gestão da Tecnologia da Informação,** da Universidade do Sul de Santa Catarina, como requisito parcial à aprovação na unidade de aprendizagem de Estudo de Caso.

Orientador: Prof. Ana Waley Mendonça

VITÓRIA DA CONQUISTA - BAHIA

2019

NORMANDO FERREIRA GUSMÃO

ENGENHARIA SOCIAL: O COMPORTAMENTO HUMANO COMO ELO MAIS FRÁGIL DA SEGURANÇA DA INFORMAÇÃO

Este trabalho de pesquisa na modalidade de Estudo de Caso foi julgado adequado à obtenção do grau de Tecnólogo em Gestão da Tecnologia da Informação e aprovado, em sua forma final, pelo Curso Superior de Tecnologia em Gestão da Tecnologia da Informação, da Universidade do Sul de Santa Catarina.

Vitória da Conquista, 08 de dezembro de 2019.

Profa. e Orientadora Ana Waley Mendonça, Mestre

Universidade do Sul de Santa Catarina

AGRADECIMENTOS

Gostaria de agradecer imensamente aos meus pais e minha esposa, mediante a tantos problemas não me fez desistir para conclusão deste curso. Aos tutores da UNISUL que sempre teve muita compreensão pelas minhas limitações e pecas aos da vida.

RESUMO

Dentro ou fora das organizações a informação é o bem mais precioso e de maior valor que se pode possuir. A partir do conhecimento é que se produz capital e valor. No espectro pessoal e nas relações cotidianas as pessoas se esquecem do valor das informações a respeito de suas próprias vidas e costumeiramente se tornam negligentes a respeito da proteção da própria intimidade e privacidade, cada vez mais se expondo e tornando-se acessíveis por meio das redes sociais. Este estudo foi realizado através de um formulário eletrônico que foi disponibilizado de forma aberta entre grupos de estudantes universitários da cidade de Vitória da Conquista-BA, que via internet podiam responder algumas questões. Assim, o objetivo geral da pesquisa foi compreender mais sobre o comportamento e o fator humano na utilização da internet, de modo a investigar a medida entre as informações e a aquisição de conhecimento. Cada uma das perguntas foi elaborada de modo a conhecer os hábitos desses usuários nas redes sociais, seus interesses e quais os cuidados administram com a navegação online, no intuito de perceber o nível de conhecimento sobre os meios de proteção utilizados para sua própria segurança, se é que fazem uso dos mesmos. Para tanto, foi utilizada ns metodologia de pesquisa um estudo de caso baseado em uma pesquisa de campo por meio de um questionário online respondido por estudantes de Vitória da Conquista-BA. Os resultados obtidos demonstraram que a despeito do nível de conhecimento acadêmico, existe um desdém quando à utilização dos serviços de proteção da segurança da informação e que grande parcela da população está fragilmente suscetível à ataques e investidas daqueles que se utilizam da Engenharia Social com má fé e objetivos ilícito.

Palavras-chave: Engenharia Social. Segurança da informação. Comportamento Humano. Redes Sociais.

SUMÁRIO

1 INTRODUÇÃO

No que tange a segurança da informação, nota-se que há um distanciamento e discrepância gigantesca entre a informação e a captura de conhecimento. E essa diferença se faz em grande parte porque o comportamento humano é fortemente alterado e ou influenciado pelas transformações sociais que acompanham as mudanças tecnológicas das últimas décadas.

A velocidade em que as informações são atualmente distribuídas e disponibilizadas não possibilita mais o acompanhamento pela mente humana, assim é necessário delimitar a área de interesse e de foco na absorção do conhecimento, ocorre, no entanto, que essa tarefa é especialmente difícil, uma vez que vivemos em uma sociedade e em tempos que se caracterizam pela liquidez, pela fluidez, e pela velocidade acentuada.

Assim o nível de exigência sobre si mesmo é alçado a níveis elevadíssimos. Urge que as decisões sejam prontamente tomadas e cada segundo seja aproveitado ao máximo. Nesse contexto, são verdadeiras dádivas divinas os aplicativos que facilitam a vida; permitem compras, realizar pagamentos, encurtam distancias e viabilizam conhecer pessoas, manter uma ponte para relacionar-se com os amigos que a cada dia ficam mais distantes e ocupados e pode-se também dizer dos efeitos psicológicos que eles proporcionam, como a ideia de engajamento, de popularidade, que tanto amaciam o ego e geram propiciam a sensação de pertencimento e identidade com alguns nichos sociais.

São tantos benefícios, que não há tempo para ser reticente, é preciso aproveitar, é preciso se render à imersão, mas isso não deve ser feito alheio aos cuidados e proteções que se deve ter como se teria para desenvolver qualquer uma dessas atividades também fora do aplicativo, como por exemplo ao realizar operações bancárias tem-se cuidado com os dados e uso das senhas diante de desconhecidos, logo é razoável que esse mesmo cuidado seja transposto para os meios eletrônicos.

