CONVIDADO

ideário

Revista Científica do
INSTITUTO IDEIA

O USO DAS REDES SURFACE E *HIDDEN WIKI* – UMA ANALISE DE PROBLEMAS DE CONSTRANGIMENTO E INJURIA DE SEUS USUÁRIOS

RENATO NOGUEIRA PEREZ AVILA (professorenato@hotmail.com) – Professor de Mestrado e Doutorado na Universidad San Carlos nas disciplinas de Técnicas de estatísticas e de Auditoria em Instituições Filantrópicas. Professor Titular de Pós-graduação Lato Senso no Instituto de Ensino Superior de Londrina na disciplina de Metodologia do Artigo Científico, membro do comitê de ética em pesquisa. Chefe do Departamento de Pesquisa do INESUL. Editor Chefe do Periódico Múltiplo Saber. Aluno do Programa de Pós-Doutoramento da Universidade Iberoamericana de Asunción – PY, em parceria com o Instituto IDEIA-BR.

RICARDO DE BONIS (ricardo@debonis.com.br) – Cirurgião-Dentista, Doutor em administração pela Universidade Americana – PY, Professor da Disciplina de "Ética na Pesquisa e na Produção Acadêmica" da Universidade Columbia Del Paraguay, Professor do curso de Pós-Doutoramento da Universidade Iberoamericana de Asunción – PY, em parceria com o Instituto IDEIA-BR.

RESUMO: Este artigo possui a intenção de utilizar diversos hardwares, softwares e experiências que jovens em nível universitário passam na Internet convencional e na rede *Hidden Wiki* da *Deep Web*. O trabalho se fez por uma pesquisa de campo com a aplicação de um questionário contendo perguntas inerentes a problemas financeiros e morais em diversos aplicativos, sites e fóruns existentes na *Hidden Wiki* e na Internet comum com a intenção de mostrar os aplicativos, sites, portais, redes sociais e ações onde pode existir algum tipo de constrangimento moral ou financeiro, comparando com isso, a realidade da segurança do usuário, quando o mesmo está na *Hidden Wiki* e na Internet comum, com a intenção de concluir as posturas de segurança necessárias.

PALAVRAS-CHAVE: Segurança de informações, *Deep Web*, Usuários de Internet.

RESUMEN: Este artículo tiene la intención de utilizar una variedad de hardware, software y experiencias que los jóvenes en el pase de nivel universitario en Internet convencional y Red oculta HiddenWiki y *Deep Web*. El trabajo fue realizado por una investigación de campo con la aplicación de un cuestionario que contiene preguntas inherentes a problemas financieros y morales en diversas aplicaciones, sitios web y foros existentes en el *Hidden Wiki* e en la Internet común con la intención de mostrar las aplicaciones, sitios, portales, redes sociales y las acciones que puede haber algún tipo de restricción moral o financiera, en comparación con por lo tanto, la realidad de seguridad del usuario, cuando está en la HiddenWiki en *Deep Web* y en Internetcomun, con la intención de completar las posturas de seguridad necesarias.

PALABRAS CLAVES: Seguridad de la Información, *Deep Web*, los usuarios de Internet.

REVISTA CIENTÍFICA DO INSTITUTO IDEIA – ISSN 2525-5975 / RJ / Revista nº 1 – ANO 6 (2017)

1. INTRODUÇÃO

O autor, através de uma pesquisa particular, iniciada no ano de 1997 e concluída em 2015, onde ocorreu uma busca, passando por diversas redes existentes dentro da *Internet*, permite que o mesmo fale, neste texto introdutório, que, pesquisar a a *Deep Web* é um trabalho complexo, pois, não se trata de um estudo simplesmente dentro na área das exatas, mas sim, o de abordar também algo antropológico, como é o caso desta pesquisa, pois, muitos anos se passaram, desde a chegada da *Internet* discada na cidade onde o mesmo reside, e foi somente em muitos anos de busca que o objetivo foi alcançado, a prova da existência da *Mariana´s Underground Web*.

Segundo (AVILA 2015), existem poucas fontes fidedignas sobre esse assunto, portanto, o referencial é extremamente diminuto existente na obra lida neste momento, isso se deve ao fato que, falando da *surface* da *Deep Web*, que comporta as extensões: *.onion, .i2P, .burble* e *.garlic*, existem conteúdos muito grandes com características especulativas, e, se tratando da *Mariana´s Underground Web*, absolutamente todo o conteúdo existente na *Internet* possui esta característica, o que dificulta deveras a busca de obras, livros, artigos e afins. O autor deste artigo é também o responsável por publicar um livro sobre o assunto, intitulado Deep Web A Internet que Não Está no Google, no mesmo, o conteúdo é totalmente confiável, fruto de anos de pesquisa, e, nele se encontra, entre diversos outros assuntos, o caminho para chegar-se na *Mariana´s Underground Web*.

