A SEGURANÇA NA NAVEGAÇÃO DA INTERNET: UM ESTUDO SOBRE O COMPORTAMENTO DOS INTERNAUTAS NA GRANDE REDE

José Jeneci de Lima

RESUMO

A *internet* tornou-se uma ferramenta de extrema importância na vida de muitas pessoas, uma vez que, estamos vivendo na era da tecnologia, pois aquele que deseja está bem informado sempre está conectado a esse mundo sem fronteira. Porém, essa conexão, muitas vezes, é feita sem controle onde os indivíduos têm acesso a todos os tipos de informações. Partindo disso, esse trabalho tem como finalidade investigar se os estudantes possuem conhecimentos e condições de filtrar as informações encontradas, pois sabe-se que a *internet* também é uma janela aberta para aqueles que desejam praticar atos ilícitos tais como: roubos de senhas e até informações pessoais. Além disso, apresentamos nesse estudo as políticas de privacidades e prevenção contra os possíveis crimes virtuais, esclarecendo aos usuários as punições cabíveis a esses tipos infrações cometidas pelos internautas na grande rede.

Palavras-chave: *Internet*. Conexão. Segurança no acesso. Alunos.

ABSTRACT

The internet has become a tool of extreme importance in the lives of students, since, we are living in the age of technology, because the one who wishes is well informed is always connected to this borderless world, but this connection is often made without where they have access to all kinds of information. Therefore, this article aims to investigate if the students have knowledge and conditions to filter the information found, as we well know the internet is also an open window for those who wish to practice illegal acts such as stealing passwords and even personal information. Without this, we will work with this clientele on the policies of privacy and prevention against possible virtual crimes, clarifying the same of the punishments applicable to these types of infractions committed by the netizens in the great network.

Keywords: Technology. Connected. Cybercrime. Learners.

1 INTRODUÇÃO

Nos últimos anos, a informática está levando as informações praticamente a todos os pontos do planeta, pois esse fato está forçando as pessoas a utilizar o computador como ferramenta de trabalho ou até mesmo para se manter bem informado. Segundo Ramos:

> Se pensarmos a tecnologia como modificadora do meio onde vivem os homens, devemos pensar que tudo é tecnologia, desde uma pedra (Idade das pedras ou pré-história) usada para utensílios e armas, até os mais modernos computadores da idade contemporânea (RAMOS, 2012, p. 4).

Não podemos negar a importância da informática no nosso cotidiano, uma vez que a mesma trouxe grande avanços tecnológicos e mudou completamente a forma de realizar determinadas tarefas.

Mas diante da necessidade de usarmos o computador diariamente para nos auxiliar nas mais diversas tarefas, também cabe a preocupação em compartilhar informações no mundo virtual. Diante de tal preocupação, o estudo em questão está diretamente ligado aos internautas e seu comportamento na grande rede o que, consequentemente, gerou a seguinte indagação para esse estudo: será possível navegar na *internet* de forma segura, compartilhando informações e também usando as redes sociais sem perfis falsos?

Buscando respostas a tal indagação, na primeira etapa deste trabalho, procuramos enfatizar os vírus de computador, sua evolução e os tipos de vírus mais conhecidos, que atacam computadores do mundo inteiro causando grandes prejuízos e preocupações no mundo real e virtual.

Na segunda parte, expomos um pouco dos cuidados que devemos ter para evitar que um vírus chegue a infectar seu computador, e também o que é um antivírus.

Na última etapa, serão apontados os cuidados ao criarmos uma senha, quais os direitos e deveres do internauta na grande rede destacando, por fim, o foco principal do trabalho que seria a pesquisa realizada com os alunos do ensino médio da Escola Estadual Gilney de Souza, na cidade São Miguel, no estado do Rio Grande do Norte, visando conhecer a fundo a realidade dos discentes referente ao seu comportamento no mundo virtual.

2 A SEGURANÇA NO ACESSO À *INTERNET*

A *internet* a cada dia está mais próxima das pessoas seja através de celulares, *tablets*, *lan house* ou computadores residenciais conectados. Porém, essa aproximação, muitas vezes, tem causado grandes problemas no que diz respeito ao uso correto dessa ferramenta, pois sabemos que pessoas mal intencionadas tiram proveitos daqueles usuários inexperientes para obter informações pessoais. De acordo com Alves "a maioria dos incidentes envolvendo a segurança da informação está diretamente ligado ao fator humano, pois este está totalmente relacionado com a segurança da informação. A segurança da informação tem início e término nas pessoas" (ALVES, 2010, p. 111).

Segundo o especialista russo Eugene Kaspersky, fundador da Kaspersky Lab (empresa criadora do Antivírus Kaspersky), muitas ameaças virtuais se instalam em nossos computadores por falta de atenção e devidos cuidados que não foram tomados. O autor afirma que:

> O progresso tecnológico caminha, inevitavelmente, para que tenhamos cada vez menos privacidade. Isso porque usamos cartões bancários, celulares e redes sociais. Mas é possível estar bem protegido contra os ataques cibernéticos e manter dados pessoais relativamente seguros. É uma questão de gerenciar senhas e ter um software atualizado–incluindo um suíte de segurança. Mas, em geral, não temos boas perspectivas de manter a privacidade no mundo interconectado de hoje. E essas perspectivas serão ainda piores em um futuro cada vez mais interconectado" (KASPERSKY, 2017).

Sabemos que as tecnologias de comunicação e informação se fazem presentes em nosso cotidiano e compartilhamos diariamente uma grande quantidade de dados, sendo que para mantê-los seguros o custo é bastante elevado. Assim afirma Novo que "nas residências, os computadores estão repletos de documentos, planilhas, correspondências eletrônicas, fotografias, vídeos, declarações de Imposto de Renda e até mesmo listas de amigos" (NOVO, 2010, p. 25).

Diante de tantas instabilidades provocadas pelos avanços tecnológicos, nossas redes de computadores passam por um procedimento de constantes reajustes e idealização de novas barreiras para evitar ataques de *hackers*. Para Ferreira:

> Melhorar um sistema de segurança da informação não está baseado apenas em aplicar em um conjunto de computadores antivírus ou barreiras de proteção (firewalls) interligada na rede de computadores de uma organização. Para se obter um sistema de segurança da informação é necessário entender os princípios de segurança para que possa se gerir políticas e soluções cabíveis para atender as necessidades de cada organização (FERREIRA, 2013, p.15).

Se os vírus biológicos têm a função de destruir nosso sistema de defesa e favorecer a entrada de doenças oportunas, os vírus de computadores são apenas pequenos programas

criados para destruir, modificar ou simplesmente roubar informações pessoais que estejam salvas no HD (Disco Rígido) de seu computador sendo que, a finalidade de um vírus de computador pode variar de uma simples brincadeira, visando apagar os arquivos causando no usuário uma grande preocupação com a perca de informações que estava armazenada no seu PC (Computador Pessoal) ou até mesmo para cometer alguns crimes cibernéticos do tipo roubar senhas de contas bancários ou divulgar informações sigilosas daquele usuário que teve o seu computador infectado.

