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

CRIMES VIRTUAIS: A internet é segura?

David Amaral Freitas[1]

Carla Cristina Rodrigues Leal[2]

[1]Discente do 2° semestre do curso de Sistemas de Informação, david.amfr7@gmail.com

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

RESUMO: Perante a evolução da tecnologia nos últimos anos, o computador se tornou uma ferramenta essencial no cotidiano do mundo moderno, sendo de fato benéfico, pois, auxilia em vários processos feitos pelo homem, há suas inseguranças, pois, sendo uma máquina de utilizar informações do usuário para seu manuseio, pode ser também uma arma para criminosos obterem estes dados para seus atos maliciosos, englobando a área computacional, O objetivo geral que é buscado neste artigo é procurar entender determinados meios de usar a internet e se proteger de seus riscos, neste artigo será tratado sobre o tema crimes virtuais referentes aos riscos e alguns métodos de se proteger, abordando todo assunto com o uso da pesquisa bibliográfica utilizando do método dialético e dedutivo para chegar em uma conclusão , sendo visado qual o limite da sua segurança para usufruir da internet sem correr riscos eminentes.

PALAVRAS-CHAVE: Tecnologia. Criminalidade Virtuais. Segurança virtual. Invasão.

VIRTUAL CRIMES: The internet is safe?

ABSTRACT: Given the evolution of technology in recent years, the computer has become an essential tool in the daily life of the modern world, being beneficial fact therefore helps in many cases man-made, there are insecurities because, being a machine to use information user for handling, can also be a weapon for criminals to obtain this data for their malicious acts, encompassing computational area, the overall objective of which is sought in this article is to try to understand certain ways to use the internet and protect their risks in this Article will be dealt with on the subject virtual crimes related to risks and some methods to protect, covering every subject with the use of literature search using the dialectic and deductive method to arrive at a conclusion, being targeted which limit your security to take advantage of internet without running eminent risks.

KEYWORDS: Technology. Virtual Crime. Cyber security. Invasion.

INTRODUÇÃO

A internet se tornou um meio de evolução entre diversas culturas e sociedades, como meio de comunicação favoreceu ao mercado mundial o caminho tecnológico, sempre desenvolvendo máquinas mais potentes e sofisticadas que além de transmitir muitas informações aos seus usuários, também traz insegurança de dados guardados na rede.

O objetivo geral que é buscado neste artigo é procurar entender determinados meios de usar a internet e se proteger de seus riscos. O avanço tecnológico vem crescendo de forma alarmante e trazendo benefícios e malefícios aos usuários desta rede de comunicação.

Antes da internet era comum se enviar cartas para comunicar, hoje é apenas necessário digitar a mensagem e apertar uma tecla, um problema específico é o modo como os usuários utilizam a internet, deixando expostas fotos, dados pessoais, usando sem o mínimo requerido de segurança, abrindo brechas para que possam ser vítimas de algum crime virtual, se tornado um real problema, mas qual seria a solução viável a este ato, teriam algum vestígio de encontrar esses criminosos ou a segurança do usuário não existe ?

> Crimes são cometidos a todo o momento em várias partes do mundo, em diversas localidades, mas com a chegada da internet, delinquentes migraram para a área virtual, podendo cometer seus atos em anonimato, tendo fáceis formas de capturar vítimas online, delitos de nível pessoal a governamentais, de furto de dinheiro a roubo de informações sigilosas. Para as autoridades o maior obstáculo é justamente descobrir as verdadeiras identidades destes delinquentes, sendo diversos deles jovens imprudentes com ampla sabedoria em informática, o nome como esses criminosos são conhecidos é o termo "cracker", o oposto de hackers, os quais – "Hacker" e "cracker" podem ser palavras parecidas, mas possuem significados bastante opostos no mundo da tecnologia. De uma forma geral, hackers são indivíduos que elaboram e modificam softwares e hardwares de computadores, seja desenvolvendo funcionalidades novas ou adaptando as antigas. Já cracker é o termo usado para designar quem pratica a quebra (ou cracking) de um sistema de segurança (OLHAR DIGITAL UOL, s/d, s/p).

Atualmente, o assunto segurança relacionado à internet, vem sendo amplamente discutido por todas as mídias e pela sociedade, que por sua vez, está mais atenta quanto à eficácia ou não da segurança frente aos novos avanços tecnológicos. Casas inteligentes e carros autônomos que necessitam de informações de seus proprietários, redes sociais. O serviço de segurança vem sendo algo requisitado por muitos, mas que poucos possuem, pois, seu

orçamento e elevado, de forma que essa rede de informações carregue muitos arquivos valiosos para serem protegidos.