Mesmo não sendo o foco deste artigo, faz-se mister esclarecer do que se trata a *Deep Web*.

A *Internet* comum, ou convencional, que é utilizada por pessoas de todo o mundo, através de buscadores, redes sociais, portais, sites, blogs, vlogs, aplicativos etc., possui somente, conforme (AVILA 2015), 20% de todo o conteúdo da *Internet*, pois, a censura que ocorre nos buscadores convencionais é sistemática e silenciosa, , existem, também conforme (SANTOS, MARCHI, 2013) inúmeras restrições existentes nos complexos algoritmos dos gigantes buscadores da Internet convencional, que resultam nesta ação. A *Deep Web* não se caracteriza em camadas, aliás, a grande diferença que a Internet possui para as outras redes de computadores utilizadas em massa, é que a mesma não é hierárquica, pois surgiu como mecanismo de defesa nos Estados Unidos da América.

> Estimativas baseadas em extrapolações de um estudo feito na Universidade da Califórnia em Berkeley em 2001, especularam que a *Deep Web* possui 7.500 terabytes de informação. Estimativas feitas por He et al.,em 2004, detectaram cerca de 300.000 sites da *Deep Web*. (HE, Bin, et. al., 2013)
>
> Também deve ser levado em consideração que, cerca de 14.000 destes eram da parte russa da Web em 2006. Em 2008, a web chamada "*Deep Web*", não referenciada pelos motores de busca representa 70% a 75% do total, ou seja, cerca de um trilhão de páginas não indexadas. (SHESTAKOV, 2011).

Nos dias atuais, os usuários da Internet, tanto na *surface* quanto na *Hidden Wiki*, não se dão conta do perigo que os mesmos se expõem durante a navegação (AVILA, 2015), os universitários, em nível de graduação, que foram fonte desta pesquisa, através do preenchimento do já citado questionário, se colocam expostos a inúmeros perigos, de cunho financeiro, quando adquirem em seu computador, *tablets* e celulares, *malwares* de todos os tipos, tanto os morais, como encontros marcados por aplicativos, quando navegam em fóruns, redes sociais e programas para *tablets* e celulares, comparando os que existem na Internet convencional, quanto na *Hidden Wiki,* ou seja, exposição a perigos virtuais oriundos de *malwares* e *peoplewares*, que podem causar constrangimentos pessoais e também resultar na ocorrência de mal funcionamento em programas e partes físicas dos aparelhos de acesso à Internet, principalmente em programas específicos que trabalham diretamente com a mesma, como no caso de browsers, servidores de e-mail, anti-vírus, *anti-malwares, firewalls* etc. (BERGMAN, 2000)

As ações de analisar os já citados perigos, tanto quanto as exposições pessoais que venham a causar constrangimentos ou oferecem perigo, como imagens roubadas e alteradas, vídeos e o roubo de dados pessoais, profissionais e de instituições financeiras como dados bancários, cartões de crédito e/ou débito, programas maléficos que se instalam nos aparelhos e enviam tudo que foi digitado, furto de senhas de sites, *blogs*, fóruns, portais e redes sociais, obtenções ilegais de arquivos pessoais que existem nos equipamentos. (SANTOS, MARCHI, 2013). Portanto, esta obra tem a finalidade de levantar e descrever analiticamente o problema de constrangimentos que podem ocorrer no tocante aos constrangimentos e injuria de seus usuários.

2. OBJETIVOS

O objetivo deste estudo foi o de analisar os problemas de constrangimentos e injurias dos usuários da Internet na sua navegação entre sites e aplicativos que são populares no Brasil.

Como objetivos específicos, este estudo intencionou:

Apontar quais são as vulnerabilidades das características das diversas posturas, locais, plataformas, programas, e, principalmente, endereços da Internet comum comparados com a *Hidden Wiki*;

- Identificar o funcionamento dos já citados locais e aplicativos no tocante a exposição das pessoas que podem oferecer perigo real para universitários;
- Buscar dados sobre a navegação na *surface* da Internet nos equipamentos de acesso a mesma, para analisar, no marco antropológico, onde existem um maior risco de constrangimento e exposição dos usuários.