Assim, é necessário esclarecer que diferente do que a maioria das pessoas leigas possa imaginar, a Engenharia Social não é um curso ou área do conhecimento, mas técnicas que podem ser usadas com finalidades morais ou imorais a depender de quem e com que finalidade as aplica.

Na ausência desses protocolos de segurança, programas de treinamento e procedimentos adequados, qualquer um está exposto e arrisca-se à tornar vítima de cibercriminosos, que se utilizam da meios ardilosos e conhecimento técnico específico para aproveitarem da falta de perspicácia e proteção dos incautos que navegam através de meios eletrônicos como se a internet fosse um mar tranquilo e não houvesse ali nenhum predador, esquecendo-se que o que se encontra na internet é a reprodução do que há fora dela, e por isso muitas vezes haverão pessoas que pretendem obter vantagem sobre outras, furtar, extorquir e praticar todo tipo de dano e atrocidade. A internet não é um mundo encantado e à parte, é um mundo real e cheio de perigos como o em que se vive.

Kevin Mitnick foi um dos maiores e talvez o mais famoso *cibercriminoso* da história dos Estados Unidos, pelo que foi capturado pelo FBI, e uma vez solto, após cumprir a sanção que lhe foi imposta, ele apresentou ao mundo através de seu livro: "A arte de enganar", o termo "Engenharia Social", nesse livro ele fornece orientações detalhadas para adesão de protocolos de segurança, caminhos como adesão de programas, manuais e treinamento em segurança técnica que qualquer individuo ou empresa deveria tomar para se precaver de investidas de *hackers* e assim reduzir a incidência de golpes e invasões, impedindo que esses permaneçam vulneráveis aos ataques e evitem aos ataques de toda sorte desses criminosos.

Desse modo, Mitnick apresenta a Engenharia Social assim (2003):

> A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia.

É de Mitnick também a assertiva de que o elo mais fraco da segurança é o fator humano. Primeiro o criminoso, e autor, explicita o seu pensamento, por causa da própria ignorância pertinente ao ser humano, isso porque o ser humano não consegue isolar as suas ações de modo puramente racional, mas move-se por credulidade, sentimentos, sensações, intuição, afetividade, desejos, todos esses passiveis de manipulação, além de tornarem o indivíduo instável e muitas vezes incauto e descuidado, e um único momento de descuido no que tange à segurança, pode ser fatal. Por isso o autor sugere que a segurança não é um

produto, e sim um processo, e que assim sendo todo o investimento tecnológico do mundo ainda não pode ser considerado inviolável, porque sempre que houver uma pessoa que o instrumentalize, haverá a possibilidade de fraquejar.

Segundo Pedro Henrique da Costa Braga a engenharia social pode parecer algo bem simplista e até tolo num olhar mais desatento, e só tem a capacidade de afetar um usuário mais leigo, mas em verdade, essas técnicas são as maiores ameaças à segurança da informação na atualidade, além de ser uma ferramenta muito mais poderosa do que se imagina e meio para se invadir os sistemas mais seguros (BRAGA, 2010).

Possivelmente o fator humano jamais será removido dos sistemas computacionais, a presença humana sempre estará lá e por isso mesmo essa possibilidade de ataque sempre se fará presente. Quando a vítima descarta ou despreza uma ameaça como essa é exatamente quando ela se torna ainda mais vulnerável, assim, quem quer que preze pela sua própria segurança ou de seu ambiente de trabalho, jamais deve ignorar um tipo de ameaça perene como esse (BRAGA, 2010).

1.1 O FATOR HUMANO

A Engenharia Social vem tratando os usuários de diversos ramos de atividades como simples fantoches, aproveitando cada dia mais da falta de informação para adquirir informação. O homem é o ponto chave para ser aplicada a Engenharia Social, pois através de aspectos psicológicos pode se definir a maneira correta de atacar aquele indivíduo.

Entre as características que podem ser mais bem exploradas temos: (i) vaidade pessoal e/ou profissional; (ii) autoconfiança; (iii) busca por novas amizades (necessidade de relacionar-se); (iv) falta de Segurança na atividade a ser realizada. Assim, ao determinar quais são as fraquezas do indivíduo é traçado um plano para poder finalizar o ataque de uma maneira sutil e simples que o usuário só irá perceber com o tempo.

1.2 REFLEXOS DA ENGENHARIA SOCIAL NAS REDES SOCIAIS

Com a necessidade das pessoas de se socializarem, as redes sociais têm se tornado grandes portais para atender as carências humanas. Entre essas carências estão mostrar pessoas que no seu íntimo estão travadas pelo seu ego.

As redes sociais tem seu lado positivo e negativo, positivamente vemos que no lado profissional, todos podem demonstrar seus feitos, currículos e trabalhos, no lado pessoal, familiares e amigos distantes podem acompanhar mais a vida deste usuário, porém negativamente vem o grande nível de informações pessoais que muitos usuários publicam facilitando assim que pessoas com más intenções, possam filtrar as suas vidas e utilizarem com má fé.