Os vírus chegam a até seu computador através de *pen drive*, cd, dvd, cartões de memória, via *bluetooth* e por meio da *internet* e estes são ativados quando o usuário executa certos programas que apresentam a extensão.exe, ou seja, programas do tipo executáveis ou simplesmente clicando em um *link* de *internet* que contém o vírus disfarçado. As dicas dadas pelos especialistas em segurança de sistema são de suma relevância, dentre elas: analisar todos os *sites* em que você acessa conferindo se eles apresentam os itens de segurança para uma navegação segura e, ainda, verificar se na barra de endereço o *site* apresenta um "s" ou a figura de um cadeado. Veja o que diz Levine:

> Mesmo que ninguém roube seu dinheiro as pessoas podem obter informações sobre suas atividades online, o que resulta em uma perda real de privacidade. E algumas pessoas estão tentando controlar sua empresa, de forma que possam usar isso para propósitos perversos. Quando um novo computador é conectado à internet, não é uma questão de se ficará sob ataque cibernético, mas de quando. E não em meses ou dias – mas em horas ou minutos (LEVINE, 2013, p. 15.)

Portanto, os internautas devem estar sempre atentos, uma vez que, a cada dia novos vírus são criados e jogados na grande rede para os mais diversos fins.

2.1 A evolução dos vírus de computador e os tipos de vírus mais conhecidos

Por volta de 1983 o pesquisador e doutor em engenharia elétrica, Fred Gohen, fez algumas análises em códigos maliciosos, batizando estes como "vírus de computador".

No ano de 1987 apareceu o **Brain**, sendo o primeiro vírus de computador a qual se tem notícia. O mesmo era capaz de infectar o *boot* de disquete que tinha capacidade de armazenamento de apenas 360 Kb e passar despercebido pelo o sistema. Neste mesmo ano também foi lançado o **Stoned,** vírus que infectava o *boot* do disco rígido e danificava o MBR, fazendo com que o sistema operacional não inicializasse.

Já em 1988 é criado o primeiro antivírus, por um programador da Indonésia. Este programa detectava o **Brain**, que eliminava o mesmo e protegia o computador de novos

ataques. Em dois de novembro deste mesmo ano, o estudante Robert Tappan Morris da Cornell University lançou na rede de computador um programa malicioso chamado de **Internet Worm** contaminando cerca de 6.000 computadores. Este programa pegava as informações dos usuários e distribuía para outras máquinas.

Em 1989, surgiu o **Dark Avenger**, vírus este que tinha o poder de contaminar rapidamente, sendo que os danos que ele causava eram percebidos lentamente. Para tentar eliminar esse tipo de vírus e os demais que circulavam no mundo da informática, nesta mesma época a IBM lançou o seu primeiro antivírus comercial e faz um investimento em pesquisas contra códigos maliciosos.

No dia 6 de março de 1992 é disseminado um vírus chamado **Michelangelo.** O mesmo ficou conhecido por ter sido espalhado na grande rede de computadores no mesmo dia em que o artista da Renascença faria aniversário. Logo, o mesmo causou uma grande especulação, uma vez que, ele gravava pastas e arquivos na unidade de disco rígido sem a permissão do usuário.

O primeiro rastreamento de um vírus foi feito no ano de 1994, o fato aconteceu na Inglaterra, o mesmo de o nome de **Pathogen**, é rastreado pela Scotland Yard (sede central ou quartel general da polícia Metropolitana de Londres) e seu criador foi condenado a 18 meses de prisão.

Já o primeiro vírus de macro foi criado em 1995 e tinha o nome de **Concept**, esse código malicioso foi desenvolvido usando a linguagem *Word Basic* da *Microsoft*, sendo que, poderia ser executado em qualquer máquina que tivesse nela instalado o *Word* ou *Macintosh*.

O vírus **Chernobyl** infectou em 1999, vários computadores nos Estados Unidos, o mesmo deixava os usuários impossibilitados de acessarem o HD e também seus dados. Países como Turquia e Coréia do Sul tiveram grandes prejuízos e na China os danos causados foram estimados em aproximadamente US$ 291 milhões.

No ano de 2000 foi a vez do vírus **Love Letter**, que se propagou pelas Filipinas e chegou a “varrer” os Estados Unidos e Europa em apenas seis horas. Estima-se que este vírus atingiu cerda de 2,5 a 3 milhões de computadores e provocou danos para mais de US$ 8,7 bilhões.

Em 2001, surgiu o **Worm**, tipo de código malicioso que se multiplicava nas páginas da *internet* e também nos *e-mails*. Neste mesmo ano é feito a descoberta de alguns programas de criação de vírus, cito: o **VBS Worm Generator**, programa esse que foi desenvolvido por

um argentino que tinha apenas 18 anos.

O fato que chamou atenção no ano de 2006 foi justamente o bloqueio a *sites* e máquinas e a captura de informações de usuários e empresas. Neste ano, as fraudes virtuais custaram para o Brasil cerca de 300 milhões de reais como estima os dados do IPDI (Instituto de Peritos em Tecnologias Digitais e Telecomunicações).

O ano de 2007 foi marcado por ter sido o ano que os vírus atingiram as redes sociais como *Orkut*. Esses vírus tinham a finalidade de enviar recados (*Scraps*) para todos os usuários como se fosse um dos seus amigos que estavam compartilhando uma mensagem e após clicar sobre esse recado seu computador já estaria infectado. Portanto, bastaria você digitar a senha da sua conta bancária que a mesma seria capturada ou até mesmo os cliques que eram executados na página do seu banco seriam todos enviados para o computador que havia distribuído o vírus.

O **Conficher ou Downadup** infectou milhões de computador em 2008 sendo que o mesmo estaria programado para entrar em atividade em 1º de abril de 2009, mas esse ataque foi superado por antivírus mais atualizados.

Os vírus do tipo multiplataforma atacaram no ano de 2012. Esses vírus eram capazes de infectar os computadores com os sistemas operacionais *Windows*, *Linux* e *Mac*. Os tais códigos maliciosos foram desenvolvidos utilizando a linguagem de programação em Java. Em 2013 um vírus criado no Brasil e distribuído por *e-mail*, ao qual este solicitava a atualização do *Adobe Flash Player*. Logo, um aplicativo era instalado PC e deixava o mesmo à disposição da rede **Bitcoin,** assim que fosse ligado e conectado à *internet*.

No ano de 2014 os cientistas de Liverpool, no Reino Unido, criaram um tipo de vírus de computador capaz de se espalhar pelo ar, por redes *wi-fi*, como uma gripe comum. Porém, a atenção deles era voltada para criar programas que reconhecessem quando seu computador está sobre um ataque virtual.

O **Thunderstrike 2**, criado em 2015, foi o primeiro vírus capaz de destruir computadores de empresas de grande porte como a Apple. O vírus foi instalado sem *internet*, através de redes sem fios, *e-mails* falsos e até mesmo por acessórios.

