10ª Jornada Acadêmica da Jornada da UEG
"Integrando saberes e construindo conhecimento"
10 a 12 de Novembro de 2016
UEG - Câmpus Santa Helena de Goiás, GO

A Segurança não gira em torno do antivírus

Raquel Cristina dos Santos[1]; Carla Cristina Rodrigues Leal[2]

[1]Discente do 2º Semestre do curso de Sistemas de Informação, raquelcristinarv@gmail.com

[2] Docente e orientadora do curdo de Sistemas de Informação, carlacrisleal@gmail.com

RESUMO: Todas as pessoas convivem com a tecnologia de informações diariamente, e para isso, é preciso garantir a segurança destas; portanto este artigo propõe a compreensão do cuidado que se deve ter ao utilizar dispositivos eletrônicos, pois a segurança não gira em torno somente do antivírus, como muitos usuários acreditam e praticam; é justamente por esse motivo, a falta de conhecimento das pessoas que pretendem entender até onde está completamente seguro. Para isso, pesquisas em publicações diversas que envolvem a Segurança da Informação e fatores relevantes a esta foram realizadas. A fim de instruir, incentivar/motivar o senso crítico a respeito do cuidado que se deve ter ao adentrar no mundo cibernético, a abordagem é simples e dinâmica, e de importância a todos. É de interesse de quem desfruta da tecnologia saber dos perigos virtuais e como se proteger; assim como aprofundar os conhecimentos na Segurança da Informação, e compartilhar/conscientizar outras pessoas. Tendo uma perspectiva mais ampla, é possível entender como é importante ter cautela ao navegar pela Internet com dispositivos eletrônicos. Surge assim, uma perspectiva crítica naturalmente, então, pequenas atitudes para se ter mais cuidado e corrigir falhas adotadas espontaneamente, e se aperfeiçoam à medida que o conhecimento cresce.

PALAVRAS-CHAVES: Informação. Humano. Compreensão. Crítica. Incentivo.

The security not revolve around antivirus

ABSTRACT: All people live with technology and information daily and for that is necessary ensure the safety of these. This article propose to understand the care that should be when use electronic devices because it doesn't revolve around only of the antivirus how many users believe and practice. It is just for this reason, the lack of knowledge of the people who it is intended to understand until where is completely safe. For this searches in various publications involving the Security of Information and factors relevant to this went performed. For to instruct, encourage/motivate the critical sense regarding the care should be when entering in the cyber world, the approach is simple and dynamic, and the subject of importance to all. It is of interest to those who enjoy technology know the dangers and how to protect yourself; as well as deeper the knowledge on Information Security, and share/to make others. Having a broader perspective, it is possible to understand how important it is to exercise caution when browsing the Internet with electronic devices. Thus arises a critical perspective naturally so small attitudes to be more careful and correct faults taken spontaneously, and if perfect as knowledge grows.

KEYWORDS: Information. Human. Understanding. Critical. Incentive.

INTRODUÇÃO

A informação é essencial para tudo o que se faz, independentemente de seu tipo ou do grau de complexidade, seja para se chegar ao shopping, comprar um presente, criar um software ou gerenciar uma empresa ou seja, ela é fundamental para o dia a dia, mesmo em pequenas atividades. Essas informações são geradas a todo o momento e vêm crescendo em quantidade e em velocidade, assim novas técnicas para manuseá-las são desenvolvidas.

Com esse volume de informação, garantir a segurança virtual e o sigilo da informação se torna essencial e um simples antivírus não a pode garantir totalmente; então é preciso entender até onde pode assegurá-la. O objetivo que pretende alcançar na execução é compreender sobre a segurança além do antivírus, depois disto entender o porquê algo que deveria proteger, não a faz com eficácia, e por fim, analisar fatores de proteção e entender falhas do sistema e apresentar algumas possíveis saídas.

Seja em um computador pessoal ou empresarial, este de alguma forma precisa estar conectado em uma rede interna ou a Internet, a fim de compartilhar e receber dados e informações de diferentes tipos que precisam estar a salvos, evitando o mau uso destas. Então surge a questão que cerca essa rede: Se os computadores estão conectados, até onde se pode garantir a segurança cibernética?