1.3 OUTROS MEIOS PARA SE UTILIZAR A ENGENHARIA SOCIAL

E-mails com “correntes”, seguidas no cabeçalho pela aquela imensa lista de endereços, facilita aos *hackers* na disseminação de arquivos infectados e links de programas espiões, muitos desses chamados de *keylogger*, onde o sistema copia tudo que é digitado pelo usuário e transmite o arquivo para os *hackers.*

Outro meio muito comum é pelo telefone, através de informações contidas na rede (internet), ou mesmo por uma simples nota fiscal que o indivíduo tem, ele liga para a vítima passando as informações como se estivesse em uma empresa idônea e oferece um serviço no qual a vítima acaba passando as informações necessárias para este aplicar um golpe.

Outras formas antigas, mas que muito ainda utilizam é ofertar ajuda a uma pessoa ingênua no caixa eletrônico, sendo cordial, educado este consegue adquirir a senha da vítima com muita facilidade. A segurança passada por estas pessoas é equivalente, ou simétrica à vontade de se aproveitar das suas vítimas.

2 TEMA

A engenharia social é um termo muito utilizado para exemplificar a situação em que pessoas usam de engenhosidade e conhecimento na internet para se aproveitar da ingenuidade e falta de informação de usuários menos precavidos, que ao utilizarem de qualquer serviço, acabam o fazendo de modo desprotegido e deixando margem para roubarem informações de qualquer gênero e com finalidades quase sempre escusas. Essa é uma técnica utilizada tanto no meio eletrônico, quanto no cotidiano. A utilização desse método requer grande capacidade comunicativa e quase sempre é explorada por intermédio do ganho da confiança dos próprios usuários, que se tornam vítimas.

O número desenfreado de redes sociais criadas atualmente, além das mais variadas ofertas de aplicativos e serviços online, propicia que os usuários estejam cada vez mais vulneráveis, fornecendo informações da sua vida, do seu cotidiano, dando margem a inúmeras formas de pessoas com más intenções de adquirirem dados para um possível ataque a este usuário. O comportamento humano individual e a sua credulidade, além da falta de acautelamento é exatamente o que alimenta essa prática e o que leva a fartar-se de êxito os *cibercriminosos*.

Assim, resta-nos questionar: qual a medida entre as informações, a aquisição de conhecimento e a efetiva proteção dos usuários de sistemas e serviços de internet?

3 OBJETIVOS

3.1 OBJETIVO GERAL

O objetivo desse estudo é o de compreender mais a respeito do comportamento e fator humano na utilização da internet e assim perceber quais as fontes práticas de suas debilidades, investigando qual a medida entre as informações, a aquisição de conhecimento e a efetiva proteção dos usuários de sistemas e serviços de internet.

3.2 OBJETIVOS ESPECÍFICOS

Da realização do estudo de caso da pesquisa de campo, são os objetivos específicos:

3.2.1 Entender, por meio da análise de dados coletados, como é possível que pessoas que detêm condições de obterem conhecimento e de praticá-lo como estudantes de ensino superior da cidade de Vitória da Conquista, podem ser vítimas e alvos fáceis de algozes por meio do uso da Engenharia Social.

3.2.2 Decifrar, por meio da análise de dados coletados, o comportamento desses estudantes, traçando estratégias de preservação e proteção para evitar que sejam vitimados ou re-vitimados por esses ataques.

4 PROCEDIMENTOS METODOLÓGICOS

4.1 CAMPO DE ESTUDO

Teremos um estudo de caso baseado numa pesquisa de campo para consultar um público estudantil residente em Vitória da Conquista-BA com acesso à internet como base da análise, para que à partir da elaboração de um questionário digital, composto de 7 (sete) questionamentos, e com acesso através do link do questionário online, que foi divulgado entre grupos on-lines de estudantes, tendo o retorno positivo de 73 (setenta e três) estudantes. As questões levantadas devem inquirir sobre a utilização e comportamento do público às redes sociais e demais serviços digitais, As respostas devem viabilizar um olhar mais claro e contundente da exposição nas redes digitais e das brechas por onde a Engenharia Social pôde ou poderia ser aplicada com esse público específico.

4.2 INSTRUMENTOS DE COLETA DE DADOS

O site que possibilitou a criação do questionário é o Survey Monkey, um site que permite a realização de questionários e pesquisas online, com ou sem custo e possui diversos recursos para filtrar essas pesquisas, delimitando inclusive o público alvo, quando necessário e de interesse do pesquisador.

Tabela 1 – Instrumento de coleta de dados

Instrumento de coleta de dados	**Universo pesquisado**	**Finalidade do Instrumento**
Entrevista	Estudantes cursando ensino superior do município de Vitória da Conquista – Bahia.	Identificar comportamento dos estudantes nas redes sociais e internet de modo geral.
Observação direta ou dos participantes	Redes sociais, aplicativos e meios de navegação online.	Verificar as brechas deixadas por esses usuários que poderiam ser acessadas por meio de Engenharia Social, além de perceber o seu nível de compreensão a respeito dos riscos a que estão se expondo.
Documentos	Questionário online.	Respostas verídicas desse público alvo formado por 73 (setenta e três) voluntários.
Dados arquivados	Gráficos confeccionados a partir das respostas obtidas.	Compilar os dados obtidos e estabelecer compreensões a respeito do material coletado.