O vírus ransomware **Locky**, foi considerado o vírus mais potente de 2016. Seus idealizadores eram fãs de mitologia nórdica, pois usavam nomes dos maiores deuses Nórdicos para novas versões do **Locky** como, por exemplo: Odin, Thor, Aesi, etc. Sua contaminação se

dava através de *e-mail*, onde o usuário recebia um documento anexado do *Microsoft Word* em uma suposta fatura que exigia pagamento, sendo que na verdade eram macros mal-intencionadas.

Em 12 de maio de 2017, o vírus **Wana Crypt0r 2.0**, atingiu cerca de 74 países, através de um ataque de *hacker* do tipo ransomware, bloqueando todos os arquivos do computador e apenas liberando os mesmos só depois do pagamento do resgate. Esse tipo de vírus fica muito bem camuflado nos documentos de Word e PDFs e são espalhados via compartilhamento de arquivo.

Os vírus vão sendo criados e jogados na grande rede de computadores e, neste momento, poderíamos fazer uma lista enorme desses códigos maliciosos, mas iremos relacionar apenas aqueles de maiores repercussões no mundo cibernético.

Um dos primeiros códigos maliciosos criados para computador foi o vírus de **Boot**. O mesmo se instala no setor de inicialização do disco rígido da máquina e impedem que esse PC seja ligado ou se ele já estiver em funcionamento o vírus, muitas vezes, fará este computador reinicializar automaticamente sem a permissão do usuário.

O ***Keyloggers*** são *malwares* criados com a intenção de monitorar tudo que é digitado no teclado pelo usuário, logo o mesmo tem a função de capturar senhas e outros dados pessoais.

Worms também são *malwares* que aproveita a rede para transmitir esse tipo de vírus para outros computadores, a sua propagação se dá de forma muito rápida, uma vez que, os mesmos chegam até os computadores das vítimas através de anexos de *e-mails*.

Spywares são códigos maliciosos que se comporta como um espião, após seu alojamento no computador ele tem o poder de concentrar informações sobre os hábitos de navegação do usuário e essas informações são enviadas aos criadores dos vírus quando o usuário conectar seu PC a *internet*.

Trojans, o popular “cavalo de tróia”, são *malwares* maliciosos enviados como se fossem um arquivo normal, mas logo que é executado realiza atividades ocultas no sistema, sendo que boa parte destes vírus oferecem controle total do seu computador, permitindo ao visitante criar ou até mesmo apagar arquivos e pastas.

Os ***Rootkits*** são cavalos de tróia bem mais avançados e que procuram se disfarçar no sistema. Esses vírus foram criados usando sofisticadas técnicas de programação e seus

estragos que podem causar no seu computador, sendo que um deles é esconder suas entradas no registro e também ocultar os processos no gerenciador de tarefas.

Os ***Adwares*** são um tipo de malwares que enchem o seu PC com anúncios e propagandas, porém sem a autorização do usuário, eles aparecem no formato de pequenas janelas (pop-up), sendo que os mesmos deixam a máquina mais lenta. O que se sabem é que as indústrias faturam milhões com esse tipo de propagandas. Um dos *sites* que mais exibe esse tipo de propaganda é o *Facebook*. Os usuários desta rede social se queixam, constantemente, da quantidade de janelas que são exibidas, principalmente quando os internautas estão usando os aplicativos de jogos virtuais.

Existe também o ***Time Bomb***, vírus conhecido como "bomba-relógio". Eles receberam esse nome por ser programados para entra em ação em determinados ocasiões, os mais populares são Michelangelo, Eros, 1º de abril e Sexta-Feira 13. Vírus desse tipo pode está no seu computador, mas só se manifesta na data programada pelo o seu criador.

Os ***Hijackers*** também conhecidos como *spyware*, são programas que alteram a página inicial de alguns navegadores de *internet* e, muitas vezes, instalam barras de ferramentas sem a sua permissão, mostrando *pop-ups* constantemente.

2.2 Cuidados que devemos ter para evitar que um vírus chegue a infectar nossos computadores

Devemos ter o máximo de cuidado na hora de fazermos um *download*, ou seja, no momento de baixar arquivos da *internet*, pois muitos *sites* não são confiáveis e não oferecem qualquer segurança para o seu conteúdo. Sendo assim, sempre que baixar um arquivo procure executar o antivírus neste arquivo para fazer uma varredura em busca de vírus.

Pen drives e cartões de memória podem trazer vírus para o meu computador e para que isso venha acontecer basta que você use esse dispositivo de armazenamento em um PC que esteja infectado por um vírus. Logo, no momento em que você usar tais periféricos no seu computador, os vírus em que estava naquela máquina passarão a existir também na sua, caso seu antivírus não o tenha detectado.

Os *e-mails* recebidos com anexos e *links* de pessoas desconhecidas devem ser analisados, lembre-se que não devemos hospedar estranhos em nossa casa, pois essa dica também é válida para o mundo virtual. Para evitar situações desagradáveis, é preciso excluir

esse tipo de *e-mails* antes mesmo de executar os arquivos em anexos ou clicar sobre os *links* inseridos neles.

Manter sempre o seu sistema operacional atualizado é outra dica importante, uma vez que, o mesmo tem suas falhas, que são chamadas de bugs e essas vulnerabilidades são descobertas por usuários mal-intencionados que navegam na grande rede e tiram proveitos dessas falhas para disseminar seus códigos maliciosos.

Para os *peoplewares* (usuários de computador) que utilizam uma grande quantidade de arquivos executáveis do tipo arquivo.EXE é fundamental fazer uso de uma máquina virtual para ler esses aplicativos, pois se a mesma for contaminada por alguns vírus, basta que você o formate, e assim o problema estará resolvido.

2.3 O que é um antivírus de computador?

Um antivírus é um conjunto de aplicativos que procura proteger o seu computador contra possíveis infecções por vírus e outras ameaças de *malwares*. Se você o utilizar corretamente, e em combinação com outros programas, como utilitários de backup de dados, ele reduzirá significativamente o risco de o seu computador ser atacado ou infectado por um vírus.

Algo que não pode faltar em um bom antivírus é a opção de varreduras rápidas e completas, também vale salientar que, o mesmo deve oferece as alternativas de escaneamento, o que nos dá à possibilidade de escolher entre os discos do computador, as pastas, os arquivos e os periféricos de entrada e saída de dados cito: *Pen drives*, cartões de memória e cds ou dvds regraváveis, qual deles o usuário deseja executar a varredura. Outro fator importante é o possível agendamento, onde o usuário pode escolher as datas para uma análise completa do seu equipamento em busca de novas ameaças.

Segundo o especialista russo Eugene Kaspersky, fundador da Kaspersky Lab (empresa criadora do Antivírus Kaspersky), muitas ameaças virtuais se instalam em nossos computadores por falta de atenção o pelo os devidos cuidados que não foram tomados. Sobre isso, o mesmo afirma que:

> Para começar, não navego em um dispositivo, seja computador, tablet ou smartphone, sem um software de segurança instalado. Não clico em qualquer link que recebo, não confio em qualquer um na internet, mesmo que jure que é meu amigo, não faço transações bancárias a partir do meu smarphone ou quando não tenho conexão segura. Também não uso programas de envio de arquivos digitais, não instalo arquivos que chegam por e-mail ou Facebook, não deixo para depois atualizações solicitadas por programas instalados nas minhas máquinas e mantenho ao menos dois back-ups, HDs com minhas informações mais relevantes e

> fotografias. (KASPERSKY, 2012.)