Desde já, tendo consciência de que a completa segurança virtual não é possível, todavia, praticar atos que a garantem com mais eficácia é uma boa saída para se prevenir de ações maliciosas. Outra hipótese, é compreender como funciona o mundo cibernético, isto pode garantir ações mais seguras, pois conhecendo o ciberespaço, seus perigos e vantagens, as atitudes são boas, ou seja, fugindo das armadilhas virtuais maldosas, tais como ter dados pessoais clonados por meio de *sites* de compras, ter o computador contaminado com vírus, entre outras ameaças.

Em razão da sociedade, esse artigo visa despertar interesse de todos em relação a segurança, principalmente nos tempos atuais há mais perigosos de ataques virtuais; de uma simples rede social a contas bancárias e sites governamentais; de um simples *download*[1] [1]da foto de um desconhecido, a segredos de Estado, e até mesmo tráfico de crianças e órgãos na *Deep Web*[2][2].

[1] Baixar arquivo de um servidor
[2] Parte obscura da Internet onde há matadores de aluguéis, ataques cibernéticos, pedofilia entre outras coisas maliciosas.

Então, tendo ciência da falta de conhecimento de grande parte da sociedade em relação a Segurança da Informação, é preciso que cada pessoa se conscientiza e também compartilhe os conhecimentos, visando formar uma grande corrente de conhecimento, proporcionando mais força e mais segurança.

Há quem opte por ter um conhecimento supérfluo sobre a Segurança da Informação, porém há quem decida aprender e aprofundar seus conhecimentos sobre a Segurança da Informação; então esses que procuram aprender cada vez mais, este artigo vem motiva-los, desperta-los, e aos que se contentam com pouco, o artigo visa informá-los, despertar interesse, para que estejam buscando aprender e a compartilhar os conhecimentos da Segurança da Informação, conhecimentos quem são essenciais nos dias atuais.

Todas as pessoas que desfrutam da tecnologia, são atemorizadas com os vírus, que podem destruir tanto softwares quanto hardwares, podendo levar uma empresa a falência; e mesmo se precavendo dos vírus, eles acabam infectando mesmo sem o conhecimento do usuário. Para entender a segurança é preciso antes compreender de qual perigo ela protege.

> Um vírus de computador é um programa ou pedaço de código que é carregado ao seu computador sem seu conhecimento ou permissão. Alguns vírus são meramente irritantes, mas a maioria dos vírus são destrutivos e designados a infectar e controlar sistemas vulneráveis. Um vírus pode se alastrar a vários computadores e redes ao criar cópias dele mesmo, assim como um vírus biológico passa de uma pessoa para a outra. (AVAST, 2016, s/p,a)

Entendendo o que é um vírus e os graves riscos que podem trazer, é preciso compreender, mesmo que superficialmente, o lado tenebroso da Internet que poucos usuários conhecem, a *Deep Web*.

Para Santos e Marchini (2013), a *Deep Web* é a parte obscura e profunda da Internet, em que ser anônimo é o que importa, já que há conteúdos que não são encontrados na Internet que se conhece, a superfície; sendo assim para ter acesso a *Deep Web*, é preciso um navegador específico para tal, e não os navegadores comuns utilizados para a superfície como o Google Chrome, Explorer, Ópera, entre outros.

Para entender melhor a *Deep Web*, entenda-a como um iceberg, onde sua ponta é a Internet que todos têm acesso, e o restante, escondido no profundo oceano é a *Deep Web*, um lado obscuro da Internet onde um computador não pode ser rastreado, onde nem todos chegam ou conhecem por inteiro, um lugar onde há coisas medonhas de todo tipo que se pode imaginar.

Não há como estar completamente seguro, segundo o *site* O Globo, o ataque a *Sony Picture Entertainment*, foi a mais arrasador nos Estados Unidos da América; a Sony teve dados

divulgados, mas não para por aí, a forma como os criminosos virtuais tem exercido seus crimes tem se espalhado, grande parte ocorre pela *Deep Web*; esta é uma das provas de que não se pode garantir a completa segurança virtual, pois se uma grande companhia com tanta proteção foi atacada, quanto mais os usuários e computadores residenciais e de pequenas empresas. Com tantos perigos, surge a necessidade de se assegurar desses males; é por isso que há os softwares de antivírus.

Para uma das maiores pioneiras da computação, Microsoft (2012), o antivírus é um software cuja função é detectar e neutralizar toda e qualquer ação maliciosa que tenta atacar um dispositivo e danificá-lo. É por esse fato que todos aqueles que desfrutam da tecnologia em computadores, celulares e *tablets* utilizam antivírus, porém poucos tem conhecimento ou ao menos uma breve noção a respeito da segurança virtual ou do que se passa no mundo cibernético.

