FACULDADE DE TECNOLOGIA ALCIDES MAYA

CURSO TÉCNICO DE INFORMÁTICA

VICTÓRIA REGINA DA SILVA PEREIRA

VINICIUS CORRÊA MEDEIROS

A Segurança e Privacidade nas Redes Sociais

PORTO ALEGRE

2020

VICTÓRIA REGINA DA SILVA PEREIRA[1]

VINICIUS CORRÊA MEDEIROS[2]

A Segurança e Privacidade nas Redes Sociais

Projeto de Pesquisa apresentado como requisito parcial para obtenção do título de Técnico em Informática da Faculdade de Tecnologia Alcides Maya.

Orientador: Prof. João Padilha Moreira[3]

Porto Alegre

2020

[1] Aluna do curso técnico em informática – email: vicksp1204@gmail.com
[2] Aluno do curso técnico em informática – email: vinicius.correamedeiros@gmail.com
[3] Professor orientador – email: professorjoaomoreira@gmail.com

SUMÁRIO

1 INTRODUÇÃO

Diante do constante avanço tecnológico, a Segurança da Informação é algo fundamental e de extrema importância na área de Tecnologia da Informação para solucionar diversos tipos de problemas relacionados à perda ou vazamento de dados e informações pessoais e empresariais. A Segurança da Informação está diretamente relacionada com a proteção de informações, no sentido de preservar o valor que elas possuem para um indivíduo ou uma empresa.

Quando falamos em rede social, o que vem à mente em primeiro lugar são sites como Facebook, Twitter e LinkedIn ou aplicativos como Snapchat e Instagram, típicos da atualidade. Mas a ideia, no entanto, é bem mais antiga: na sociologia, por exemplo, o conceito de rede social é utilizado para analisar interações entre indivíduos, grupos, organizações ou até sociedades inteiras desde o final do século XIX (RESULTADOS DIGITAIS, 2017).

Segundo (HOLANDA, 2020), muito antes das Redes Sociais na internet existirem, as pessoas costumavam se encontrar para conversar e trocar ideias relacionadas a assuntos de interesse comum. Com o surgimento das Redes Sociais, esse tipo de comportamento foi se tornando cada vez mais simples e conveniente, pois permitiu que pessoas de diversos lugares ao redor do globo se comunicassem entre si sem precisar estar juntas.

A primeira Rede Social teve origem em 1995, no Canadá e EUA, e chamou-se Classmates.com, cujo objetivo era, principalmente, reunir os estudantes, colegas e amigos de uma faculdade para se conectarem mais facilmente (TECHTUDO, 2014).

1.1 Definição do Tema ou Problema

Há diversos perigos nas Redes Sociais, como por exemplo, a exposição de dados pessoais e vazamento de dados ou ser vítima de crimes cibernéticos, o que será abordado mais adiante no trabalho. Por ser uma plataforma de relacionamentos, as Redes Sociais geralmente encorajam seus usuários a preencherem e publicarem detalhes sobre si em seus perfis, a fim de que as pessoas, que visitarem sua página, tenham algum conhecimento sobre elas ou para algum amigo conseguir encontrá-las de forma mais rápida. Porém, ao fazer isso, o usuário poderá estar divulgando informações e que podem acabar sendo cobiçadas por pessoas mal intencionadas.

A exposição exagerada nas redes sociais, não causa problemas apenas nos casos extremos de sequestro e violência. [...] Por mais ingênua que pareça, dependendo da situação, uma foto, por exemplo, pode dizer muito: locais que você frequenta, a localização exata da sua casa, a escola que seu filho estuda, bens que você possui… E, na internet, para mentes criminosas, esse tipo de informação pode ser usadas para uma série de golpes, fraudes e até para planejar um sequestro (SANTINO, 2019).

1.2 Delimitações do Trabalho

Uma pesquisa sobre o quanto as pessoas compartilham informações nas Redes Sociais e o impacto que isso causa na vida delas.

1.3 Objetivos

1.3.1 Objetivo Geral

Ressaltar que a Segurança da Informação é relevante ao fazer uso das Redes Sociais, de modo que se possa estar presente, fazendo bom uso e ainda assim, assegurar a integridade de suas informações pessoais.

1.3.2 Objetivos Específicos

a) Apontar os possíveis riscos aos quais os usuários se submetem ao utilizar das Redes Sociais sem tomar as devidas precauções;

b) Analisar, através de uma pesquisa, como os usuários utilizam as Redes Sociais normalmente;

c) Compreender como os cibercriminosos e pessoas mal intencionadas geralmente interceptam e fazem uso indevido de informações alheias;

d) Descrever exemplos de crimes virtuais mais frequentes e apresentar maneiras de se proteger para evitar ser vítima desses criminosos;

e) Sobressaltar as formas de usuários fazerem uso das Redes Sociais de forma consciente e segura, sem se expor e manter a privacidade de suas informações pessoais.

1.4 Justificativa

Este projeto visa enfasar a importância de sermos prudentes no uso e no cuidado ao inserir e pesquisar dados nas mídias sociais, usufruindo com equilíbrio e segurança as informações, sejam elas pessoais ou de interesse global.

2 REVISÃO BIBLIOGRÁFICA

2.1 Redes Sociais

Redes sociais é um conceito onipresente nos dias de hoje e ocupa espaço crescente no discurso acadêmico, nas mídias, nas organizações ou no senso comum (MARTELETO, 2010).

Atualmente, as Redes Sociais são um dos meios de comunicação mais relevantes na realização de atividades comerciais e relações interpessoais. No entanto, é necessário estar alerta ao acessar e compartilhar informações e dados, pois podemos estar comprometendo a segurança das mesmas.

Doneda (2012, pg. 4) define Redes Sociais como “serviços prestados por meio da Internet que permitem a seus usuários gerar um perfil público, alimentado por dados e informações pessoais, dispondo de ferramentas que permitam a interação com outros usuários, afins ou não ao perfil publicado”.