O governo intervém contra esses criminosos a bastante tempo, pois todas as pessoas têm acesso ao uso da internet, e criminosos são usuários também, um problema comum na internet é a liberdade e a facilidade de manuseio, o fato é que os delituosos conseguem se manter em anonimato e fazer tudo sem ser identificados, cada usuário precisa tomar suas próprias medidas de segurança, para que não sejam alvos de crimes.

O Proposito deste tema recorre ao uso cotidiano dos milhões de usuários de internet, sendo um vasto meio de transmitir diversas informações, e buscar compreender os riscos existentes, fazendo assim prevenção contra possíveis crimes virtuais, usando a rede de forma segura como meio de aprendizagem para que traga benefícios a sociedade.

Perante ao grande número de usuários de internet, o nível de informação cresceu em grande escala, junto a essas informações trouxeram meios de transpor dados pessoais que expõem a vida de várias pessoas, sendo um meio de expor o caráter do usuário, a internet se tornou acessível para todos, mas não totalmente segura, onde existem crimes de diversas formas, a segurança precisa ser identificada, se o erro está no usuário ou na falha dos sistemas que são utilizados.

O assunto tratado traz meios de conhecimento sobre a forma como a tecnologia vem sendo tratada como meios de aprendizagem e de formas que influenciam os acadêmicos a se protegerem contra riscos e crimes virtuais.

Segurança Virtual

O conceito de segurança sempre é um ponto a ser trabalhado, porém a proteção quem criam são os próprios usuários, mas de fato existem sistemas bastante seguros contra invasões entre tantos métodos de criptografia e bloqueio de riscos, mas de modo tudo pode ter uma falha para ser infringido, sendo oriundas de falhas humanas e não de um sistema computacional.

COMO MELHORAR A SEGURANÇA NA INTERNET

Boas práticas podem reduzir significativamente os ataques virtuais, mas a maioria dos usuários se descuida e facilita o acesso de hackers

Certifique-se de que há um software de segurança instalado

Evite fazer transações bancárias a partir de smartphones ou em conexões sem segurança

Não instale arquivos que chegam por e-mail ou por meio de redes sociais

Faça as atualizações sempre que o computador solicitar. Não deixe para depois

Mantenha um HD externo com arquivos importantes e fotografias

Evite transações bancárias que necessitam de cartão de crédito

Redobre a atenção às redes sociais: não compartilhe qualquer tipo de link pela rede

Gerencie suas senhas. É aconselhável ter várias, uma para cada finalidade. Outra dica é atualizá-las ou modificá-las frequentemente

FIGURA1: Como melhorar a segurança na internet
Fonte: ISTOE(s/d, s/p).

O melhor meio de se proteger na internet é precaver de alguns riscos, por invulnerabilidade de alguns fatores na máquina deixada por mau uso do usuários, faz o computador ser alvo fácil para invasões, é necessário que equipamento possua um software de segurança instalado no sistema operacional utilizado, evitar fazer transações e uso de dados pessoais pela rede tanto nos computadores quanto em smartphones, fazer sempre um backup em uma mídia externa de seus arquivos importantes, não abrir qualquer e-mail, evitar clicar em links atrativos na internet, mantê-lo atualizado, evitar instalar aplicativos desconhecidos, e escolher uma senha segura para seu acesso, pra que de modo não deixe seu computador todo vulnerável a supostos usuários maliciosos.

> *Se por um lado a tecnologia dá aos usuários ampla liberdade e máxima igualdade individual, por outro lado ela lhes retira a habilidade de distinguir as pessoas com as quais se relacionavam virtualmente, além de lhes restringir a capacidade de diferenciar a sensação de segurança da ideia de segurança como realidade. (* DIREITONET, s/d ,s/p)

A Internet inventa possível o meio de conhecer sobre as pessoas sem ser necessário contato físico, dando assim um meio de relacionar com outros usuários, sendo possível se passar por outra pessoa para se comunicar, pois a internet e um meio de não ter toda certeza de que o

outro usuário realmente seja quem diz ser, justamente por não estar presente visualmente: "A consciência digital, independente da idade, é o caminho mais seguro para o bom uso da*internet*,[sic] sujeita às mesmas regras de ética, educação e respeito ao próximo" (DIREITONET, s/d, s/p).