2.4 Os cuidados ao criarmos uma senha

Password ou senha, em qualquer que seja o sistema de computação é o que credencia o usuário como sendo ele mesmo e possibilitando este indivíduo a ter acesso aos dados disponíveis naquele sistema, sendo também responsável pela a sua conduta na grande rede de computadores. Portanto, mesmo que alguém venha a usar a sua a sua senha, com o seu conhecimento ou não, você é quem tem a responsabilidade de ter acesso às informações e como vai utilizá-la. Sendo assim toda atenção deve ser dada as senhas para não chegue até as mãos de pessoas mal intencionas.

Na hora de criar sua identificação procure fazer a mesma não tão simples de ser descoberta pelos invasores de computadores. Evite nomes de pessoas, data de nascimento e datas que marcaram a histórias ao longo desses anos. Uma senha será boa ou forte aquele que tem no mínimo oito caracteres e entre eles existam letras maiúsculas e minúsculas, números e símbolos. Vejamos a dica dada por Abreu:

> Quanto mais elaborada for a senha, mais segura, e portanto mais difícil de ser descoberta. Assim, ao elaborar uma senha, é recomendável misturar letras maiúsculas, minúsculas, números e sinais de pontuação. Uma regra realmente prática e que gera boas senhas é selecionar uma frase randomicamente e utilizar dela, a primeira, segunda ou última letra de cada palavra. Por exemplo, no uso da frase "batatinha quando nasce se esparrama pelo chão" podemos gerar a senha "!BqnsepC" (o sinal de exclamação foi acrescentado no início para se obter um símbolo na senha). (ABREU, 2011, p. 18)

Como forma de garantir uma navegação segura na *internet*, alguns *sites* disponibilizam uma opção para que na hora em que você for criar uma conta, escolha quanto tempo deverá ser válida aquela senha. Esse tempo mínimo pode ser de apenas 72 horas e, caso venha a marcar essa alternativa, sempre que decorrer esse tempo você será obrigando a criar uma nova senha para poder ter acesso aquele *site*. Portanto, situações como essas evitam, muitas vezes, que sua identificação seja descoberta por invasores do ciberespaço.

2.5 Direitos e deveres do internauta na grande rede

Durante muito tempo no Brasil para inibir os crimes cibernéticos, era necessário mover uma ação penal ou punir os infratores dentro dos artigos do Código Civil, levando os mesmo a serem responsáveis por danos morais ou materiais.

A referência na história do Brasil para os crimes virtuais foi a lei 12.737/2012. A mesma é conhecida como "Lei Carolina Dieckmann", que entrou em vigor no dia 03 de abril

de 2013. Ela tem seu nome em virtude de, na época, o computador da atriz ter sido invadido por *hackers* que publicaram algumas fotos íntimas contidas no mesmo. Por causa desse delito, o senado sancionou esta lei para inibir esses tipos de crimes. Em sua legislação está determinado que: aquele que interromper provedores ou derrubar *sites* fica sujeito a pena de um a três anos, de acordo com o artigo 266. Ainda vale salientar a referência que a mesma faz ao artigo 154-A no Código Penal, que prevê a detenção de três meses a um ano aos agentes causadores de invasões em equipamento de informáticos. Portanto, está determinado lei, que aqueles que invadirem computadores e enviar-lhes códigos maliciosos do tipo: cavalos de tróia ou acionarem webcams mesmo que seja de forma remota podem ser enquadrados.

Mas em 2016, o governo regulamentou a lei que disciplina o uso da *internet* no Brasil, que logo ficou conhecida como o Marco Civil da Internet ou Lei nº 12.965, que tem como objetivo estabelecer princípios, garantias, direitos e deveres para os usuários de *internet*. Vejamos o que diz o Art. 21:

> O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a disponibilização desse conteúdo (BRASIL, 2014).

Também convém lembrar que a referida lei estabelece que os internautas têm o pleno direito de não ter o sigilo de suas comunicações feitas pela a *internet* revelado, salvo o caso, em que um mandado jurídico for expedido no intuito de esclarecer uma investigação criminal. É suma relevância ressaltar que os internautas também têm seus deveres a cumprirem, quando estão navegando na rede mundial de computadores e entre todos os seus deveres esses são imprescindíveis para uma navegação prudente e segura. Vejamos os mesmos:

- ✓ Jamais violar a privacidade de outros internautas ou usuários**;**
- ✓ Em hipótese alguma enviar ou transmitir qualquer tipo de dados que seja de domínio de terceiros, sem a devida permissão;
- ✓ Nunca alterar, apagar dados e informações de terceiros;
- ✓ De forma alguma enviar ou transmitir arquivos com vírus de computador, com conteúdo destrutivo e invasivo;
- ✓ Usar os devidos cuidados com os dados de sua identificação individual sempre que navegar na *internet*, utilizando e informando apenas quando for necessário;
- ✓ Não utilizar IP de maquinas zumbis de rede ou de correio eletrônico falsos;
- ✓ Guardar sigilo absoluto sobre a sua identificação de usuário tais como nome e senha;

- ✓ Sempre fornecer informações verdadeiras e de sua titularidade ao se cadastrar em algum site;
- ✓ Jamais transgredir o direito autoral de terceiros, por meio de qualquer tipo de cópia de material, sem a autorização do verdadeiro proprietário**;**
- ✓ É dever do usuário configurar seu sistema de informática de forma a protegê-lo de invasões que resultem em disseminação de vírus;
- ✓ Nunca enviar ou comunicar quaisquer tipos de informações que induzam, estimulem ou brotem atitudes discriminatórias, recados violentos ou delituosos que atentem contra a moral e bons costumes da ordem pública;

Portanto, é perceptivo que se o internauta se portasse de tal forma, os crimes ditos virtuais não teriam tanta repercussão e gravidade, mas vale a pena salientar ao usuário que ele é responsável por qualquer tipo de informação ou afirmação originadas com seu nome de usuário e senha.

3 METODOLOGIA

Para atingir os objetivos propostos realizamos, inicialmente, uma pesquisa bibliográfica na área de conhecimento elencado. Estudiosos como Vergara (1990) afirma que "uma pesquisa bibliográfica pode ser vista como sendo, estudo sistematizado desenvolvido a partir de material publicado em livros, revistas jornais, isto é material acessível ao público em geral". Quanto ao tipo de abordagem o referido estudo se caracteriza como uma pesquisa qualitativa e quantitativa[1] ao mesmo tempo, uma vez que, uma pesquisa quali-quantitativa nos fornece um cruzamento de informações gerando assim uma maior confiabilidade dos dados catalogados.