Fonte: CAVALCANTI e MOREIRA (2008)

5 APRESENTAÇÃO E ANÁLISE DA REALIDADE OBSERVADA

5.1 ESTRUTURA DO RECURSO ANALISADO

O psicólogo Ricardo Mégre, em entrevista para o jornal “Diário de Aço” realizada por Marcelo Camargo em 2017, aponta que a internet é, atualmente, a maior rede de relações existentes, onde tudo e todos estão conectados ao mesmo tempo. O psicólogo aponta que a ferramenta internet, aliada às redes sócias servem como máscara para a verdade dos sujeitos por trás dos avatares do campo virtual (CAMARGO, 2017).

De igual modo, a redação do “Diário do Nordeste”, jornal digital, aponta que a conexão à internet significa uma abertura para o conhecimento, mas também para ameaças inimagináveis do mundo externo, como os *scams*, os golpes realizados na rede mundial de computadores por intermédio de e-mails falsos.

Já Andy Bochman, da “Harvard Bussiness Review Brasil” em parceria com a UOL, aponta que se de alguma forma estiver conectado à internet, nunca estará completamente seguro, por mais que haja um grande investimento em segurança digital. (BOCHMAN, 2018)

De acordo com Leonardo Werner Silva do jornal “Folha de S. Paulo”, a criação da internet se deu em 1969 com o nome original de “Arpanet”, nos Estados Unidos, tendo, incialmente, a função de interligar laboratórios de pesquisa, servindo de garantia de comunicação entre os cientistas e os militares; pertencia, então, ao departamento de Defesa norte-americano (SILVA, 2001).

O crescimento do *arpanet* se tornou maior, no mundo acadêmico, em 1982, tendo sido expandido para países além dos Estados Unidos da América para países como Holanda, Dinamarca e Suécia (SILVA, 2001).

O uso comercial da *arpanet* foi liberado em 1987, após quase duas décadas de uso apenas científico e acadêmico; assim, em 1992, iniciou-se o surgimento dos mais diversos provedores de acesso à internet; no mesmo ano o Word Wide Web foi inventado, pelo laboratório Europeu de Física de Partículas (CERN) (SILVA, 2001).

Segundo Anna Adami do “InfoEscola”, com o surgimento da internet e a aproximação entre as pessoas com o aprimoramento desta tecnologia, surgiram as redes sociais, ainda na

década de 90. Conceitua a rede social como uma estrutura que inter-relaciona empresas ou pessoas conectadas pelas mais diversas relações, de acordo com suas preferências e particularidades.

A primeira rede social foi criada em 1995 e se chamava “Classmates”, tendo como objetivo reunir antigos colegas de escola ou faculdade que haviam perdido contato, uso que ainda se mostra comum nos dias atuais; criada por Randy Conras e abrangia, incialmente, apenas os Estados Unidos e o Canadá, chegando a ter cerca de 50 milhões de usuários cadastrados ainda na década de 90 (LUIZ, 2019).

Considerando os benefícios que a tecnologia proporciona devem ser observados os malefícios que envolvem o uso inadequado da rede, como a ausência de privacidade dos internautas, invasão de privacidade e uso de imagens sem o consentimento (SANTOS, 2015).

A velocidade da comunicação e o avanço das redes geram um uso excessivo em momentos inadequados, como em reuniões e família sem um diálogo presencial, estando num estado de atenção plena aos aparelhos de comunicação com o mundo externo (SANTOS, 2015).

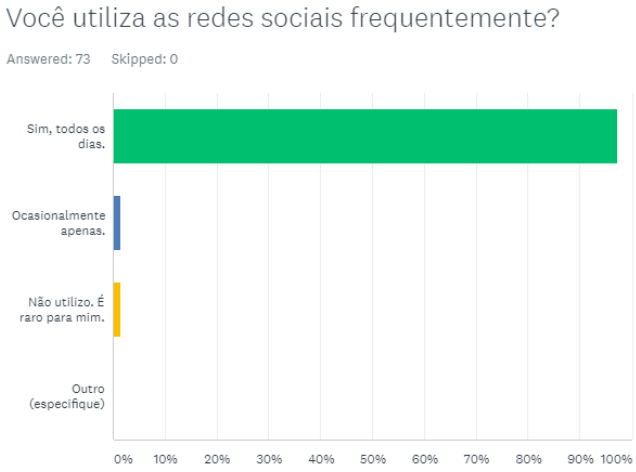
De acordo com “O Estadão”, estudos realizados pela consultoria Comscore, mais de 114 milhões de pessoas por mês acessam as redes sociais no Brasil. Dentre o público alvo, o domínio não é apresentado pelos adolescentes; segundo a pesquisa, 27% do público das redes sociais são adultos com mais de 45 anos, em plataformas como *Facebook. Instagram, twitter, pintrest, LinkedIn, Snapchat* e *YouTube.*A segunda principal faixa etária correspondia a indivíduos entre 25 e 34 anos.