Para Nunes (2019, pg. 141) “A comunicação no século XXI ganhou novo terreno com o desenvolvimento da internet e com a propagação exponencial das redes sociais que ligam pessoas em todo o mundo, cruzando oceanos e continentes. Entre os muitos benefícios das redes sociais se destaca a importância da comunicação estabelecida entre os usuários (por mensagem, post, foto ou vídeo) com o objetivo de promover bons hábitos de saúde, prevenir doenças e outros comportamentos nocivos que podem por a própria vida em risco”.

A partir do momento em que as redes sociais se consagram no gosto dos usuários da internet, diferentes sites são criados. As principais redes sociais do século XXI surgiram no ano de 2004 e 2005 (Flickr, Orkut e Facebook). No entanto, uma característica desse ambiente é a evolução e a rápida transformação. No caso do Brasil, a rede social de maior sucesso na década passada foi o Orkut, porém, em pouco tempo, os usuários substituíram essa rede pelo Facebook e na atualidade o Orkut se encontra com suas atividades finalizadas (AMARAL, 2016).

Para criar um perfil nas redes sociais é necessário se cadastrar e preencher informações pessoais. As redes sociais incentivam os usuários a inserirem informações pessoais a fim de serem reconhecidas mais facilmente por pessoas que fazem ou passem a fazer parte do seu círculo de amizades, dessa forma, podem estar sujeitas a ataques cibernéticos por exporem demasiadamente seus dados.

No entanto, Amaral (2016, pg. 38) afirma que “Por causa disso, muitas pessoas criam perfis falsos, o que lhes permite disseminar informações e interagir com outros usuários sem poderem ser reconhecidos, o que consideramos um dos aspectos complexos do sistema. Na maioria das vezes os perfis falsos e ocultos são

empregados para disseminar mentiras, espalhar preconceitos e outras coisas nocivas contra determinados usuários. Porém, essas questões complexas também podem ser localizadas em perfis reais, quando determinados usuários abandonam princípios éticos e usam a virtualidade para atacar e discriminar pessoas e comportamentos".

Para Deslandes e Arantes (2017, pg. 175), as pessoas se conhecem e se relacionam umas com as outras pelas redes sociais de forma muito veloz, desse modo, a proporção de crimes virtuais também crescem rapidamente, principalmente os ocorridos nas redes sociais. "Tais crimes aumentaram muito, devido à facilidade encontrada para praticá-lo, onde muitas informações pessoais estão disponíveis na rede. Assim, os criminosos coletam dados e informações privilegiadas para extorquir ou simplesmente prejudicar o outro, causando prejuízos moral e financeiros". (DESLANDES; ARANTES, 2017, pg. 175).

2.2 Segurança

Um dos grandes desafios da Tecnologia da Informação é a segurança dos dados e informações e, em especial, no armazenamento e transporte das mesmas.

Atualmente, as informações, sejam elas empresariais ou pessoais, são objetos de valor, confidenciais e que não devem ser manipuladas por qualquer pessoa que possa utilizá-las com más intenções ou para fins ilícitos. Num contexto organizacional, essas informações podem estar relacionadas com os dados armazenados em software e seu uso eficientes, com estratégias de extração de dados, que são utilizadas para identificar um perfil de usuário ou um consumidor, no caso de uma empresa, personalizando o negócio com um diferencial competitivo.

2.2.1 Características

A Segurança da Informação têm como base os seguintes aspectos denominados Pilares da Segurança da Informação:

- **Confidencialidade**: Capacidade que um sistema possui de impedir a visualização e o uso indevido de informações que são delegadas somente à determinados usuários que possuem autorização para tal;
- **Integridade**: Atributo da segurança que garante que nenhuma pessoa, não autorizada, use e altere a informação, assegurando assim, sua autenticidade.
- **Disponibilidade**: É a garantia de que a informação esteja sempre disponível para uso legítimo, no qual o sistema cumpriu a tarefa solicitada sem falhas internas.

2.2.2 Porque se preocupar com a Segurança da Informação?

Existem diversos motivos que exigem que empresas e usuários de Redes Sociais se preocupem em proteger e manter a autenticidade de suas informações. A segurança é uma preocupação constante quando se trata de tecnologia da informação. Roubo de dados, *malwares* e uma série de outras ameaças acontecem a todo momento sendo necessário se proteger delas (TECH ENTER, 2019).

Os riscos associados à falta de segurança são inúmeros; uma empresa pode perder dados importantes caso haja uma falha em seu banco de dados, deixando-o vulnerável ao ataque de hackers ao sistema da organização, onde terão acesso direto aos dados de clientes e informações confidenciais da empresa.

Por outro lado, os benefícios esperados por um bom sistema de segurança cibernético vão evitar: fraudes, espionagem comercial, vazamento de dados, uso indevido, sabotagens e diversos outros problemas que possam prejudicar uma empresa ou pessoas físicas, que expõem seus dados e informações pessoais diariamente nas mídias sociais.

A Segurança da Informação impede que os dados e informações caiam nas mãos de pessoas não autorizadas [...] destruídos sem autorização, roubados ou danificados. Também garante a continuidade do negócio, mantendo as informações disponíveis, integras e com a certeza de sua autenticidade, detectando, documentando e combatendo as ameaças aos sistemas, infraestrutura e dados (INFONOVA, 2018).

2.3 Crimes Cibernéticos

Apesar das inúmeras vantagens e recursos de se utilizar a internet é importante ter consciência dos riscos e complicações que podem comprometer sua segurança, tanto para pessoas físicas quanto para empresas e organizações.

Crimes cibernéticos são atividades criminosas que podem ser realizadas por pessoas ou organizações e que geralmente visam o lucro, embora haja casos onde os motivos sejam pessoais ou políticos.

Quando o alvo dos criminosos é atingir um computador ou uma rede de computadores são utilizados vírus e malware para infectar os computadores com o intuito de danificar ou impedir serviços de funcionarem, disseminar malwares, informações ou imagens ilegais.