Se todo usuário fosse orientados a utilizar a internet como educados na escola a ser um bom cidadão, a internet seria um local de consciência e menos problemas, mas de todo modo, independente da educação, vai do caráter da pessoa exercer seu papel, se escolhe ou não ter caráter, fazendo assim, um usuário ciente de seus atos.

MATERIAIS E MÉTODOS

A metodologia cientifica que será utilizada para a elaboração desse trabalho é a pesquisa bibliográfica, a qual é Segundo Lakatos e Marconi (1987, p. 66) a qual "trata-se do levantamento, seleção e documentação de toda bibliografia já publicada sobre o assunto que está sendo pesquisado, em livros, revistas, jornais, boletins, monografias, teses, dissertações, material cartográfico, com o objetivo de colocar o pesquisador em contato direto com todo material já escrito sobre o mesmo. "

Os métodos utilizados são: dedutivo e dialético, os quais aprimoram a pesquisa, sendo estes:

> Método dedutivo – que partindo das teorias e leis, na maioria das vezes prediz a ocorrência dos fenômenos particular (conexão descendente) […]
> Método dialético – que penetra o mundo dos fenômenos tendo em vista sua ação reciproca, da contradição inerente ao fenômeno e da mudança dialética que ocorre na natureza e na sociedade (GIL,1991 p.91).

Nesse sentido, a seguir será apresentada a fundamentação teórica com seus respectivos subtítulos e autores que abordam o assunto

RESULTADOS E DISCUSSÕES

A Internet possui diversas camadas de informações, onde a maioria dos usuários possuem apenas uma parte de seu conteúdo livre, a liberdade de utilizar a internet é de todos

que a tem acesso, porém é um local onde procede muitos dados pessoais, sendo fácil de reconhecer muitos usuários que não tem o mínimo de ciência dos riscos corridos na rede, fazendo assim alvos fáceis para supostos criminosos. O usuário precisa se precaver de cada ato, e buscar se assegurar, não se iludir com qualquer anuncio e propaganda, pois esses são simples atos de fragilidade do usuário: "O ciberespaço não dispõe de fronteiras territoriais, mas de normas ou técnicas, que regulam sistemas de acesso e que não pertencem ao mundo jurídico. Assim, não vigora o conceito de soberania e nem de competência territorial" (RAMÓN, s/d, p.25-26, apud EGOV UFSC s/d).

Dentro da internet não existe hierarquia, nem divisões territoriais, mas sim camadas de acessos que guardam informações sigilosas, que não estão ao alcance de leis jurídicas dentro deste ciberespaço, de modo que as leis são implantadas na defesa de sistemas e informações de usuários, constituindo está proteção apenas na superfície da internet, dentro ao meio corporativo, onde as empresas de cyber segurança se focam mais na proteção de sistemas de empresas.

> Quanto mais a internet e os recursos tecnológicos fazem parte do nosso di [sic] a dia, mais o princípio da intimidade se torna mitigado. Em todo canto existem pessoas publicando fotos, vídeos ou informações sobre o que estão realizando. A pratica do chamado check-in é um exemplo disso, pois permite, inclusive, a geolocalização do indivíduo. Considerando isso, podemos dizer que a principal forma da pessoa ter a sua privacidade respeitada é se manter longe da internet, o que poucas pessoas conseguiriam fazer nos dias atuais (JORGE apud CRIMES CIBERNETICOS, s/d, s/p).

A tecnologia vem aumentando a cada dia trazendo novos recursos, trazendo um maior foco em seu uso, direcionando você a caminhos para se expor ao mundo, obrigando você exibir sua localização para poder usufruir do sistema, a verdade e que a maior segurança para você relacionado a internet é você não utiliza-lo. "Todavia, a realidade é que os atos que praticamos quando estamos conectados ao estonteante mundo virtual não nos isenta de sanções previstas no mundo jurídico, uma vez que são as possibilidades de sanções que garantem a eficácia do direito " (DOWER, 2005, s/p).

Mesmo de modo geral todo o uso da internet eleva aos usuários o direito de liberdade em suas pesquisas, mas não o isenta na liberdade das leis, fazendo assim com que precise seguir as mesmas leis no mundo virtual.