5.2 DESCRIÇÃO E ANÁLISE DA REALIDADE OBSERVADA

Da efetivação do estudo de caso com pesquisa de campo, tivemos um retorno de 73 respondentes. As questões apresentadas foram as seguintes: (i) você utiliza as redes sociais frequentemente? ; (ii) você realiza ou já realizou transações financeiras (compras, pagamentos, transferências...) pela *internet* ou aplicativos virtuais?; (iii) se sente confortável e seguro na internet? ; (iv) sente que de algum modo se expõe nas redes sociais (informações pessoais, fotos de familiares e próprias, localização)?; (v) utiliza algum dispositivo ou ferramenta de segurança ao navegar na *internet* e utilizar redes sociais?.

Com relação ao primeiro questionamento (você utiliza as redes sociais frequentemente?) realizado, mostrou-se unânime a resposta dos estudantes:

Gráfico 1 – Pergunta: você utiliza as redes sociais frequentemente?

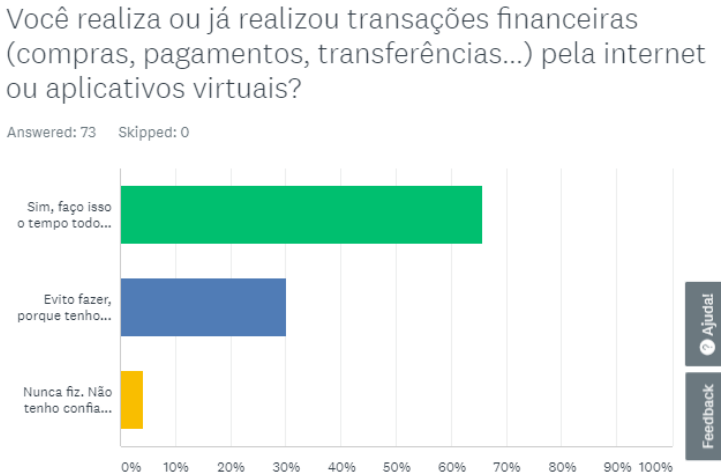


Fonte: autoria própria (2019)

A essa pergunta todos os entrevistados responderam, 70 estudantes que sim, todos os dias; 1 estudante respondeu que ocasionalmente apenas e 1 estudante respondeu a terceira assertiva, “Não utilizo. É raro pra mim”.

Com relação ao segundo (você realiza ou já realizou transações financeiras (compras, pagamentos, transferências...) pela *internet* ou aplicativos virtuais?) questionamento realizado, mostrou-se a resposta dos estudantes:

Gráfico 2 – Pergunta: você realiza ou já realizou transações financeiras (compras, pagamentos, transferências...) pela *internet* ou aplicativos virtuais?

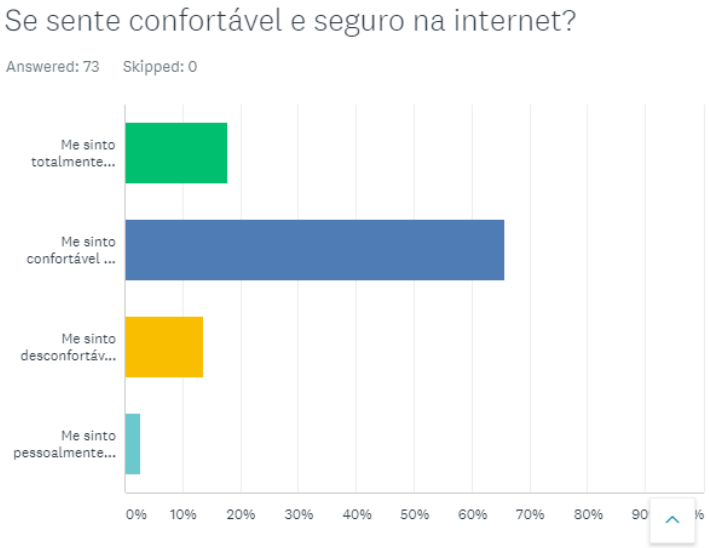


Fonte: Autor (2019)

A esta pergunta: 48 dos entrevistados responderam que “Sim, faço isso o tempo todo. Considero muito prático e eficiente” conforme a primeira assertiva. 22 estudantes responderam que evita fazer esse tipo de transação por medo de dar algo errado e apenas 3 estudantes disseram nunca ter realizado.

Com relação ao terceiro (se sente confortável e seguro na internet?) questionamento realizado, mostrou-se a resposta dos estudantes:

Gráfico 3 – Pergunta: se sente confortável e seguro na internet?