3. METODOLOGIA

Uma investigação, qualiquantitativa e prospectiva, que buscou acadêmicos de diversos cursos de graduação, que não tinham feito nenhum tipo de pós-graduação,

REVISTA CIENTÍFICA DO INSTITUTO IDEIA – ISSN 2525-5975 / RJ / Revista nº 1 – ANO 6 (2017)

em curso das mesmas e devidamente matriculados na Instituição onde a pesquisa foi realizada, oriundos dos cursos de bacharelado em administração de empresas, bacharelado em ciências contábeis, tecnologia em radiologia, tecnologia em gestão financeira, tecnologia em gestão de recursos humanos, tecnologia em logística, licenciatura e bacharelado em educação física, farmácia e enfermagem.

Segundo o critério de inclusão e exclusão, foi adotado que a graduação foi o único ponto que foi estudado para a confecção deste estudo.

O questionário possui doze perguntas, cada uma sobre um procedimento de segurança de ações ou programas, existentes, uns na *Internet* convencional e na *Hidden Wiki*, com o objetivo de analisar as ações de proteção dos usuários quando se expõem em ambos os ambientes com a finalidade de observar onde se encontram os verdadeiros perigos, tanto morais quanto financeiros.

Desta amostragem, o acadêmico mais novo possui 17 anos e o mais velho, 51 anos de idade, o número de mulheres foi de 119 e os homens foram de 91 alunos.

A grande maioria é composta por pessoas solteiras, seguidas por pessoas casadas, seguidos por divorciados e um viúvo. Deste levantamento, 66 tem filhos e somente 14 acadêmicos estão desempregados, nesta mesma ótica, absolutamente nenhum se encontra em um sub-emprego. Muitos deles são profissionais liberais, autônomos, concursados, trabalhando em empresas, comércios e indústrias e afins.

Obviamente, a maioria dos acadêmicos mora em Londrina, mas existem acadêmicos oriundos de cidades até 110 quilômetros quadrados da cidade sede da Instituição estudada.

4. AMOSTRAGEM

O questionário foi aplicado em 210 acadêmicos de graduação, sendo:

CURSO	MASCULINO	FEMININO
Bacharelado em Administração de Empresas	31	43
Bacharelado em Ciências Contábeis	06	07
Bacharelado em Farmácia	04	00
Bacharelado em Enfermagem	06	30
Tecnologia em Gestão Financeira	03	06
Tecnologia em Radiologia	13	15
Bacharelado e Licenciatura em Educação Física	11	04
Tecnologia em Recursos Humanos	03	13
Tecnologia em Logistica	14	01

5. ANALISE E DISCUSSÃO DOS RESULTADOS DA PESQUISA

Conforme dito anteriormente, o questionário possui doze perguntas, sendo de opções, onze, mais a última é um enunciado para ser respondido em texto. Cada pergunta fala sobre um procedimento ou aplicativo, que podem causar problemas

morais e financeiros, o mesmo possui cabeçalho com os campos: nome, idade, RG, curso, empresa onde trabalha, estado civil, sexo, filhos, e quantidade de filhos caso anterior afirmativo.

5.1. PRIMEIRA QUESTÃO

A primeira questão tratou de um aplicativo para celulares que, uma vez instalado, o mesmo busca outras pessoas que possuem o mesmo aplicativo com o uso de um *Global Position System* (GPS), que estão próximos, a cada foto, existe a opção de negar ou aceitar, antes, ele permite que a pessoa que está vendo em seu programa, os dados do outro por uma grande rede social, uma vez observado, a outra pessoa recebe um aviso de quem está perto e lhe achou atraente, onde ele pode analisar da mesma forma e responder ou mandar uma mensagem, onde ambas podem conversar e marcar encontros, públicos ou privados, onde algo ruim pode ocorrer.

Pelo questionário, 15 mulheres responderam que já usaram este aplicativo, e, para 3 delas a experiência foi ruim, e para 12 delas, foi uma experiência boa, a faixa etária variou de 19 anos para as mais novas e a mais velha possui 32 anos, mas, impera uma média de 20 a 24 anos, realmente bem jovens se submetem a correr este risco sem saber do que pode ocorrer.

Quanto aos homens, 16 usaram o aplicativo, o mais novo, tinha 19 anos e o mais velho tinha 33 anos de idade, mas, a idade média foi maior que das mulheres, a média foi de uma faixa etária maior, variando entre 27 a 28 anos de idade, e 5 deles alegaram ter sido uma experiência ruim.