Criminalidade sempre foi algo existente no mundo, por diversos meios e modos, mas com a tecnologia os crimes de fato evoluíram, de modo com que migrassem para um mundo

virtual e acabasse afetando usuários no mundo real, deixando mais do que redundantes seus modos, fazendo expor a privacidade de outro, furtando dinheiro e informações, deixando a criatividade do criminoso inventar novos meios de prejudicar a vítima.

> Os crimes virtuais próprios são aqueles em que o sujeito se utiliza necessariamente do computador o sistema informático do sujeito passivo, no qual o computador como sistema tecnológico é usado como objeto e meio para execução do crime nessa categoria de crimes está não só a invasão de dados não autorizados mais toda a interferência em dados informatizados como, por exemplo, invasão de dados armazenados em computador seja no intuito de modificar, alterar, inserir dados falsos, ou seja, que atinjam diretamente o software ou hardware do computador e só podem ser concretizados pelo comutador ou contra ele e seus periféricos, para alguns doutrinadores como Marco Túlio Viana trata esse tipo de conduta como próprios:
> "São aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)."(Fundamentos de direito penal informático. Apud âmbito jurídico., 2003, p. 13-26)

Os crimes virtuais são de modo todo ato que infringe o computador para danificar de algum modo seu sistema afim de prejudicar outros usuários, fazendo com que o computado seja acessado pelo criminoso de modo com que ele possa alterar, modificar, ou inserir dados falsos em um sistema, ou até mesmo inutilizando a própria máquina, gerando assim a danificação de seus periféricos.

CONCLUSÃO

Em relevância com o tema tratado nesse artigo, chegou-se a debater vários fatores coerentes a utilização da internet, deixando visado ações existentes da criminalidade na rede, onde mesmo apresentando sequenciais fatores de ocorrências sobre esse assunto, o questionamento da segurança veio a ser essencial para o conjunto tratado desta realidade, chegando a ser pertinente ao anonimato, regendo assim meios de precaver para evitar tais atos ilegais.

Em contato com o assunto veio a perceber-se que, contudo, a segurança é um fator que não é completamente assegurado de sua função, não se pode confirmar estar seguro de acessar a internet, podendo haver riscos de apenas acessa-la, como apresentado ao trabalho pode-se prevenir de vários riscos, fazendo um uso consciente da rede evitando se expor e utilizar sumas informações que podem lhe causar problemas futuros, fazendo a prevenção contra possíveis ocorrências, deixando a segurança em presente momento ao critério do usuário, até surgir novos meios de estabelecer um conforto real por uma real segurança.

REFERÊNCIAS

DIREITONET. **Crimes cibernéticos.** s/d. Disponível em: <http://www.direitonet.com.br/artigos/exibir/8772/Crimes-ciberneticos>. Acessado em 20 de agosto de 2016.

------ **Crimes cibernéticos.** s/d. Disponível em: <http://www.direitonet.com.br/artigos/exibir/8772/Crimes-ciberneticos>. Acessado em 20 de agosto de 2016.

DOWER, N.G.B **um novo mundo de criminalidades reais.** 2005. Disponível em: <http://www.jurisway.org.br/v2/dhall.asp?id_dh=785>. Acessado 20 de agosto de 2016.

FORENSE. **Fundamentos de direito penal informático.** 2003. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529>. Acessado 20 de agosto de 2016.

ISTOE. **Como se proteger de crimes virtuais.** s/d. Disponível em: <http://istoe.com.br/241403_COMO+SE+PROTEGER+DE+CRIMES+VIRTUAIS+/>. Acessado em 20 de agosto de 2016.

JORGE **crimesciberneticos.** 2013. Disponível em: <http://www.crimesciberneticos.net/2013/06/internet-e-privacidade.html>. Acessado 20 de agosto de 2016.

MOLES, Ramón J. **Territorio, tiempo y estrutura del ciberespacio.** s/d. Disponível em: <http://www.egov.ufsc.br:8080/portal/conteudo/crimes-virtuais-elementos-para-uma-reflex%C3%A3o-sobre-o-problema-na-tipifica%C3%A7%C3%A3o>. Acessado 20 de agosto de 2016.

OLHAR DIGITAL. **Qual a diferença entre Hacker e Cracker?** s/d. Disponível em: < http://olhardigital.uol.com.br/fique_seguro/noticia/qual-a-diferenca-entre-hacker-e-cracker/38024>. Acessado em 24 de setembro de 2016.