Uma discussão de grande valia no meio acadêmico atual é a questão das medidas de segurança envolvendo as novas tecnologias da comunicação. Mesmo com tantos recursos de proteção aplicados aos sistemas computacionais não temos garantia de estarmos 100% seguros na grande rede. Sobre isso, Serrano afirma que:

> Essas ameaças do mundo da informação eletrônica, são frutos de mentes doentias que se privilegiam de conhecimentos em linguagens de programação, e a partir delas, criam códigos que fazem de nossos vulneráveis computadores, verdadeiros bonecos de marionetes (SERRANO,2001, p. 2).

Então podemos dizer que, ao navegarmos na *internet* estamos sempre sobre um

[1] Pesquisa que envolve métodos quantitativos e qualitativos, de modo a obter uma compreensão e explicação mais ampla do tema estudado.

campo minado que todo movimento deve ser feito com muita atenção e nunca esquecermos de manter nossos computadores com *softwares* defensores atualizados para minimizar a zona de risco. Assim nos fala Fernandes:

> Zonas de ricos correspondem às partes vulneráveis do sistema e todas as redes possuem algumas. No caso de uma, rede conectada à Internet sem qualquer Firewall, ela como um todo está sujeita a ataques. Isto não implica que ela seja vulnerável, mas num caso como este, em que toda a rede pode ser alcançada por uma rede não confiável, toma-se necessário garantir a segurança de todos os *hosts* presentes na mesma. No caso da utilização de um Firewall a zona de risco é normalmente reduzida ao próprio Firewall ou ao subconjunto dos *hosts* da rede, diminuindo as preocupações dos administradores no que diz respeito a ataques diretos. O uso do Firewall representa a redução da zona de risco a um único ponto de falha, no entanto, se este for violado está novamente, se expande, passando agora a incluir toda a rede protegida (FERNANDES, 2000, p.90).

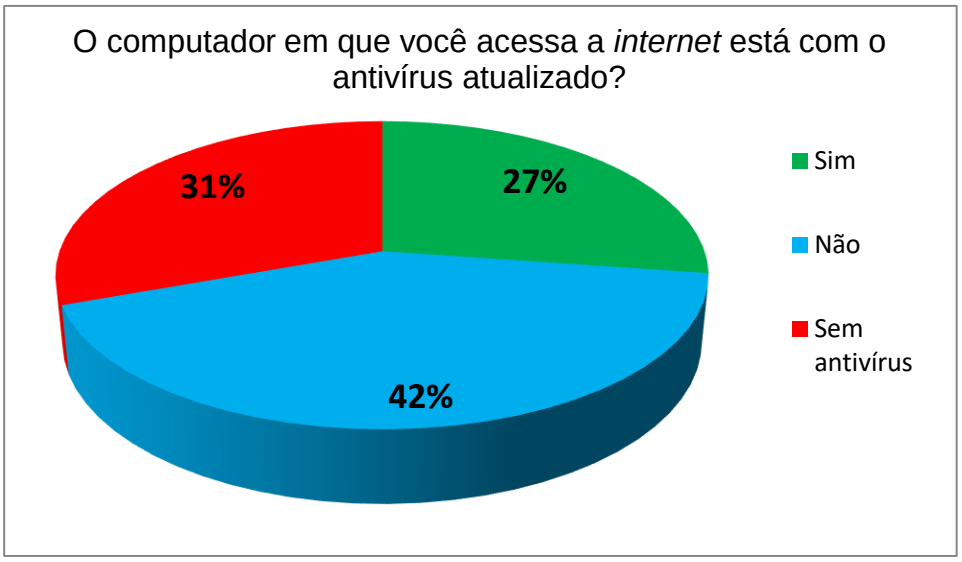
Nesse sentido, esse artigo tem como finalidade discutir a importância do uso seguro da *internet*, utilizando as ideias dos autores citados como base teórica. Realizamos, de antemão, a pesquisa bibliográfica em base de dados universitários, tais como: *google* acadêmico, CAPES, revistas científicas como a *Scielo*.

Após a revisão bibliográfica, desenvolvemos uma pesquisa na Escola Estadual Gilney de Souza, localizada na cidade de São Miguel, no estado do Rio Grande do Norte, com alunos do Ensino Médio dos turnos matutino e vespertino, tendo como instrumento de coleta de dados um questionário de perguntas fechadas, visando a obtenção de respostas mais precisas sobre a segurança na *internet* e, ainda com o intuito de analisar comportamento desses discentes na grande rede.

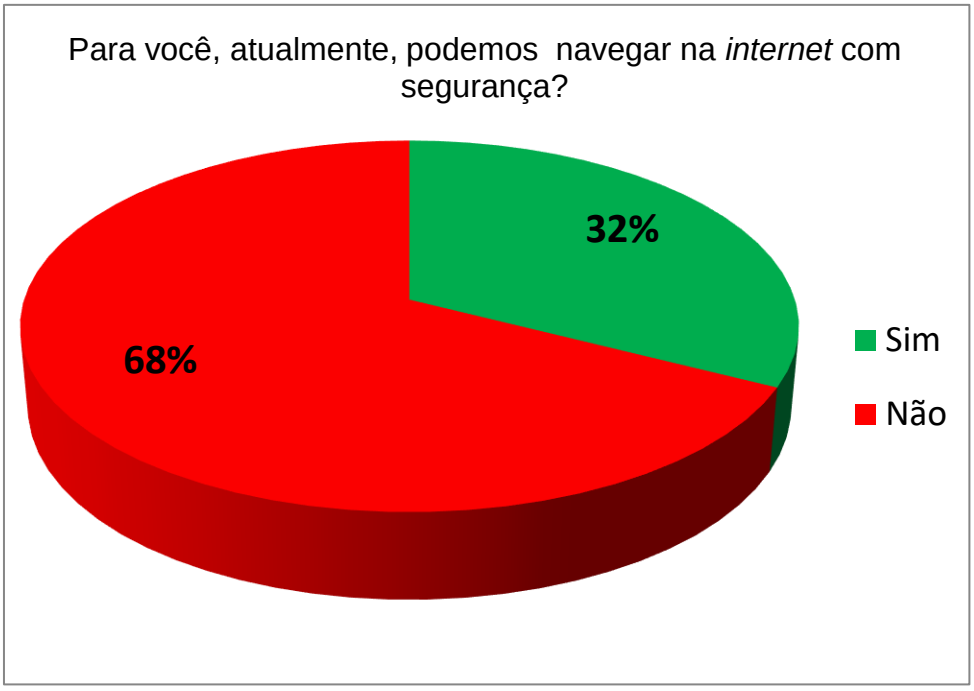
4 ANÁLISE DOS DADOS

Foi aplicado um questionário fechado com nove questões para os alunos, com intuito de identificar o nível de conhecimento desse público com relação à segurança na *internet* e também avaliar seu comportamento quando está acessando a rede mundial de computadores. Segundo Gil (1999, p.128), pode ser definido como questionário “a técnica de investigação composta por um número mais ou menos elevado de questões apresentadas por escrito às pessoas, tendo por objetivo o conhecimento de opiniões, crenças, sentimentos, interesses, expectativas, situações vivenciadas etc.”