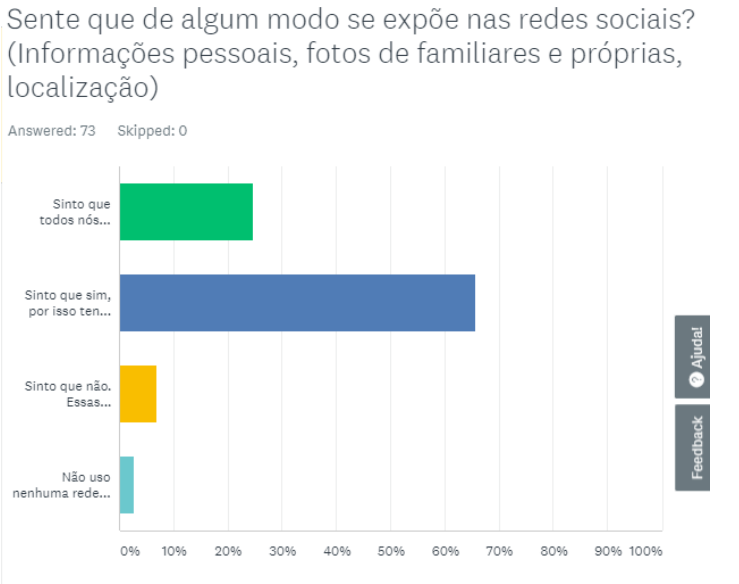


Fonte: Autor (2019)

Desse modo, responderam: 13 estudantes responderam de acordo com a primeira assertiva (me sinto totalmente confortável e seguro(a), não vejo problema algum); 48 optaram pela segunda assertiva (Me sinto confortável e acho divertido, mas não me sinto muito seguro(a)); 10 escolheram a terceira resposta (me sinto desconfortável, acho que as pessoas se exibem demais. Acho que não é um ambiente muito seguro também) e 2 estudantes marcaram a última assertiva (me sinto pessoalmente desconfortável, mas acho que é um ambiente bem seguro).

Já com relação ao questionamento de número quatro (Sente que de algum modo se expõe nas redes sociais? (Informações pessoais, fotos de familiares e próprias, localização), as respostas foram:

Gráfico 4 – Pergunta: sente que de algum modo se expõe nas redes sociais (informações pessoais, fotos de familiares e próprias, localização)?

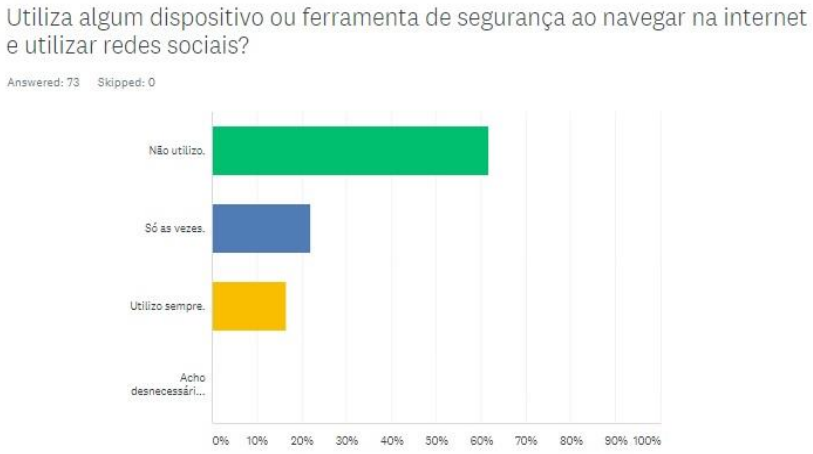


Fonte: Autor (2019)

Mostrou-se o resultado em: 18 foram os respondentes que marcaram conforme a primeira assertiva (Sinto que todos nós estamos expostos o tempo todo, isso não me incomoda); 48 marcaram a segunda assertiva (sinto que sim, por isso tenho muito cuidado com as informações que divulgo. A exposição me incomoda); 5 estudantes responderam de acordo com a terceira assertiva (sinto que não. Essas informações estão seguras comigo, não divulgo nada nas redes sociais) e apenas 2 marcaram conforme a quarta assertiva dizendo não possuir rede social.

Por fim, o quinto e último questionamento (utiliza algum dispositivo ou ferramenta de segurança ao navegar na *internet* e utilizar redes sociais) mostrou os seguintes resultados:

Gráfico 5 – Pergunta: utiliza algum dispositivo ou ferramenta de segurança ao navegar na internet e utilizar redes sociais?



Fonte: Autor (2019)

Dos respondentes 45 admitiram que não utilizam nenhum dispositivo ou ferramenta de segurança; 16 disseram que só as vezes; 12 pessoas disseram utilizar sempre e ninguém disse considerar desnecessário esse tipo de proteção.

6 PROPOSTA DE SOLUÇÃO DA SITUAÇÃO-PROBLEMA

Não há como extinguir por completo o risco de incidência da engenharia social, no entanto, ainda que não se possa solucionar integralmente o problema, existe métodos que podem amenizar a sua prática e proteger os usuários que façam a adesão desses recursos, sendo sem sombra de dúvidas o melhor e mais assertivo deles o investimento em conhecimento.