2.4 Exemplos de Crimes Cibernéticos

2.4.1 Ataques de Malwares

Malware é a abreviação de software malicioso, é um termo usado para descrever qualquer código ou programa que seja prejudicial aos sistemas. Caracterizam-se por serem intencionalmente prejudiciais, pois invadem os sistemas e desabilitam ou danificam computadores e outros dispositivos, assim, assumindo o controle parcial de suas operações (MALWAREBYTES, 2020).

Malwares são usados como uma forma de ganhar dinheiro de forma ilícita. Podem roubar, criptografar ou apagar dados; alterar ou sequestrar funções fundamentais do computador e inclusive espionar sua atividade sem permissão.

Um computador comprometido por malware pode ser usado por criminosos cibernéticos para diversos fins. Entre eles, roubar dados confidenciais, usar o

computador para realizar outros atos criminosos ou causar danos aos dados (KASPERSKY, 2020).

Os quatro principais tipos de malware que se deve estar atento são:

- **Ransomware**: Ransomware é um tipo de malware usado para extorquir dinheiro, pois mantém os dados ou o dispositivo da vítima como refém em troca de um resgate (KASPERSKY, 2020). O Malware geralmente é instalado após clicar em algum link enviado por e-mail, sites maliciosos ou algum arquivo enviado através de mensagens em anexo;

- **Spyware**: É um tipo de Malware que pode coletar informações sobre a atividade dos computadores infectados, sem o conhecimento do usuário. Ele opera de modo totalmente discreto, de forma que sua presença possa passar despercebida facilmente. Silenciosamente, um Spyware pode monitorar todas as atividades da máquina, como teclas digitadas, uso e atividades na web, etc. Esses registros passam a ser armazenados secretamente pelos criminosos (REAL PROTECT, 2015).

- **Worms**: São programas maliciosos que se espalham de um computador para outro. Diferente dos vírus, eles operam de forma autônoma, ou seja, não se ligam a outro programa. Geralmente se espalham por uma rede de computadores através das vulnerabilidades de segurança ou outras formas como envio de e-mails e se copiando por compartilhamentos. Worms não causam danos aos arquivos de sistemas e outros programas importantes, porém, consomem largura de banda, o que diminui o desempenho da rede. Também podem se multiplicar e baixar componentes perigosos como um Ransomware (REAL PROTECT, 2015).

- **Trojan:** Um Trojan (ou Cavalo de Tróia) é um tipo de Malware que se disfarça como algo legítimo para ganhar a confiança do usuário e assim obter permissão para ser instalado, por isso é preciso ter cuidado com sites que oferecem downloads gratuitos. A partir da instalação, o controle da máquina fica nas mãos do hacker. Os danos que um Trojan pode causar a uma empresa variam de roubo de dinheiro eletrônico, senhas e detalhes de logins,

> modificações e destruição de arquivos a até mesmo monitoramento de atividades do usuário (REAL PROTECT, 2015).

2.4.2 Phishing

Phishing é o ato de pescar informações, uma forma desonesta que cibercriminosos utilizam para enganar usuários e obter acesso a informações sigilosas como dados de cartões de crédito e nomes de usuário, senhas, CPF e números de contas bancárias.

As mensagens de campanhas de phishing podem conter anexos infectados ou links que redirecionam para sites maliciosos. Elas também podem solicitar que o destinatário forneça informações confidenciais (KASPERSKY, 2020).

2.5 Tipos de Crimes Virtuais

Atualmente, os crimes cibernéticos são tão comuns quantos outros crimes contra o patrimônio pessoal, visto que existem delegacias especializadas para a efetuação dessas denúncias.

De acordo com Ceia (2018, p.16):

> Os crimes podem ser de diversos tipos, comprometendo somente a parte computacional, provocando uma falha em um sistema, ou um bloqueio, uma perda de informação, causando lentidão ou algo parecido. Podem também atingir somente a parte humana, por exemplo, no caso dos fatos psicológicos, expondo a vida pessoal da vítima, ou ainda causando dano em ambas as partes.

Os crimes virtuais mais comumente praticados são a espionagem cibernética (hackers acessam dados do governo ou empresa); cryptojacking (exploração de

criptomoedas sem os devidos recursos); extorsão cibernética e ataques de ransomware. Esses são os crimes que mais acontecem no geral, entretanto, o assunto principal a ser tratado nesse trabalho são as redes sociais, então será abordado com mais profundidade os crimes relacionados ao tema mais adiante.

2.6 Crimes Cibernéticos nas Redes Sociais

As redes sociais surgiram com o intuito de facilitar o contato e comunicação, além de pessoas poderem compartilhar momentos memoráveis e importantes entre amigos e familiares à longa distância, através de mensagens, fotos e vídeos. As plataformas sociais mais populares hoje em dia são o Facebook, Instagram, Youtube, Whatsapp e Twitter. Contudo, apesar de suas vantagens, criminosos se escondem por trás dessas plataformas, procurando sua próxima vítima.

São diversos os crimes frequentemente praticados na internet e nas redes sociais. De acordo com Cruz e Rodrigues (2018, pg. 3) “[...] criminosos utilizam-se da rede para assediar pessoas, realizar discriminações, vender produtos ilegais como drogas, bem como realizar calúnia, injúria e difamação, apologia ao crime, pedofilia, espionagem, estelionato, roubo de identidade e inclusive terrorismo.”

Há também outros perigos como o Cyberstalking, que é a versão virtual do stalking, ou seja, o ato de perseguir, assediar ou ameaçar uma pessoa constantemente.

2.6.1 Cyberstalking

Evidenciado anteriormente, cyberstalking é uma perseguição virtual que envolve ameaças contra uma pessoa. Expor demasiadamente a rotina de vida nas redes sociais é um ato cometido por muitas pessoas e também é um dos principais comportamentos que podem facilitar a vida dos stalkers.