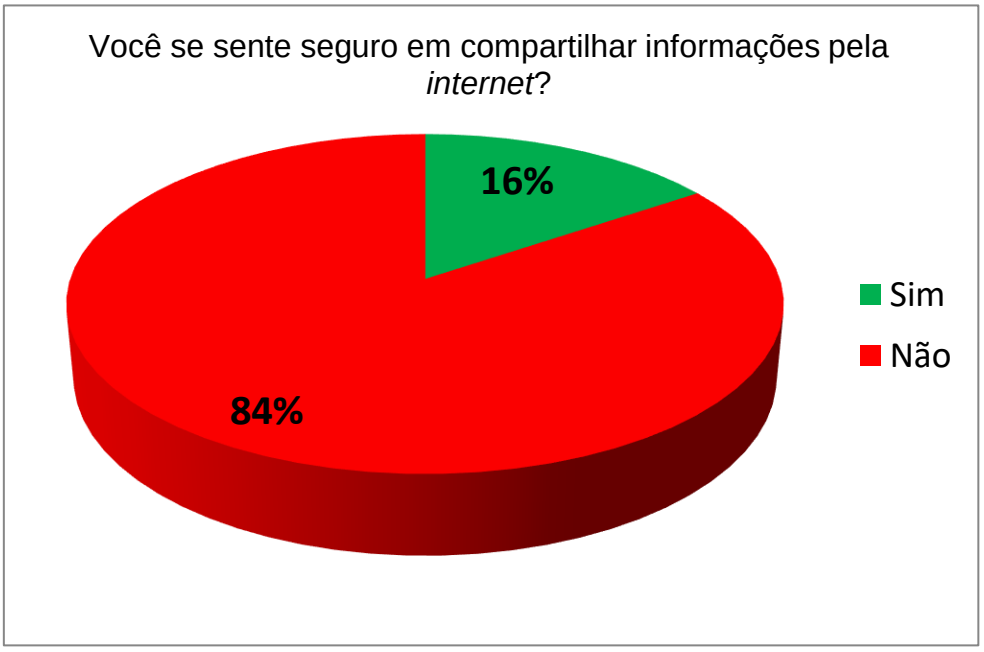
Esta pesquisa foi realizada no dia 01 de novembro de 2017, com 184 estudantes do ensino médio, dos turnos matutino e vespertino. Com isso, obtivemos os seguintes resultados conforme as perguntas e respectivas respostas que originaram os gráficos abaixo:



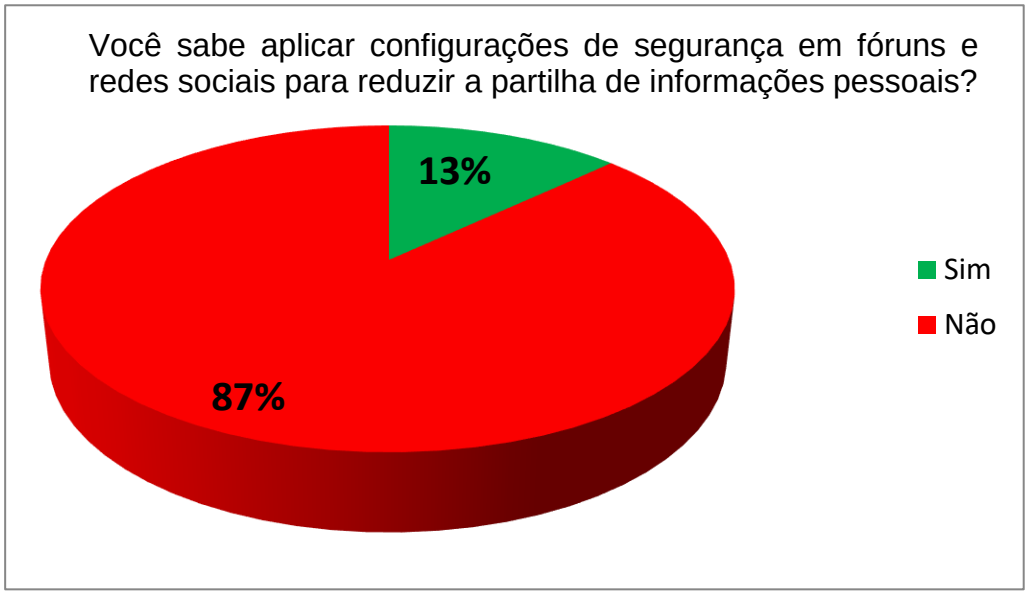
Ao serem questionados sobre o computador em que acessa a *internet* teria um antivírus atualizado, obtivemos as seguintes informações: 27% responderam sim, 31% disseram não e 42% alegaram que usavam o computador sem antivírus, o que torna estes usurários totalmente vulneráveis aos possíveis ataques de vírus ou *hacker* em sua máquina.



Quando perguntamos aos mesmos se sentiam seguros, na atual realidade, em navegar na *internet*, 32% destes entrevistados responderam que sim e outros 68% responderam que não. Logo, podemos concluir deste questionamento que a maioria demonstrou ter consciência e sensibilidade de que não estão totalmente seguros navegando na *internet*.

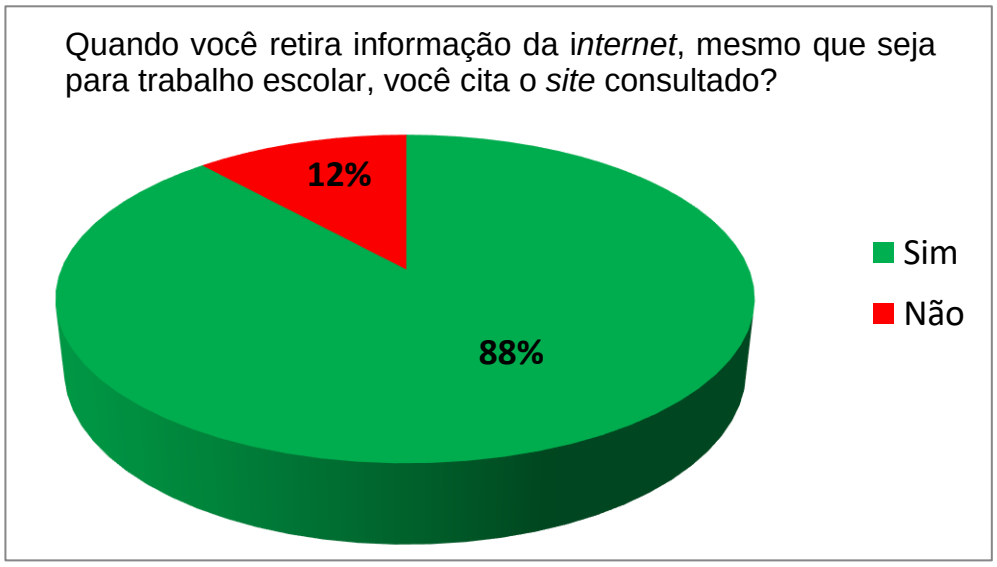


Ao opinar sobre o compartilhamento de informações pela *internet*, 16% disseram sim que estavam seguros em expor suas informações, sendo que 84% disseram que não e que, muitas vezes, compartilhavam, mas se sentiam preocupados em fazer tal operação na grande rede.