A existência deste aplicativo é de conhecimento de um número médio dos que receberam o questionário, o que era de se esperar, pois os jovens preferem se comunicar através de um aplicativo de mensagens instantâneas muitíssimo popular no Brasil, usando uma grande rede social.

Uma pesquisa noticiada no site O Globo, em seu site oficial, http://oglobo.globo.com/sociedade/tecnologia/pesquisa-revela-que-30-dos-usuarios-do-tinder-sao-casados-12-ja-estao-num-relacionamento-16081887, acessado em 30 01 2017, realizada pela GlobalwebIndex, revela um resultado um tanto inusitado, nela, levantou se que 30% dos usuários deste aplicativo são casados e 12% se encontram em um relacionamento fixo, segundo a pesquisa, apenas 54% dos entrevistados eram solteiros, foi verificado que, existia uma maior amplitude, ela foi realizada em 24 de abril de 2016, onde o referido software possuía 47.000 usuários.

5.2. SEGUNDA QUESTÃO

A segunda questão foi sobre problemas que existem em sites bancários, principalmente os ataques de negação de serviços, também conhecidos como *denialofservices*, onde as pessoas que atacam o site bancário com o envio de vários pacotes de dados que sobrecarregam os portais de tal maneira que, os portais de bancos saem do ar, então, o responsável pelo ataque, insere, linkado no endereço eletrônico do banco, um portal clone onde os desavisados acabam por inserir seus dados no site e acaba por ter transtornos, mesmo os bancos sendo responsabilizados. Além disso, podem existir problemas bancários oriundos de erros dos clientes.

REVISTA CIENTÍFICA DO INSTITUTO IDEIA – ISSN 2525-5975 / RJ / Revista nº 1 – ANO 6 (2017)

Entre os jovens do sexo masculino, foram 5 os que tiveram problemas com sites bancários, entre eles, 4 tiveram seus problemas resolvidos, e 1 não conseguiu resolver o mesmo, passado então pelo constrangimento e prejuízo no uso de sites bancários.

No caso das mulheres, também foram 5 as pessoas que alegaram terem tido problemas com sites de bancos, portanto, levando em consideração que o número de mulheres que responderam ao questionário foi maior do que os homens, então elas foram menos afetadas com este problema. Outro ponto que deve ser lembrado é que todos os 5 problemas levantados por elas foram resolvidos.

Existem dados, publicados no portal do jornal O Estado de São Paulo, de autoria de (TOZETTO, 2015) que notícia que o cibercrime causa, anualmente, um prejuízo para instituições bancarias de um bilhão e oitocentos milhões de Reais.

5.3. TERCEIRA QUESTÃO

A terceira questão foi o uso de sites de leilões e vendas, brasileiros e de outros países, esses endereços permitem que pessoas físicas possam comprar de pessoa física e também de pessoa jurídica, funcionam como venda direta e como leilões de prazos estabelecidos onde leva o item quem deu o lance maior, existem nesses sites, produtos novos e usados, e de todos os tipos, desde papel de carta e colecionáveis até veículos e imóveis.

Comprar de pessoas físicas pode trazer problemas com mais frequência do que de pessoas jurídicas, mas um sistema de confirmação de que tudo deu certo é realizado tanto entre o vendedor, quanto pelo comprador, oferece uma segurança no negócio, pois as reputações de ambos estão em jogo.

Entre os relatório, os homens, foi levantado 21 problemas entre sites de leilões e vendas com pessoas físicas e jurídicas, dentre eles, 13 conseguiram resolver o problema e 8 não conseguiram resolver o mesmo. Interessante o fato que, um número grande de pessoas usam sites deste tipo.

Já as mulheres somaram 26 problemas em sites de leilões, sendo que em 14 deles houve uma resolução e 12 não conseguiram resolver, todas elas usaram um site de leilões e vendas que também existe no Brasil, nenhuma compra neste tipo de sites (de leilões) no estrangeiro. Muito interessante que, mesmo a resposta sendo optativa, no pequeno espaço em branco, 5 mulheres resolveram escrever, em breves palavras o que ocorreu de errado, buscando desabafar o prejuízo, mesmo se tratando de quantias pequenas.