> O termo Cyberstalking [...] é versão virtual do stalking, comportamento que envolve perseguição ou ameaças contra uma

> pessoa, de modo repetitivo, manifestadas através de: seguir a vítima em seus trajetos, aparecer repentinamente em seu local de trabalho ou em sua casa, efetuar ligações telefônicas inconvenientes, deixar mensagens ou objetos pelos locais onde a vítima circula, e até mesmo invadir sua propriedade.
>
> (TRUZZI, 2019)

Alguns casos de cyberstalking entre famosos são o da atriz Thaís Melchior e Ana Hickmann:

> No último dia 4 de setembro, foi divulgada a notícia de que a atriz Thaís Melchior desativou seus perfis nas redes sociais após receber ameaças e xingamentos de fãs da novela que participará. Thaís não foi a primeira celebridade a se assustar com o assédio vindo da internet. Em caso muito mais emblemático, um fã da apresentadora Ana Hickmann, não satisfeito em monitorar e perseguir sua vida nas redes sociais, invadiu seu quarto de hotel e atirou contra ela, acertando sua assessora. O desfecho da tragédia se deu com a morte do fã obsessivo pelo cunhado da apresentadora.
>
> (BARBOSA, 2018)

Pessoas famosas acabam sendo um alvo muito frequente de casos de assédio e mensagens de ódio, no entanto, situações como estas citadas acima acometem inúmeras pessoas ao redor do mundo, sem a necessidade de serem pessoas públicas.

2.6.2 Como evitar o Cyberstalking?

Não há realmente uma garantia de não ser vítima de tal crime, pois não existe um ambiente virtual que seja totalmente seguro. Entretanto, há maneiras de se proteger adotando algumas precauções nas redes sociais, envolvendo manter um comportamento prevenido, assim, reduzindo os potenciais riscos.

> Evitar fazer checkin em locais públicos em tempo real;Evitar publicações pessoais abertas ao público; Não mencionar e-mails ou números de celulares pessoais nas redes sociais; Evitar publicar abertamente fotos dos filhos menores de idade; Tomar cuidado com as “curtidas” em publicações de terceiros, fanpages, locais e assuntos de seu interesse. Evitar confirmar presença em eventos públicos. Deixar sua lista de amigos oculta. Seu stalker poderá monitorar sua atividade na rede social, praticando engenharia social: verá quem são seus amigos, os locais que frequenta, os eventos que comparece, os assuntos que tem interesse, tendo acesso a uma gama infinita de informações gratuitas sobre você. Fazer uso das listas de privacidade disponibilizadas por algumas redes sociais (mas ter em mente que mesmo algum “amigo” da lista poderá tirar print de sua publicação e desvirtuar seu conteúdo); Não preencher totalmente as informações solicitadas pelos formulários das redes sociais, principalmente telefone; atentando-se ao cadastramento somente das informações obrigatórias para acesso à rede; Ter consciência de que a maioria das redes sociais sincronizam os seus perfis com os contatos cadastrados na agenda do seu celular. Ou seja: Facebook, Instagram e Whatsapp (por exemplo) cruzam seus perfis dessas plataformas entre si e sincronizam com os números de celulares cadastrados em seu telefone, sugerindo periodicamente seus perfis para que essas pessoas o adicionem, e vice-versa. Ter cautela com o que publica/compartilha nas rede sociais ou com o conteúdo que encaminha para terceiros. Qualquer material poderá ser manipulado ou distorcido, e servir como conteúdo para difamação ou extorsão, contra você mesmo ou contra terceiros, bem como gerar fake news, ou outros incidentes. As consequências dessas situações podem ser desastrosas, acabando com uma reputação profissional, com a imagem de uma marca ou instituição, ou deixando marcas indeléveis na vida de um indivíduo.
>
> (TRUZZI, 2019).

2.7 As Redes Sociais mais utilizadas

Há diversas plataformas sociais disponíveis na internet que abrangem diversas atividades de interações sociais e compartilhamento de multimídia como

fotos e vídeos entre amigos e familiares ou qualquer pessoa que faça parte da sua rede de amizades.

Algumas das redes sociais mais utilizadas são:

- **Instagram**

É uma rede social de compartilhamento de fotos e vídeos. No Brasil, o Instagram é a rede social mais popular e recentemente registrou a marca de 1 bilhão de usuários ativos.

- **WhatsApp e Messenger**

Não são consideradas redes sociais, pois são apenas aplicativos de comunicação, porém são muito utilizados no Brasil. Neles, os usuários podem trocar mensagens instantâneas, inclusive enviar fotos e vídeos.

- **Facebook**

Em 2018 o Facebook era a rede social mais popular no Brasil, mas agora está em segundo lugar. Entretanto continua sendo uma rede social muito utilizada. É utilizado por pessoas de diversas faixas etárias para manter contato com pessoas conhecidas ou fazer novas amizades, compartilhar conteúdos diversos como fotos e vídeos sobre variados assuntos como humor, esportes e reportagens.

- **Youtube**

O Youtube é uma plataforma de compartilhamento vídeos muito popular e conta com 1,9 bilhão de usuários ativos atualmente. Não é necessário uma conta para utilizar o Youtube, assim, podendo assistir aos vídeos da plataforma normalmente.

- **Linkedin**

Linkedin é uma rede social para negócios, voltada para profissionais e que também pode ser utilizada por empresas. É uma boa plataforma para quem está em busca de empregos.

- **Twitter**

É uma rede social de *microblogging*, ou seja, permite que os usuários façam breves atualizações de imagens ou texto e publicarem, para que sejam vistas tanto publicamente quanto para um pequeno grupo restrito.

2.8 Privacidade e Segurança

As redes sociais não garantem a segurança total da informação que foi carregada para um perfil, mesmo quando esses posts foram ajustados para serem privados (SOCIEDADE INTERNACIONAL, 2013).