6.1 PROPOSTA DE MELHORIA PARA A REALIDADE ESTUDADA

A maneira mais eficaz de combate à essas ameaças é o investimento em treinamentos, vez que o usuário treinado é capaz de visualizar em grande parte dos casos a tentativa de invasão da sua privacidade e assim incorre numa probabilidade muito menor que a usual de se deixar vitimar.

Nas redes sociais é preciso evitar a divulgação excessiva da vida pessoal, sendo esse meio uma forma simples, mas muito eficaz de evitar que esse tipo de engenharia aconteça. Deve-se evitar colocar fotos de família descriminando quem são, onde o usuário frequenta ou irá frequentar, assim pode-se evitar sequestros relâmpagos, supostas ligações para suas residências simulando ações criminosas.

Nas escolas é imprescindível que sejam ministradas aulas de informática com ênfase em segurança da informação, essa prática desde a mais tenra idade seria uma excelente forma de preparar crianças e adolescentes, para que sejam resguardados preventivamente.

Instituições financeiras nos alertam frequentemente que não enviam senhas ou efetuam qualquer atividade por e-mail, alertam sobre as falsas ajudas fornecidas nos caixas eletrônicos entre outros, esse tipo de cuidado e informação alastrada incessantemente propicia um comportamento mais acautelado e consciente dos seus usuários.

6.2 RESULTADOS ESPERADOS

Através da aplicação das medidas de segurança pessoal propostas, espera-se que haja uma maior segurança entre os usuários das redes sociais e da internet, para que, desse modo, haja um desenvolvimento sadio das relações interpessoais pelo uso da rede.

Pretende-se que, assim, demonstrem maior confiança e segurança para a realização de transações financeiras pelo uso da internet e aplicativos virtuais; bem como o aumento da segurança pessoal de dados, informações e imagens pessoas daqueles que as usam. Com a introdução, cada dia maior, das redes de informação, no dia-a-dia dos usuários e não-usuários, faz-se imprescindível que este seja um ambiente que transmita segurança e conforto para a sua utilização.

É necessária a utilização da internet e seus componentes de forma consciente e benéfica, Principalmente, objetiva-se o incentivo do "auto-cuidado", pelos usuários, para evitar consequências danosas ao uso irresponsável e descuidado da rede mundial de computadores e das redes sociais.

A utilização de ferramentas de proteção para vírus de computador, afim de neutralizar ameaças externas, configura papel central na proteção e na garantia de segurança aos usuários *on-line*, assim como a instalação de programas certificados e com garantia, afastando completamente os *softwares* piratas.

6.3 VIABILIDADE DA PROPOSTA

Já no que se refere à viabilidade da proposta, esta pode ser desenvolvida de modo individual, sem a necessidade de um dispendioso gasto financeiro pelos usuários da rede, já que, tal investimento, demonstra, numa perspectiva para o futuro, maior proteção para uma maior segurança.

Ademais, a proteção com base nas propostas aparentas, de certo modo, imediata, por se tratarem de cuidados minimamente desgastantes e custosos, já que, a atenção e a disponibilização de informações de cunho pessoal na internet dependem única e exclusivamente do próprio usuário.

Existem soluções praticas que, de forma individual, podem ser implementadas pelos usuários para a proteção pessoal e proteção dos seus dados pessoais; proteções básicas como não deixar a webcam e o microfone ligado em desuso, realizar o *logon* de e-mail's e redes sociais após o uso, mesmo em computadores particulares e a não divulgação de dados pessoais na internet, bem como o cuidado necessário com o *download* de dados da internet. A aplicação de cuidados básicos com a proteção pessoal, confere, facilmente, uma maior segurança no uso da internet, ponto de grande relevância do presente estudo de caso.

7. CONSIDERAÇÕES FINAIS

O avanço tecnológico trouxe consigo diversas facilidades; a possibilidade de se comunicar com pessoas que estão distantes, de trabalhar dentro de casa, de realizar transações bancárias com facilidade por meio da tela de um celular, bem como comprar, tirar fotos, envia-las e arquiva-las.

Entretanto, seu uso desmedido e despreocupado abre brechas na proteção individual dos usuários, ocorrendo, desse modo, o fenômeno da engenharia social, ferramenta de ataque à sistemas de informação, em especial, a de empresas.

Mitnick, ao eluciadar as formas para a eficácia da engenharia social apontava que o primeiro passo para a obtenção de informações por *hakers* é o convencimento do alvo, já que o comportamento humano é a causa da vulnerabilidade maior dos sistemas de segurança, por serem indivíduos que possuem traços comportamentais que os tornam suscetíveis ao ataque (GEER, 2017).

A disponibilização voluntária de informações pessoas nas redes sociais possibilita que indivíduos mal-intencionados enviem e-mails infectados de modo a despertar o interesse da vítima, ao inserir no mesmo conteúdo que desperte a sua curiosidade (GEER, 2017).