"Ciência cujo objeto de estudo concentra-se na comparação dos sistemas e mecanismos de controle automático, bem como na regulação e comunicação não só nos seres vivos, porém também nas máquinas" (MICHAELIS, 2016, s/p). A cibernética é praticamente um mundo virtual, onde há população, inocentes e criminosos; de crianças a velhos; de crimes a prazeres. Todos estão conectados a esse universo sem regras. E neste ponto encontra-se a *Deep Web.*

Para algumas pessoas terem o antivírus em seu dispositivo eletrônico é o suficiente, já para outros é só o primeiro passo; mas o que realmente importa é que ter um bom antivírus e mantê-lo atualizado é fundamental para adentrar no mundo cibernético, seja na *Deep web* ou não, pois informações também são roubadas na Internet que todos conhecem, e até mesmo em computadores conectados entre si, em uma rede intranet.

Se em bom estado, ou seja, atualizado e regularizado, e o dispositivo escaneado regularmente afim de encontrar vírus, para remove-los, o antivírus consegue barrar ações maliciosas que tentam invadir o computador ou qualquer outro dispositivo eletrônico, porém é de extrema importância saber que os vírus e as diferentes formas que se apresentam evoluem tanto quanto a proteção contra os mesmos, o que acaba deixando o antivírus desatualizado, e o computador vulnerável aos vírus maliciosos

MATERIAIS E MÉTODOS

Esse trabalho utilizou como metodologia científica a pesquisa Bibliográficas, que segundo Lakatos e Marconi (2000), abrange toda bibliografia já tornada pública sobre um determinado estudo seja em livros, jornais, pesquisas, monografias, entre outros meios de divulgação.

O método de estudo aplicado neste artigo é o método indutivo; que acordo com Gil (1991), caminha para constatações particulares a partir de observações afim de explicar fatos e propor hipóteses para solução do problema, não deixando de lado a análise crítica para se comprovar o estudo. Os teóricos abordados foram: Avast (2016); Eiras (2004); Gil (1991); Lakatos e Marconi (2000); Puttini (2001); Michaelis (2016); Microsoft (2012); Santos e Marchini (2013).

A seguir serão apresentados alguns pontos importantes para se compreender o ciberespaço, a segurança virtual e atitudes que podem fazer a diferença para qualquer pessoa que utiliza um computador conectado à alguma rede.

A vulnerabilidade da segurança

Nem toda segurança é completa, há diversos fatores que interferem diretamente ou indiretamente na Segurança da Informação, estes que abrem portas e deixam o sistema cada vez mais indefeso. Através das vulnerabilidades, nos pontos fracos na segurança surgem as ameaças para aproveitar das falhas e provocar prejuízos e perdas a organizações ou pessoal.

Sendo assim, é preciso conhecer onde estão os pontos fracos seja em dispositivos pessoais ou corporativos; para isto pode-se identificar essa vulnerabilidade, que Nascimento (2013) destacou:

- Estrutura física: A parte física do ambiente em que o dispositivo/máquina que gerencia ou armazena as informações (servidores) se encontra pode comprometer a segurança da informação;
- Hardware: Um vírus não ataca somente o software, mas através do software pode danificar o hardware também; porém, se o hardware estiver defeituoso, as chances de ataques diretamente ou indiretamente se tornam grandes;
- Software: É onde acontece a maior parte das invasões por ser geralmente o ponto mais fraco; a vulnerabilidade do software surge com a instalação incorreta de

programas; com a permissão de acesso de forma equivocada; e até mesmo com aplicativos, mensagens, ofertas, entre outros recebidos por e-mail;

- Humano: O fator humano na segurança é tão importante quanto o software para o bom funcionamento da máquina, porém assim como o software o fator humano é um grave ponto fraco. Seja com atitudes intencionais ou não; criando senhas fracas; não tendo um treinamento correto, assim como a falta de conhecimento sobre Segurança da Informação.

Pelo fato do antivírus não garantir total segurança, já que há outros fatores de vulnerabilidade envolvidos, como os pontos fracos citados acima e levando em consideração o fator de evolução de vírus, os ataques e a forma como eles se manifestam; entende-se que é impossível garantir completa segurança, pois sempre haverão falhas por parte do dispositivo ou de quem o manuseia, o usuário.