Em sua página no jusbrasil, (SANTOS, 2016) afirma que, *"as principais causas de problemas em sites de vendas e leiloes são, a ingenuidade, a escassa atenção e a ignorância técnica são as principais posturas que favorecem problemas neste tipo de negociação, ele afirma que, contas abertas com documentos falsos com a intenção de receber pagamento adiantado e depois sumir*

do contato com o cliente, adultério em páginas, para se parecer como um comerciante com boa reputação, triangulação, onde pega números de contas de usuários, oferecer serviços e produtos inexistentes são os golpes mais comuns". Os mesmos problemas contidos nessa questão do questionário aplicado nessa pesquisa.

5.4. QUARTA QUESTÃO

A quarta questão abordou o auto preenchimento nos cabeçalhos onde se encontra o endereço de e-mail do destinatário da mensagem, de fato, este recurso é muito útil, mas, entretanto, existem inúmeros e-mails em caixas de correio eletrônico existem endereços que começam com as mesmas letras, o que pode resultar, se não enviado com atenção, para a pessoa errada, causando problemas pessoais e profissionais.

Entre as mulheres, foi constatado que 13 delas cometeram esse deslize, mas em apenas 1 dos casos, o problema não foi resolvido.

Todos os casos foram ocorridos com destinatário de emprego e negócios, uma das que se encaixaram neste grupo, em um pequeno espaço em branco, respondeu que enviou um segundo e-mail e conseguiu resolver o problema.

Entre os homens, foram afirmativas as respostas de 13 deles, e, em 2 casos, o erro não pode ser contornado. De fato, o autor previa, para este assunto, um número menor de ações erradas sobre esta tecnologia de comunicação, isso se deu pelo fato que, impossível não usar um e-mail pessoal e um e-mail laboral.

Existem conteúdos que nunca devem ser postados, como mensagens motivacionais as 6 horas da manhã, festejos pessoais, correntes, mensagens em caixa alta, imagens e filmes eróticos, com nudez e pornográficos, fotos fortes. Não precisa de uma mensagem ser pessoal para ser ofensiva.

5.5. QUINTA QUESTÃO

A quinta questão se iniciou alertando o fato que, o que se escreve não se volta, e ela abordam as postagens e constrangimentos que podem ocorrer em um antigo chat, onde as pessoas se expõem onde não existe nenhum tipo de controle, as postagens em uma grande rede social e em um popular programa de mensagens instantâneas utilizado em massa nos telefones celulares aqui no Brasil.

Entre as mulheres, 45 afirmaram ter tido algum constrangimento utilizando esses portais e aplicativos, sendo que, 14 delas conseguiram resolver os problemas causados, mas, a maioria, que representa 31 mulheres, não conseguiram reverter o problema, de fato, nesta questão, era de se esperar que houvesse um número maior de perigos reais e constrangedores.

Já os homens foram 38 que alegaram terem tido problemas no uso destas ferramentas, e, dentre eles, 20 não conseguiram resolver o problema gerado ou resultado de suas postagens. Vale lembrar que, em programas de mensagens em tempo real, é possível que o usuário se comunique com várias pessoas ou grupos de uma só vez.

REVISTA CIENTÍFICA DO INSTITUTO IDEIA – ISSN 2525-5975 / RJ / Revista nº 1 – ANO 6 (2017)

De acordo com (LEÃO, 2015), a intimidade deve ser levada em consideração para evitar aborrecimentos, principalmente por mensagens de áudio. Ela ainda cita o fato que se deve pensar bem antes de redigir e postar mensagens e recursos gráficos para evitar transtornos e arrependimentos, observar os horários para enviar conteúdo, destacando muito cedo ou muito tarde, observar bem os emoticons e não inserir os mesmos em grande quantidade, fotos de dias de rotina devem ser evitadas, mas as de viagens e eventos são mais aconselháveis. A mesma afirma que, mensagens em grupo são mais delicadas, pois geram conflitos com mais regularidade.

5.6. SEXTA QUESTÃO

A *Deep Web* é o assunto da sexta questão, na mesma, é questionado o maior perigo referente a segurança de ataques e de *downloads* contendo arquivos maliciosos.

Foram 7 os homens que tiveram este problema, sendo que 2 deles não conseguiram resolver os mesmos. De fato, o autor esperava uma quantidade menor deste tipo de problemas, já que navegadores de *interface* amigável que se encontram na *Deep Web* foram desenvolvidos há pouco tempo, mas, mostrou que as pessoas estão perdendo o medo de navegar em redes pertencentes à *Deep Web*.