É preciso ter muita atenção com as informações compartilhadas nas redes sociais e evitar fornecer ou publicar informações pessoais como nome, endereço, e-mail, CPF e números de telefone ou documentos. Outras informações que geralmente são publicadas em redes sociais são fotos e vídeos, idade e sexo, contatos, interesses e localização geográfica. Esses dados podem ser coletados por pessoas mal intencionadas, portanto, quanto menos informações sobre a rotina de vida for compartilhada, mais seguro será o uso das redes sociais.

Ao fazer um cadastro em uma rede social para criar um perfil, é apresentado um formulário para o usuário preencher suas informações. Muitas dessas informações são desnecessárias, como endereço, por exemplo, portanto, o ideal é preencher somente o essencial para o cadastro.

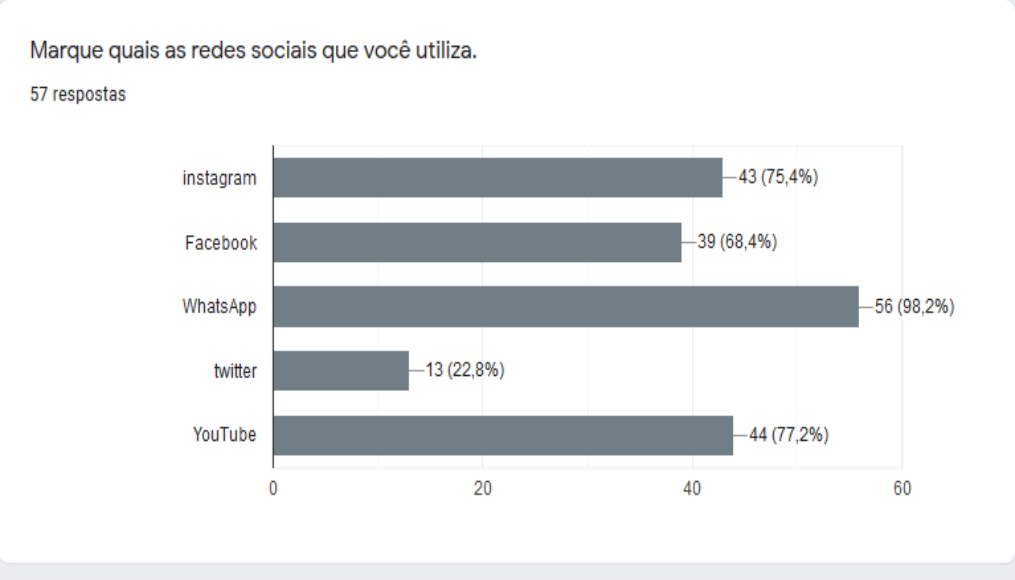
Contudo, o correto é verificar as informações de privacidade em seu perfil, não coloque informações como números de telefone e e-mail como informações públicas. Além disso, no Facebook, por exemplo, a página de seu perfil pode ser configurada de forma que somente seus amigos e pessoas que você aceitou em sua rede de amizades possam ver suas informações, dessa forma, pessoas desconhecidas não poderão ter muito acesso sobre você, nem sua lista de amigos. Outro ponto muito importante é ler os termos de privacidade e segurança antes de aceitar e criar um perfil, seja em rede social ou qualquer aplicativo.

2.9 Coleta e Análise de Dados

Através do Google Forms, plataforma que auxilia na criação de enquetes para pesquisas, foi realizado um questionário com perguntas relacionadas às Redes Sociais, para avaliar como e quais estão sendo utilizadas. O questionário foi divulgado pelo Whatsapp e Facebook e teve entre 57 a 77 respostas.

Baseado nos resultados da pesquisa, podemos ter uma base de como os usuários estão desfrutando das redes sociais.

Figura 1. Redes Sociais utilizadas pelas pessoas que responderam o questionário

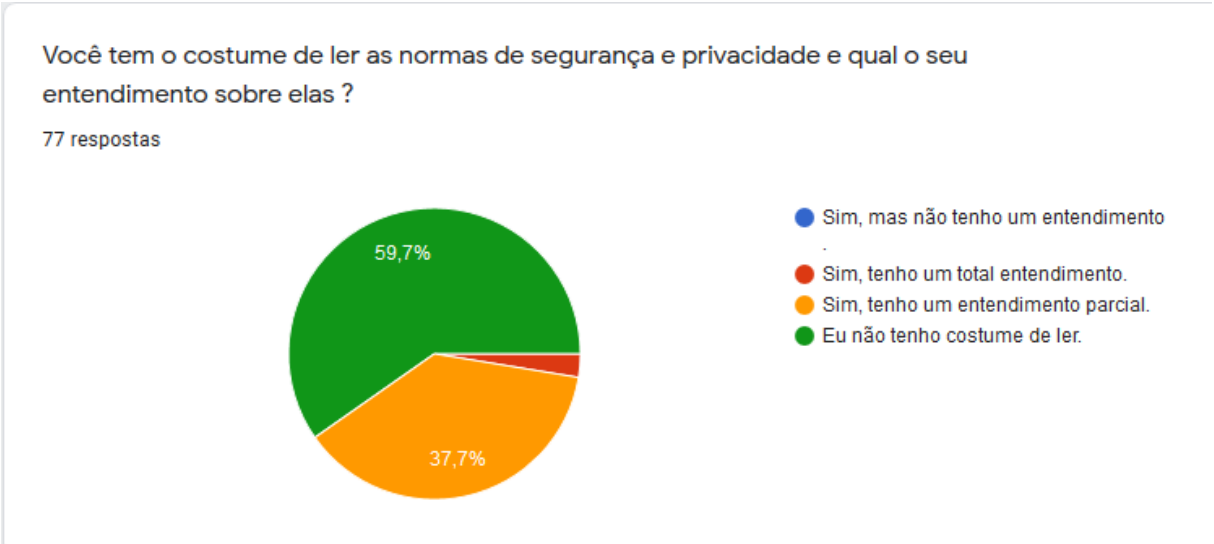


Fonte: (Pereira, Victória; Medeiros, Vinicius, 2020).