Foi possível perceber, da realização do questionário *on-line*, a quase unanimidade sobre a frequência diária do uso das redes sociais, o que interfere diretamente no uso destas para realizar compras, pagamentos e afins; mas, neste ponto, os dados apontam certa queda no percentual do primeiro questionamento, ainda que a maior parte confirme já ter realizado.

Todavia, no que se refere ao conforto e à sensação de segurança no uso da internet, a maior parte demonstrou que apesar se sentirem confortáveis e acharem o ambiente divertido, não se sentem muito seguros, seguido por aqueles que se sentem seguros e não veem algum problema relacionado à segurança.

O receio de se tornar a próxima vítima gera, em boa parte dos voluntários do presente estudo, uma insegurança na utilização da *internet* e das redes sociais, além de uma constante sensação de exposição completa pessoal e de terceiros.

Entretanto, a falta de cuidado e atenção no uso das redes auxilia na insegurança dos usuários, já que, parte da proteção, tem como início o interesse pessoal e a preservação de informações pessoais. O excesso do uso também se mostra como uma característica negativa, ao ponto em que gera o distanciamento presencial.

Encontramo-nos num impasse, onde há um crescente desejo por proteção no meio virtual e a ausência de cuidado pessoal com a exposição e a utilização deste. Mínimos cuidados, tomados de forma individual, podem se configurar responsáveis para que seja conferido um *status* maior de segurança e conforto no uso da rede mundial de computadores e aplicativos derivados dos seus sistemas.

8. REFERÊNCIAS BIBLIOGRÁFICAS

ADAMI, Anna. **Redes Sociais.** Disponível em: https://www.infoescola.com/sociedade/redes-sociais-2/. Acesso em: 03 nov 2019

AUTOR DESCONHECIDO. **Adultos com mais de 45 anos são principais usuários de redes sociais no País, diz estudo.** Disponível em: https://link.estadao.com.br/noticias/cultura-digital,adultos-com-mais-de-45-anos-sao-principais-usuarios-de-redes-sociais-no-pais-diz-estudo,70002907108. Acesso em: 02 nov 2019.

AUTOR DESCONHECIDO. **Descubra agora 8 formas de se proteger na internet.** Disponível em: http://www.globalsegmg.com.br/8-formas-de-se-proteger-na-internet/. Acesso em: 09 nov 2019

AUTOR DESCONHECIDO. **Insegurança na internet ameaça usuários.** Disponível em: https://diariodonordeste.verdesmares.com.br/editorias/negocios/inseguranca-na-internet-ameaca-usuarios-1.648609. Acesso em: 01 nov 2019

BOCHMAN, Andy. **Insegurança na internet.** Disponível em: https://hbrbr.uol.com.br/inseguranca-na-internet/. Acesso em: 30 out 2019

BRAGA, Pedro Henrique da Costa. **Técnicas de Engenharia Social**, 2010. Disponível em: <https://securityinformationnews.files.wordpress.com/2014/02/tecnicas_de_engenharia_social.pdf>. Aceso em: 11 nov. 2019.

CAVALCANTI, Marcelo e MOREIRA, Enzo. **Metodologia de estudo de caso**: livro didático. 3. ed. rev. e atual. Palhoça: Unisul Virtual, 2008. 170 p.
CAMARGO, Marcelo. **Relações humanas são modificadas pelas redes sociais, aponta psicólogo.** Disponível em: https://www.diariodoaco.com.br/noticia/0054059-relacoes-humanas-sao-modificadas-pelas-redes-sociais-aponta-psicologo. Acesso em: 29 out 2019

GEER, David. **Conheça seis das técnicas de engenharia social muito eficazes**. Disponível em: https://cio.com.br/conheca-seis-das-tecnicas-de-engenharia-social-muito-eficazes/. Acesso em: 27 out 2019

LOHN, Joel Irineu. **Metodologia para elaboração e aplicação de projetos**: livro didático. 2 ed. rev. e atual. Palhoça: Unisul Virtual, 2005. 100 p.

LUIZ, André. **Classmates: conheça a primeira rede nacional da história,k ainda ativa.** Disponível em: https://acrediteounao.com/primeira-rede-social-da-historia/. Acesso em: 09 nov 2019

MITNICK, Kevin D; SIMON, William L. **A arte de enganar: Ataque de Hackers: Controlando o Fator Humano na Segurança da Informação.** Makron Books, Pearson Universidades. 01. Ed. 2003**.**

RAUEN, Fábio José. **Roteiros de investigação científica**. Tubarão: Unisul, 2002.
SILVA, Leonardo Werner. **Internet foi criada em 1969 com o nome de "Arpanet" nos EUA.** Disponível em: https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml. Acesso em: 05 nov 2019

SANTOS, Wilma Santana dos. **A influência da internet na vida das pessoas.** Disponível em: https://br.blastingnews.com/sociedade-opiniao/2015/07/a-influencia-da-internet-na-vida-das-pessoas-00466575.html. Acesso em: 22 nov 2019.