Quanto as mulheres, 12 afirmaram que já passaram por este transtorno, sendo que 3 delas não conseguiram reverter o problema causado. Isso existe por conta de conhecimento em segurança, pois, os acadêmicos que responderam esta pesquisa desconhecem a segurança além do *anti-virus,* como outros softwares tipo *anti-trojanse firewals.*

(AVILA, 2015) Afirma que, se proteger na *Deep Web*, é necessário o uso de um servidor de *proxi*, utilizar 2 anti vírus, e procurar conhecimento de segurança especifico para a *Deep Web*, mas, os sites que possuem grandes perigos para *hardwares* e *softwares*, não serão acessados, pois o usuário comum não vai encontrar os *links* dos mesmos ou sites que só pessoas autorizadas podem acessar os mesmos.

5.7. SÉTIMA QUESTÃO

Existem inúmeras moedas virtuais, mas o *bitcoin* é a mais popular de todas, mesmo tendo um supervalorizamento junto as moedas convencionais, ela foi adotada, pois seu criador sumiu desde a implantação da mesma, um *bitcoin* custa aproximadamente duzentos e quarenta Reais.

Ele pode ser adquirido por cartão de credito, e sua principal característica é que ele não possui código de rastreio, bem como, nenhum outro registro.

Como esperado, nenhum dos que responderam o questionário, compraram *bitcoins*, de fato, o uso desta moeda não está ligado em compras realizadas na Internet, tanto em produtos quanto em serviços. O *bitcoin* é usado fora da internet convencional.

Bitcoin é o termo tendência do momento. A cada dia pipocam novas notícias sobre a moeda digital: entre os mais recentes, temos a abertura de uma loja virtual que trabalha com pagamentos exclusivamente em Bitcoin, a BitcoinShop.us; a chegada de caixas eletrônicos de Bitcoins, que seriam como casas de câmbio automatizadas que permitiriam saques de Bitcoins em dinheiro e

como a compra de novas moedas através de depósitos financeiros na própria máquina; e a inclusão do termo no Dicionário Oxford, um dos mais importantes do mundo.O entusiasmo com a novidade, no entanto, pode ser danoso. Existem relatórios de entidades financeiras, como o Banco Central Europeu, que mostram que o Bitcoin tem bastantes pontos em comum com esquemas de pirâmide, também conhecidos pelo nome de "marketing multinível". Perceba, não estamos falando que comprar Bitcoin seja o mesmo que investir no TelexFree, mas é preciso estar consciente de que a Bitcoin ainda é uma moeda em desenvolvimento, sem controle de governos. Por isso é preciso estar ciente de que vários problemas podem acontecer, como os roubos ou quem sabe uma brusca desvalorização da moeda, que pode acarretarem perdas financeiras pra quem quis usar as Bitcoins como forma de investimento. (LAFLOUFA, 2015).

5.8. OITAVA QUESTÃO

A oitava questão foi preparada para pessoas que usam aparelhos móveis, pois existe um *plugin* para acessar a *Deep Web* através dos dois mais populares sistemas operacionais para celulares utilizando o navegador TOR. A inclusão desta pergunta foi pelo motivo que esses aparelhos ganham, cada vez mais, popularidade entre as pessoas de todas as idades e origens.

Foram 8 homens que alegaram usar o TOR para acessar a *Hidden Wiki* e 4 deles alegaram que seus dispositivos móveis foram afetados. Já no caso das mulheres, 5 utilizaram o TOR pelo dispositivo móvel e nenhuma delas teve danos em seus equipamentos.

O autor esperava um número maior de pessoas que acessam a *Deep Web*, pois esse tipo de equipamento é extremamente popular. Importante citar que, em 4 questionários, esta questão ficou em branco, possivelmente pelo fato de desconhecerem essas ações e utilizações.

5.9. NONA QUESTÃO

O assunto desta pergunta foi sobre os *cookies* que as empresas e uma grande rede social para espionar os gostos dos usuários e depois utilizar os dados para facilitar sua busca, mas com intenção de vender produtos e serviços específicos baseados nesses banco de dados. Entre as mulheres, 66 delas afirmam ter percebido essa prática, sendo que somente 6 delas cancelassem suas contas em sites e rede social. Já entre os homens, 44 alegaram ter percebido, de maneira simples, esse fenômeno, mas, somente 2 deles cancelaram suas contas. Observa-se aqui que, a força desta rede social é imensa, pois, tudo gira em torno dela, por isso, escapar é muito difícil.