Na figura 1, percebe-se que o WhatsApp é mais utilizado como aplicativo de comunicação e rede sociais mais utilizada é o Instagram, com 43 das 57 respostas.

Na Figura 2, mostra quantas pessoas tem o costume de ler as normas de segurança e privacidade e seu conhecimento sobre elas.

Figura 2. Leitura e conhecimento das políticas de Privacidade e Segurança

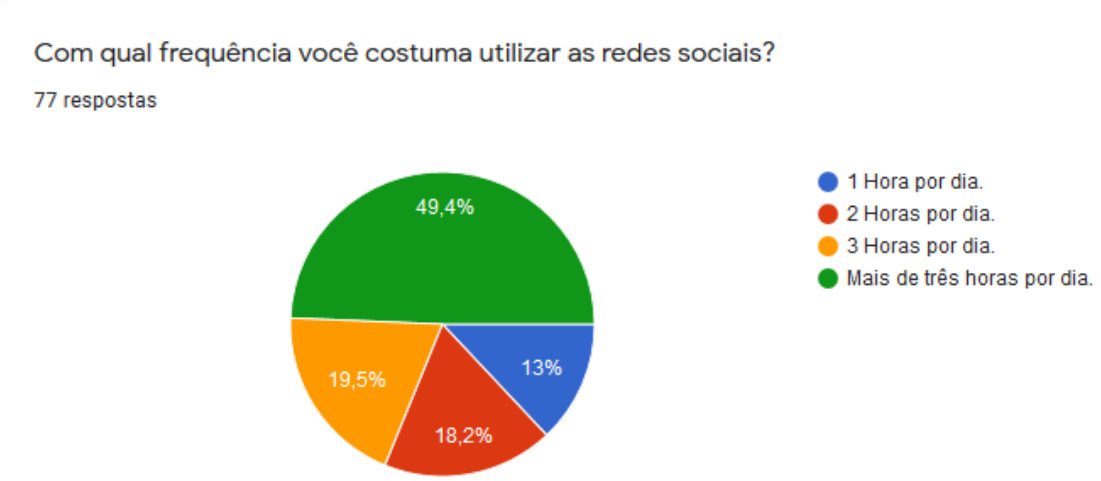


Fonte: (Pereira, Victória; Medeiros, Vinicius, 2020).

Aqui podemos ver que 59% das 77 pessoas não tem o costume de ler as Políticas de Privacidade e Segurança antes de aceitar os termos.

Na Figura 3 é apresentado o tempo que costumam passar nas redes sociais.

Figura 3. Quantidade horas gastas nas redes sociais

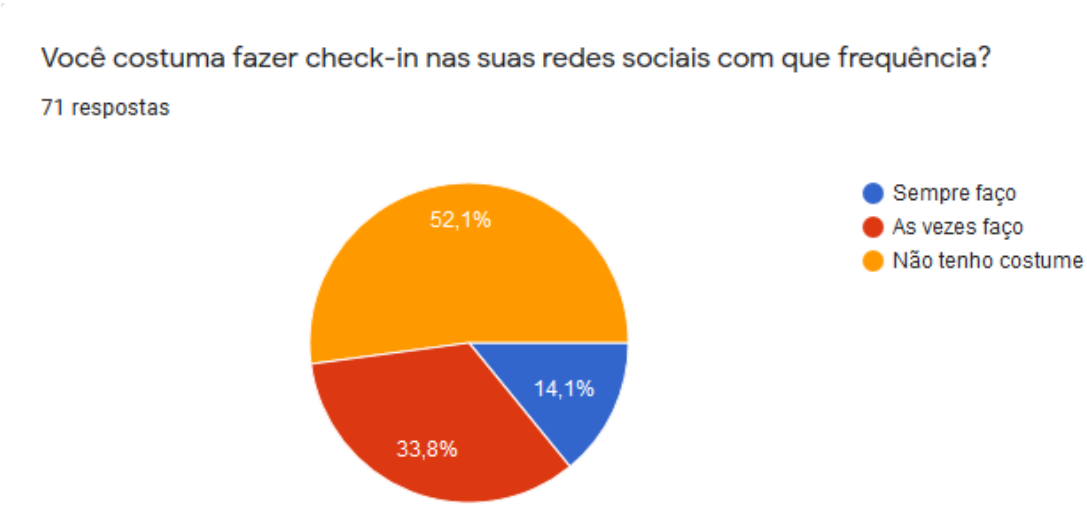


Fonte: (Pereira, Victória; Medeiros, Vinicius, 2020).

Cerca de metade das pessoas passam mais de 3 horas por dia nas redes sociais, enquanto apenas 13% ficam até 1 hora por dia.

A Figura 4 aborda a frequência e costume de as pessoas compartilharem sua localização publicamente.

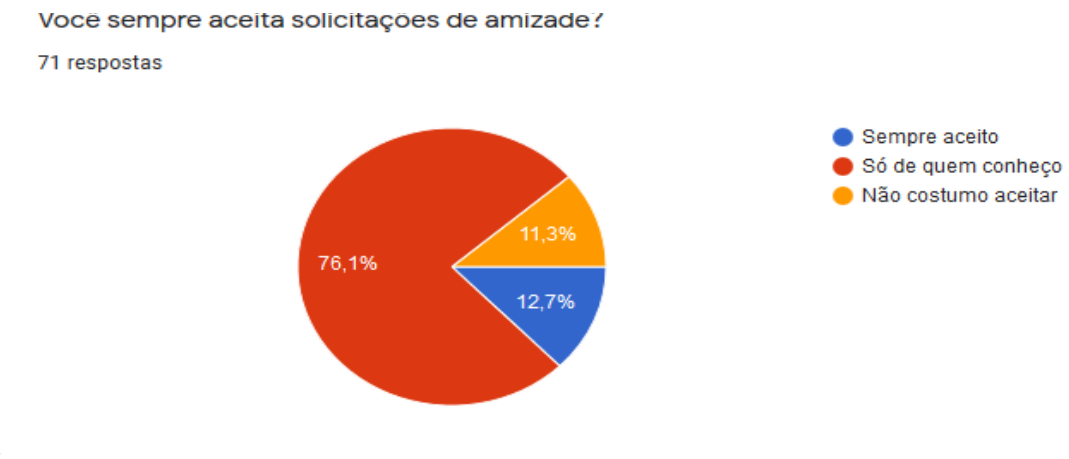
Figura 4. Compartilhamento de localização atual



Fonte: (Pereira, Victória; Medeiros, Vinicius, 2020)

Segundo os dados da Figura 4, a maioria não tem costume de compartilhar sua localização em tempo real, enquanto 14% divulgam sua localização sempre.