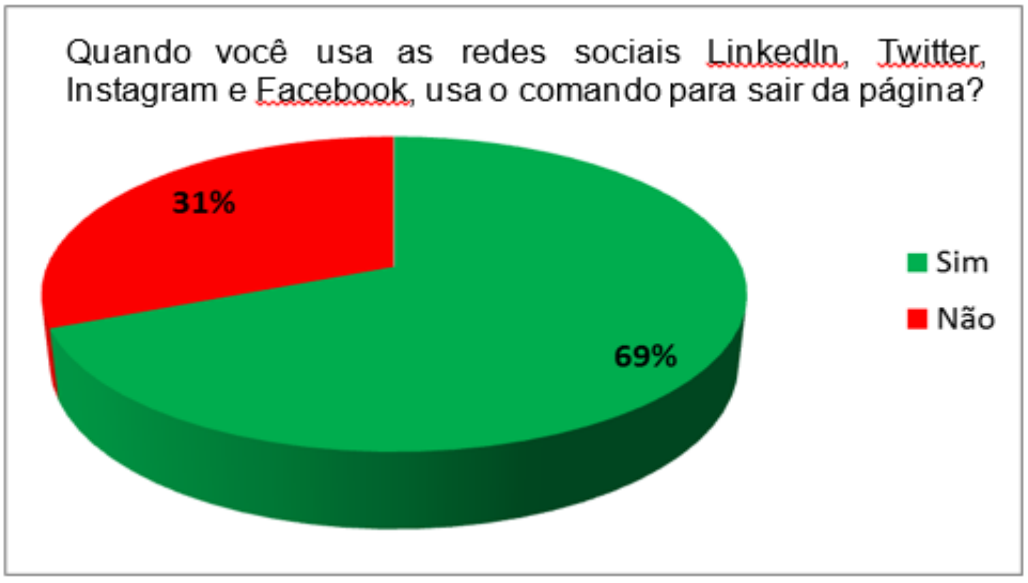


Nessa questão, solicitamos que eles respondessem se saberiam aplicar configurações de segurança em fórum e redes sociais para evitar o compartilhamento de informações pessoais e apenas 13% responderam que sim, que saberiam fazer esse tipo de procedimento, enquanto outros 87% afirmaram que não sabiam fazer essas configurações quando estão usando os fóruns e as redes sociais, mostrando assim que esses internautas podem ter suas

informações acessadas por quaisquer outras pessoas sem a sua permissão pela falta de conhecimento.

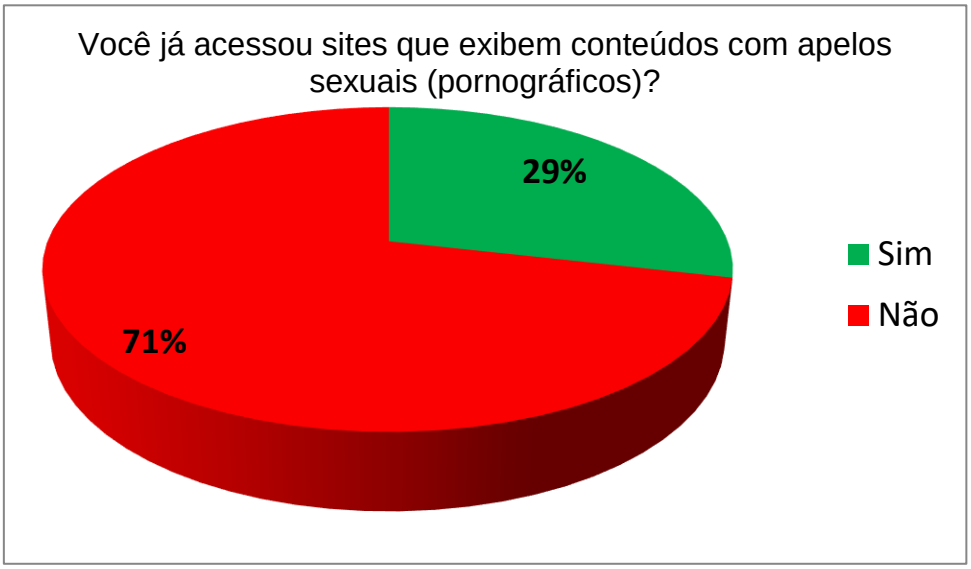


O resultado obtido quanto à citação de uma fonte de informação utilizada por eles para os trabalhos escolares foi a seguinte: 88% afirmaram sim, que citam a origem das informações, enquanto que 12 % não citam em seu trabalho de onde foram retiradas as mesmas.

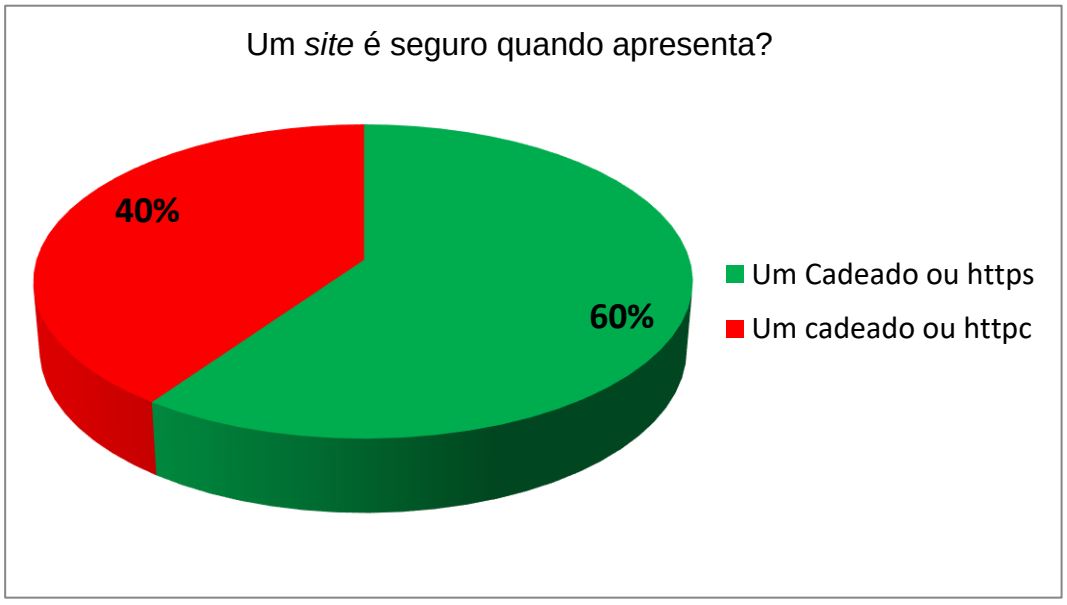


Já com relação às redes sociais do tipo *LinkedIn, Twitter, Instagram* e *Facebook,* questionamos os alunos sobre como eles encerram a seção; 69% responderam que usam o comando "sair da página", enquanto 31% responderam que não usam esse comando, sendo que eles alegam que simplesmente clicar no botão fechar que se encontra no lado direito na parte superior do *site* seria suficiente. Logo, sabemos que esse tipo de procedimento oferece

perigo, pois mantém o usuário conectado mesmo estando fora da página ou até mesmo com o seu computador desligado, falhas desse tipo facilita a publicação e o hackeamento desses *sites* sem o seu conhecimento.