Porém, sabendo das vulnerabilidades, e tendo conhecimento a respeito da Segurança da Informação em aspecto pessoal e empresarial, é muito mais fácil proteger sua corporação e também seu computador pessoal, e as chances de sofrer um ataque, de violar as informações são menores, justamente pela perspectiva mais ampla e crítica construída com o conhecimento.

RESULTADOS E DISCUSSÕES

Os ataques a dispositivos eletrônicos começam muitas vezes de uma forma sutil, a discrição tem início abrindo-se portas para vírus maiores; mas de onde vem esses "pequenos" vírus?! Eles surgem de links sugeridos e abertos na caixa de mensagem de e-mail, podem vir junto a instalação de um aplicativo, ou até mesmo no download de um vídeo.

É então que entra o *firewall*[3], para impedir que os pequenos e discretos vírus não abram as portas para outros maiores; para melhor entendimento, entenda que o *firewall* é o porteiro de um prédio, cujo monitora as portas do computador e barra quando necessário os softwares maliciosos.

Além do *firewall*, é essencial ter um bom antivírus, como já mencionado, e manter seu banco de dados com os tipos de ameaças detectadas atualizado, já que os vírus e a forma

[3] Parede de fogo. É responsável por controlar todo o fluxo de dados do computador e/ou da rede, permitindo assim somente programas de confiança.

como se manifestam evolui constantemente; os softwares de proteção possuem ferramentas adicionais que acabam se tornam importantes, como uma limpeza, ou uma varredura no computador, analisando todos os arquivos e programas, afim de mantê-lo livre de *malware*[4].

Outro cuidado que se deve ter é com os *spywares*; segundo a corporação Avast (2016), *spywares* são *malwares* que dificilmente são detectados, estes coletam informações de todos os tipos do computador e do usuário, até mesmo as informações pessoais que são inseridas em sites; no entanto, além de coletar eles também repassam os dados a terceiros com intenções de tirar proveito.

Muitas vezes o computador pode conter *spyware* e o usuário nem ao menos desconfiar, os hackers utilizam- os para poder espionar o usuário e transferir as informações do usuário, com intenções maliciosas para tirar vantagem.

Muitas vezes os *spywares* surgem quando o usuário baixa músicas ou filmes muito facilmente, na instalação de programas, ou então ao abrir um anexo em seu e-mail.

Para identificar um *spyware* é preciso que o usuário conheça bem seu computador e os programas que ele possui, pois assim que surgir ícones novos que sejam estranhos e fora de seu conhecimento, mensagens de erro aleatoriamente ao se utilizar funções que antes funcionavam sem problema algum, esse possa ser examinado, porque há a possibilidade de ser um *spyware*.

Muitos antivírus já possuem a função *antispyware*, porém há também softwares *antipyware* específicos para ter mais eficácia em identificar e aniquilar os *spywares*; barrando-os antes que estes danifiquem os dados da máquina, ou da rede em que este está conectado.

Além desses cuidados que o usuário deve ter, é preciso que o usuário também tenha consciência e cuidado ao navegar pela Internet, é preciso ter cautela ao acessar sites e inserir dados pessoais, ao baixar mídia digital, ao fazer *download* de arquivos anexados a e-mails, principalmente se este for de origem comercial, com propagandas e propostas atrativas.

O usuário deve ser prudente com esse tipo de mensagem, *spam*[5], que segundo Eiras (2004), os *spams* são mensagens de serviços muito semelhantes aos originais de empresas, porém trazem vírus e *malwares.*

Ao acessar *sites* de cadastro principalmente os que solicitam senhas, e documentos pessoais, como os de compras e públicos, é preciso cautela, e observar alguns fatores que fazem a diferença, como por exemplo na barra de endereço do *site* a sigla *https*, a mesma deve estar

[4] Software malicioso.
[5] Nome dado a mensagens recebidas que não são desejadas

da cor verde, assim como um cadeado que a acompanha (em páginas seguras que possui campos para inserir informações pessoais); outro ponto importante a ser observado são as propagandas que surgem, muitas vezes, não tem nada a ver com o conteúdo de origem e acabam se tornando um alerta para que navega na página de que esta propaganda pode ser vírus.

Por fim, para não dar chance aos *hackers* e manter a segurança uma orientação importante é criar senhas fortes, com letras, números e símbolos; e para diminuir as chances mais ainda, vale a estratégia de criar um banco de palavras-chave, ou seja, um conjunto de palavras para auxiliar a se lembrar das senhas, guardando-o em um ligar seguro.