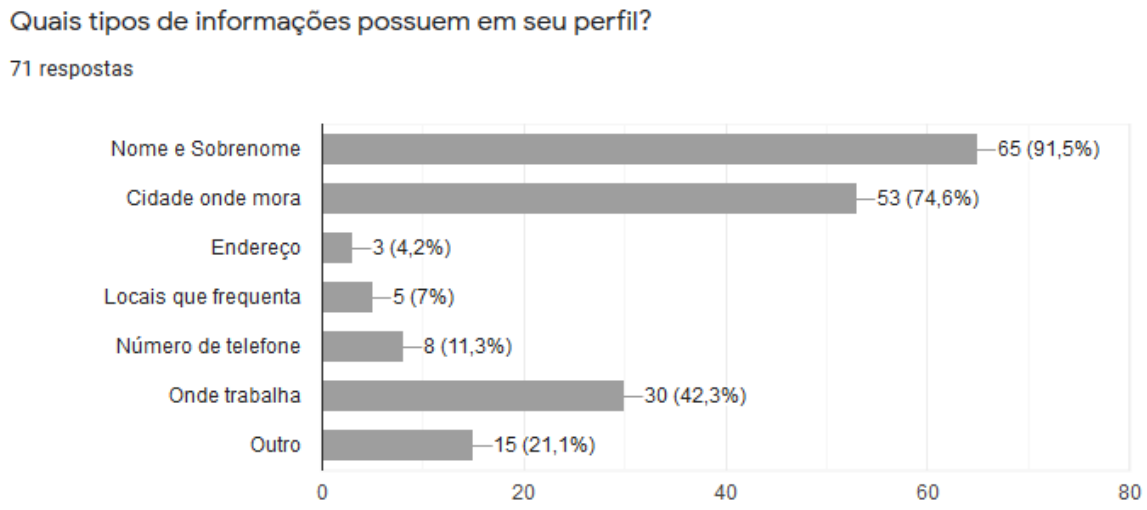
Figura 5. Solicitações de amizades recebidas



Fonte: (Pereira, Victória; Medeiros, Vinicius, 2020)

Analisando o gráfico, nota-se que a maioria só aceita solicitações de amizade de conhecidos, 12,7% sempre aceitam solicitações de qualquer pessoa e 11,3% não costumam aceitar nenhuma solicitação.

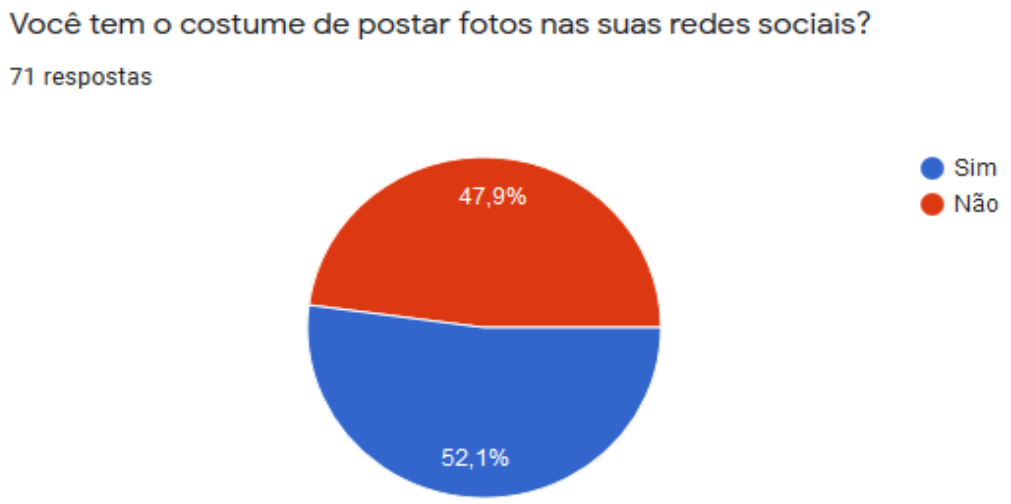
Figura 6. Perguntas sobre Informações contidas no perfil



Fonte: (Pereira, Victória; Medeiros, Vinicius, 2020)

Grande parte das pessoas publicam em seus perfis somente o necessário, como nome e sobrenome, cidade e local de trabalho, enquanto algumas, ainda poucas, compartilham endereço, locais frequentados e números de telefone.

Figura 7. Quantas pessoas compartilham suas fotos nas redes sociais



Fonte: (Pereira, Victória; Medeiros, Vinicius, 2020)

Analisando o gráfico, evidenciamos que um pouco mais da metade compartilham fotos suas em redes sociais, enquanto um número um pouco menor que esse não costuma publicar suas fotos.

3 METODOLOGIA

Pesquisa de tipo exploratória com abordagem qualitativa, baseada no método de análise de documentos.

Através da analise de jornais, artigos, revistas e periódicos acadêmicos em busca de compreensão e interpretação do material pesquisado, a fim de elaborar conclusões para o projeto, sem oportunidade de pesquisa de campo.