5.10. DÉCIMA QUESTÃO

A décima questão falou do contrato virtual de uma grande rede social ao qual todos devem ler e aceitar para poder criar uma conta, no conteúdo do mesmo, tudo que é postado, como textos, imagens, fotografias, vídeos e afins, são de propriedade eterna e exclusiva desta rede social, e, no caso negativo, foi perguntado para os alunos que, por este motivo, eles cancelariam as suas contas nesta rede social.

REVISTA CIENTÍFICA DO INSTITUTO IDEIA – ISSN 2525-5975 / RJ / Revista nº 1 – ANO 6 (2017)

Entre os homens, 13 alegaram que leram por completo este documento, mas, somente 3 deles levariam isso em conta para cancelar seu perfil, o restante não se submeteram a cancelar sua conta.

Já as mulheres, 14 delas leram inteiro este contrato, e, dentre elas, 6 estariam dispostas a cancelar seus perfis. No caso das mulheres, imagens em redes sociais são mais constrangedoras, mas, mesmo em maior número de entrevistadas que os homens, foram poucas as que tiveram esta atenção.

5.11. DÉCIMA PRIMEIRA QUESTÃO

A questão fala do primeiro buscador de *Deep Web* que possui os atrativos gráficos de um buscador comum, ele pode ser usado na *Hidden Wiki* e na Internet convencional, a questão era se o mesmo era seu principal buscador.

Entre os homens, 11 alegaram que usam este buscador como seu principal, mas que possuem problemas quando navegando na Internet convencional, sites como servidores de e-mail e demais endereços de compras ou redes sociais não permitem o acesso, e solicitam a mudança de senha quando usam outro buscador para acessar esses tipos de endereços eletrônicos.

Já entre as mulheres, 2 somente usam este buscador como principal, pois possuem curiosidades na *Hidden Wiki*, e que a interface deste buscador é muito amigável.

5.12. DÉCIMA SEGUNDA QUESTÃO

Esta questão foi elaborada para ser respondida em um pequeno texto, e solicitava que, se a pessoa já tivesse algum problema na Internet em geral moralmente, financeiramente ou intelectualmente, que ela, caso afirmativo, escrevesse em texto.

Entre os homens, haviam uma reclamação de constrangimento com uso impróprio de imagens, alega o acadêmico que, foi em pequena escala, dois que reclamaram de compras, um em um site brasileiro e outro em um site da China, o primeiro recebeu um produto que não fazia jus a descrição do mesmo no site e o outro não recebeu o produto.

Com as mulheres, uma alega que foi vítima de seus concorrentes quando ela inseriu produtos e serviços em uma grande rede social, sofreu críticas sobre os produtos e sobre os preços, outra disse que teve sua conta bancária invadida, mas o banco estornou o prejuízo. Outra, em uma já desativada rede social, disse que teve suas fotos acessadas e usadas em sites de conteúdo adulto, outra por comprar em um site de equipamentos esportivos e o boleto gerado era de um valor maior do que era mostrado no site, a empresa disse que foi cometido um erro e cancelou a compra devolvendo seu dinheiro, outra, por fim disse foi infectada por um trojan no seu *pendrive* oriundo de *download* e o mesmo ocorreu, em outro tempo, no seu *smarthphone*.

6. CONSIDERAÇÕES FINAIS

De fato, estudar a *Deep Web* dentro das ciências exatas é algo extremamente complexo, mas, avaliar, com os recursos atuais, o uso da *Deep Web* envolvendo pessoas em nível de graduação vem crescendo, mas ainda é pequeno, por isso, as perguntas falavam da *surface* também, pois a intenção era comparar ambas, como escrito nos objetivos, analisar o uso de programas, na *surface* e na *Hidden Wki,* na comparação de ambas e focado nos problemas encontrados em diversos aplicativos e softwares oriundos da rede convencional e da *surface* da *Deep Web*.

A exposição de pessoas a esses *malwares* oriundos de redes sociais, fóruns, aplicativos, bancos, portais, existe conhecimento por parte da mesma, mas são menores os riscos devidos a tecnologias ligadas a criptografia de Internet, então, as vulnerabilidades são realizadas por programas de segurança e pelas próprias empresas que fornecem o serviço.

Os voluntários, usam sites e aplicativos com conhecimento mediano, e acabam pondo em risco muitas coisas, os jovens desconhecem perigos que os rodeiam por todas as partes, incluindo a Internet, por isso aprendem em sala de aula ou por auto didática rápido, ao contrário, os mais velhos e idosos demoram para aprender, pois conhecem o perigo.