Ao serem questionados sobre o acesso de *sites* com conteúdo de apelo sexual, chegamos as seguintes conclusões: 71% afirmaram nunca ter visitado esse tipo de página e 29% confirmou que já teve acesso aos *sites* e conteúdo, sendo que, muitas vezes, o endereço para o qual o internauta é direcionado não aparece, gerando um problema que impede o usuário saber para onde está sendo levado e qual a verdadeira intenção desse desvio de endereço.



E para finalizarmos o nosso questionário, perguntamos aos discentes, quando era que um *site* apresentava as devidas ferramentas de segurança, sendo que 60% falaram que o *site* era seguro quando apresentava um cadeado ou https nas suas configurações; já 40% alegavam desconhecer esses itens de segurança. Logo, podemos perceber que esses internautas não possuem um bom domínio de navegação quando se trata de segurança na grande rede de computadores.

4 CONCLUSÃO

Por meio do que foi exposto percebe-se a grande dificuldade de uma conexão segura, já que a quantidade de códigos maliciosos que são criados e distribuídos no mundo virtual é gigantesco. Sabemos que a tecnologia cada vez mais domina o mundo e revela a necessidade de termos nossos sistemas informatizados com mais segurança e confiabilidade. Para FERNANDES.

> Ameaças como os atuais “vírus” ou “cavalos de Tróia” potencializam este tipo de vulnerabilidade, permitindo ao invasor adquirir domínio total da estação e capturar toda e qualquer informação armazenada, inclusive a senha de acesso aos servidores da mesma rede. A privacidade e proteção na utilização do correio eletrônico, requer sistemas, específicos e soluções de identidade digital que permitem a troca de mensagens criptografadas - garantido o sigilo, e integridade no trajeto e na armazenagem. (FERNANDES, 2000, p.5).

Neste artigo, destacamos a importância de identificarmos as dificuldades e os pontos fracos de segurança no ciberespaço, concepção essa que deverá estar presente em cada internauta para poder minimizar a grande quantidade de ataques virtuais. Nesse sentido, vale a pena ressaltar o quanto é importante o uso de antivírus bons e atualizados e, que também não devemos abrir mão de um programa de *firewall*, criando assim uma barreira defensora dos possíveis ataques que seu computador venha a sofrer.

Ao longo deste trabalho utilizamos várias dicas para não abrir ou executar arquivos suspeitos ou de origem não confiáveis, conseguidos através da *internet*. Também direcionamos nossa atenção para os arquivos “attachados” (arquivo anexado a uma mensagem *de e-mail*) pois, muitas vezes, esse tipo de arquivos têm as ferramentas necessárias para que seu computador seja manipulado por indivíduos maus intencionadas.

Ao longo do texto relatamos ainda os cuidados que devemos ter ao criarmos nossas senhas para podermos acessar certos conteúdos na grande rede, procurando sempre dificultar sua identificação ou decodificação, lembrando que as mesmas serão nossa identificação no mundo virtual.

Por fim, de acordo com a pesquisa que foi realizada na Escola Estadual Gilney de Souza, na cidade de São Miguel, no estado do Rio Grande do Norte, ficou claro que os alunos possuem, até certo ponto, o domínio quando o assunto é segurança na grande rede. Porém, ao mesmo tempo a pesquisa aponta alguns despreparos de uma grande parte destes internautas. Em uma das perguntas chave do nosso questionário os alunos foram indagados sobre o reconhecimento dos elementos de seguranças contido em um *site,* onde obtivemos um percentual bem alto de desconhecimento desse item tão importante na hora da navegação. Isto é, foi possível perceber que essa porcentagem ainda é bastante elevada quando se trata de segurança na grande rede de computadores, de maneira geral.

No entanto, esperamos ter alcançado nossos objetivos com este trabalho, já que o mesmo tem a finalidade de conscientizar os estudantes do ensino médio e todos os internautas de um modo geral, quanto aos cuidados, direito e deveres que deveram ter ao se conectarem a *internet*. Esperamos ainda que esse estudo contribua como embasamento para investigações futuras relacionadas à segurança no acesso a grande rede.

7 REFERÊNCIAS

ABREU, Leandro Farias dos Santos. **A Segurança da Informação nas Redes Sociais**. São Paulo, 2011.

ALVES, Cássio Bastos. **Segurança da Informação vs. Engenharia Social: Como se proteger para não ser mais uma vítima**. Brasília, 2010.

BRASIL. Comitê Gestor da Internet no Brasil. **Cartilha de Segurança para Internet**. São Paulo, 2013.

BRASIL. **Marco civil da internet: Lei n. 12.965**, de 23 de abril de 2014. 2. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2015.

FERNANDES, Débora Winter et al. **Segurança na internet**. Florianópolis, 2000.

FERREIRA, Jeferson Luiz Miranda. **Segurança em Redes sem Fio**. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 5. ed. São Paulo: Atlas, 1999.

GUILHERME, Luís Miguel Borges. **A Segurança na Internet: Noções básicas**. São Paulo, 2010.

LEVINE, John, and Margaret Levine Young. **Internet para leigos**. Alta Books Editora, 2013.

KASPERSKY, Eugene. **O cibercrime se tornou cruel", diz Eugene Kaspersky**.RevistaVeja,27junho2017.EntrevistaconcedidaaAngelaNunes. Disponível em:

<http://veja.abril.com.br/mundo/o-cibercrime-se-tornou-cruel-diz-eugene kaspersky/>. Acessado em 02 de outubro de 2017.

KASPERSKY, Eugene. **Vírus eletrônicos prosperam com ajuda de erros primários de usuários de computadores e celulares**. Revista Veja, 16 setembro 2012. Entrevista concedida a Fernando Valeika. Disponível em: <http://veja.abril.com.br/noticia/vida-digital/virus-eletronicos-prosperam-com-juda-de-erros-primarios-de-usuarios-de-omputadores-e-celulares-diz-kaspersky>. Acessado em 20 de março 2017.

NOVO, Jorge Procópio da Costa. **Softwares de segurança da informação**. Manaus: Centro de Educação Tecnológica do Amazonas, 2010.

RAMOS, Márcio Roberto Vieira. **O uso de tecnologias em sala de aula**. **V Seminário de Estágio do Curso de Ciências Sociais do Departamento de Ciências Sociais-UEL. Londrina**, v. 11, p. 212, 2012.

SERRANO, Paulo. **Vírus: cuidados que se deve ter com o seu computador**. Agosto de 2001. Disponível em <http://www.apostilando.com/download.php?cod=2751&categoria=Diversas>. Acesso em: 17out. 2017.

VERGARA, Sylvia Constant. **Tipos de pesquisa em administração**. Rio de Janeiro, 1990.

VILHENA, Antonio. **Dicas de segurança para seu micro: vírus**. Em: <http://www.boadica.com.br/layoutdica.asp?codigo=215>. Acessado em: 02 de fev 2017.