4 CONCLUSÃO

Concluímos que a Segurança da Informação assume um papel fundamental na segurança virtual, contudo, a conscientização os usuários através de informações detalhadas sobre cuidados e prevenções na internet também é uma peça chave para utilizar de modo racional e evitar crimes cibernéticos, pois a faixa etária de pessoas que utilizam frequentemente as redes sociais e a internet é muito ampla. Portanto, pessoas que não tem conhecimento sobre o assunto acabam sendo as vítimas mais cobiçadas por esses criminosos virtuais.

5 REFERÊNCIAS BIBLIOGRÁFICAS

BARBOSA, Gustavo Alves Parente. **Cyberstalking: da curiosidade ao crime**. 18 de set. 2018. Disponível em: <https://www.migalhas.com.br/depeso/287604/cyberstalking-da-curiosidade-ao-crime>.Acessado em: 16 mai. 2020.

CEIA, Joan Moraes de. **Crimes cibernéticos e segurança da informação**, 2018. Disponível em:< https://app.uff.br/riuff/handle/1/8998>. Acessado em: 10 mai. 2020.

CRUZ, Ana Laura. **Você sabe quais são as redes sociais mais utilizadas no Brasil em 2020?**, 2020. Disponível em:< https://www.maioresemelhores.com/redes-sociais-mais-utilizadas-brasil/>. Acessado em: 17 mai. 2020.

DICAS de como se proteger contra ataques cibernéticos. **Kaspersky**, c2020. Disponível em:<https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime>. Acessado em: 15 mai. 2020.

MARTELETO, Regina Maria. **Redes Sociais, Mediação e Apropriação de Informações: situando campos, objetos e conceitos na pesquisa em Ciência da Informação**, 2010. Disponível em:<https://www.arca.fiocruz.br/handle/icict/2247>. Acessado em: 19 abr. 2020.

QUATRO tipos de malware que você deve ficar atento. **Real Protect**, 2015. Disponível em:< https://realprotect.net/blog/4-tipos-de-malware-que-voce-deve-ficar-atento/>. Acessado em: 15 mai. 2020.

TUDO sobre malware. **Malwarebytes**, c2020. Disponível em:< https://br.malwarebytes.com/malware/>. Acessado em: 14 mai. 2020.

TRUZZI, Gisele. **Cyberstalking: aprenda os perigos e saiba como se proteger**, Isto é Dinheiro, 21 de fev. 2019. Disponível em: <https://www.istoedinheiro.com.br/cyberstalking-aprenda-os-perigos-e-saiba-como-se-proteger/>. Acessado em: 16 mai. 2020.

TECH ENTER. **Princípios Básicos da Segurança da Informação**, 2019. Disponível em: <https://techenter.com.br/principios-basicos-da-seguranca-da-informacao/>. Acessado em: 19 mai. 2020.

GAIDARGI, Juliana. **Segurança da Informação. O que faz? Para que serve?**. Infonova, 9 dez, 2018. Disponível em: <https://www.infonova.com.br/artigo/seguranca-da-informacao-o-que-faz-para-que-serve/>. Acessado em: 19 mai. 2020.

GONÇALVES, Pedro. **Segurança e privacidade nas redes sociais**. Sociedade Internacional, 9 mai, 2013. Disponível em: <https://www.sociedadeinternacional.com/seguranca-e-privacidade-nas-redes-sociais/>. Acessado em: 25 abr. 2020.

REDES sociais. **Resultados Digitais**, 2017. Disponível em: <https://resultadosdigitais.com.br/especiais/tudo-sobre-redes-sociais/#>. Acessado em: 25 abr. 2020.

HOLANDA, Isabel. **A influência das redes sociais na comunicação humana**. Fortes Tecnologia, 2020. Disponível em: <https://blog.fortestecnologia.com.br/a-influencia-das-redes-sociais/>. Acessado em: 26 abr. 2020.

JESUS, Aline. **História das redes sociais: do tímido ClassMates até o boom do Facebook**. Techtudo, 2014. Disponível em: <https://www.techtudo.com.br/artigos/noticia/2012/07/historia-das-redes-sociais.html>. Acessado em: 26 abr. 2020.

CRUZ, Diego; RODRIGUES, Juliana. **Crimes cibernéticos e a falsa sensação de impunidade**. 2018. 18f. Revista Científica Eletrônica do Curso de Direito, 13ª Edição. Disponível em: <http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf>. Acessado em: 15 mai. 2020.

SANTINO, Renato. Os perigos da exposição desenfreada nas redes sociais. Olha Digital, 9 fev. 2019. Disponível em: <https://olhardigital.com.br/video/os-perigos-da-exposicao-desenfreada-nas-redes-sociais/82625>. Acessado em: 15 abr. 2020.

DONEDA, Danilo. **Reflexões sobre proteção de dados pessoais nas redes sociais**. Universidad de los Andes. Facultad de Derecho (Bogotá, Colombia). Dez. 2012. Disponível em: <https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/10_Danilo-Doneda_FINAL.pdf.pdf >. Acessado em: 19 mai. 2020.

MORAIS NUNES, Alexandre. Comunicação através das redes sociais digitais. **Revista Alceu**, [S.l.], v. 20, n. 38, p. 129-141, jun. 2019. ISSN 2175-7402. Disponível em: <http://periodicos.puc-rio.br/index.php/revistaalceu/article/view/924>. Acesso em: 20 mai 2020.

AMARAL, Rogério Do. **Exposição privada nas redes sociais: uma análise sobre o Facebook na sociedade contemporânea**. 2016. 215f. Tese de Doutorado em Educação – Faculdade de Ciências e Tecnologia, Universidade Estadual Paulista, Presidente Prudente. Disponível em:<https://repositorio.unesp.br/bitstream/handle/11449/143853/amaral_r_dr_fct.pdf?sequence=3>. Acessado em: 20 mai. 2020.

ARANTES, Álisson Rabelo; DESLANDES, Maria Sônia. Os perigos dos crimes virtuais nas redes sociais. **Sinapse Múltipla**, v. 6, n. 2, p. 175-178, 2017. Acessado em: 20 mai. 2020.