Então de tempo em tempo se altera a senha do cartão, do e-mail, de redes sociais, de dispositivos, dos acessos de uma forma geral. Ex. Uma pessoa possui cinco senhas diferentes, e as mantem seguras, então a cada três meses ela altera a permissão de suas contas de modo que as senhas sejam diferentes, desta forma, caso se esqueça/confunda as terá em mãos.

CONCLUSÃO

Diante dos fatos entende-se que garantir por completo a segurança não é possível, todavia boas práticas para se prevenir do perigo não se limitam a ter um antivírus, porém, conclui-se que diante do conhecimento a respeito de Segurança da Informação e dos perigos e vantagens que o ciberespaço oferece, a navegação pela Internet ou por outro tipo de rede, pode se tornar mais segura de acordo com as atitudes de quem navega na rede.

Diante do aprendizado do mundo cibernético, a maneira de navegação não será mais a mesma, nem tampouco a disposição de sempre estar aprendendo, buscando novos conhecimentos para não se tornar uma vítima de crimes virtuais. Um olhar crítico em relação ao que acontece em volta é desenvolvido aos poucos e aperfeiçoado.

Estar no mundo cibernético se tornou algo de extrema importância a todas as pessoas, a ponto de um soldado morrer em uma guerra se não estiver conectado, um país pode ser prejudicado seriamente caso não confie e/ou não esteja presente no neste mundo. O mundo cibernético se tornou relevante de uma tal forma que nada consegue viver fora dele, porém tudo se adapta.

REFERÊNCIA

AVAST, Software Incorporation. **Hacker.** 2016.**a**. Disponível em: < https://www.avast.com/pt-br/c-hacker> Acesso em: 07 set 2016

AVAST, Software Incorporation. **Malware**. 2016.**b**. Disponível em: < https://www.avast.com/pt-br/c-malware> Acesso em: 07 set 2016

AVAST, Software Incorporation. **O que é um spyware**. 2016. **c**. Disponível em: < https://www.avast.com/pt-br/c-spyware> Acesso em: 07 set 2016

AVAST, Software Incorporation. **Vírus de computador**. 2016. **d.** Disponível em: < https://www.avast.com/pt-br/c-computer-virus> Acesso em: 07 set 2016

EIRAS, Marcelo Coradassi. **Engenharia Social e Estelionato Eletrônico.** 2004. Disponível em:< https://docs.google.com/file/d/0Bx7iZfTfN4y0VlZyc29ENDNBUm8/edit> Acesso em: 07 set 2016

GIL, Antônio Carlos. **Como elaborar projetos de pesquisas**.3ed. São Paulo. Atlas 1991.

LAKATOS, Eva Maria., MARCONI, Marina de Andrade. **Metodologia Cientifica**. 3ed. São Paulo. Atlas, 2000.

MEDEIROS, Carlos Diego Russo. **Segurança da Informação.** Implantação de medidas e ferramentas de Segurança da Informação. 2001. Disponível em:
< http://www.projetoderedes.com.br/apostilas/apostilas_seguranca.php>
Acesso em: 07 set 2016

MICHAELIS, Moderno dicionário da língua portuguesa. **Cibernética**. São Paulo: Companhia Melhoramentos. 2016. Disponível em: <http://michaelis.uol.com.br/> Acesso em: 07 set 2016

MICROSOFT. Microsoft. **O que é um software Antivírus?**. 2012. Disponível em:

< https://www.microsoft.com/pt-br/security/resources/antivirus-whatis.aspx>
Acesso em: 07 set 2016

NASCIMENTO, Nelson José do. **Ameaças e vulnerabilidades da segurança. Como precaver**. 2013. Disponível em:
<http://www.portaleducacao.com.br/educacao/artigos/48819/ameacas-e%20vulnerabilidades-da-informacao-como-precaver> Acesso em: 25 set 2016

O GLOBO. **Ataque contra a Sony Pictures deve custar mais de U$100 mil, diz especialista**. 2014. Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/12/ataque-contra-sony-pictures-deve-custar-us100-mi-diz-especialista.html> Acesso em: 25 set 2016

SANTOS, Carlos H. Aguiar dos. MARCHI, Késsia Rita da Costa. **O Que a Deep Web Pode Oferecer Além da Surface Web**. 2013. Disponível em:
<ttp://ftp.unipar.br/~seinpar/2013/artigos/Carlos%20Henrique%20Aguiar%20dos%20Santos.pdf> Acesso em: 07 set 2016