Compras e vendas são facilitadas pela Internet, tanto de pessoas físicas quanto jurídicas, mas transtornos existem nos dois, e existem compras em outros países que dão errado também, o que dificulta muito a resolução do problema.

E, por fim, a navegação na *Hidden Wiki* ficou mais segura, logo será equivalente à da Internet convencional.

Fato é que as pessoas se expõem em maior perigo na Internet convencional do que na *Hidden Wiki*, isso se dá pelo fato que as pessoas não usam a *Deep Web* com frequência menor ou não a conhece.

Nos bate papos existentes na Internet convencional, existem trocas de imagens de conteúdo erótico e pornográfico, onde não existe nenhuma dificuldade para os menos desavisados entrarem em contato com outras pessoas em encontros pessoais, isso ocorre desde o início da Internet. Importante citar também que, nos telefones celulares, existem aplicativos que possibilitam esta exposição ao perigo.

Os bancos devem ser utilizados presencialmente, pois, o uso do caixa eletrônico e o acesso on-line podem resultar em prejuízos irreversíveis.

O que mais preocupa os mesmos são vazamento de imagens, percas de senhas e compras não finalizadas, pois causam transtornos que, muitas vezes, não são resolvidos.

No questionário, foi apresentado o fato que, mesmo com probabilidade de envolvimento de problemas oriundos de posturas, sites, programas, e, principalmente, endereços da Internet, é comum comparados com a *Hidden Wiki*, pelo fato dos entrevistados utilizarem mais a *Internet* comum que a *Hidden Wiki*, os problemas são maiores na mesma.

Quanto aos riscos de constrangimento e exposição dos usuários, sem dúvida, se encontram em todos os programas e endereços eletrônicos abordados, mas é no aplicativo para dispositivos moveis que os maiores problemas ocorrem com frequência maior, obviamente, pelo fato que o mesmo é amplamente utilizado.

Por fim, com a chegada da estética em buscadores e domínios na *Hidden Wiki*, a navegação na mesma está, rapidamente, perdendo suas características que amedrontam os usuários comuns, portanto, a *Hidden Wiki*, está começando a ser uma concorrente, com conteúdo não legalmente proibido, a *Internet* convencional, pois os conteúdos criminosos estão, fora dos buscadores da *Hidden Wiki*, onde eles não possuem acesso e/ou conhecimentos não significativos de como encontrar os mesmos, pois, é claro que todo crime deixa rastros, e são necessários conhecimentos, muito além de saber usar um browser especifico para a *Deep Web* em seu buscador de interface mais amigável, é necessário conhecimento especifico. A *Internet* convencional apresenta mais riscos que a *Hidden Wiki* pois é muito mais utilizada.

Concluindo, os softwares estudados nessa obra, oferecem, como descrito nos enunciados do questionário, perigos que foram listados neste estudo e nesta conclusão , são reais e presentes, pois este artigo abordou os mais utilizados softwares e serviços no Brasil, e todos os citados, oferecem problemas morais e financeiros, pois as pessoas não tem uma ideia do funcionamento de seus programas de segurança, como firewalls e anti trojans e vírus, além de desconhecer fatos relacionados as posturas de navegação com segurança, em virtude deste fato, este texto demonstrou, em suas questões que, resultaram no fato que, em pelo menos uma questão, tiveram um problema, de tamanhos diferentes, alguns, como escrito, não puderam ser resolvidos e foram assimilados.

7. REFERÊNCIAS BIBLIOGRÁFICAS

AVILA, Renato Nogueira Perez. **DEEP WEB – A Internet que Não Está no Google.** Rio de Janeiro. CiênciaModerna. 2015.

- BERGMAN, Michael K**. The Deep Web – Surfacing Hidden Value.** S. I. BrightPlanet LLC. 2000.
- GlobalwebIndex. **Pesquisa Revela que 30% dos Usuários do Tinder são casados e 12% já estão num Relacionamento Serio.** Disponível em: http://oglobo.globo.com/sociedade/tecnologia/pesquisa-revela-que-30-dos-usuarios-do-tinder-sao-casados-12-ja-estao-num-relacionamento-16081887. 20016. (sic) (acessado em 31/01/2017).
- HE, Bin; ET.al. **Accessing the Deep: A Survey.** Communications of the ACM (CACM) 50. 94 TO 101. DOI 10.1145. 1230819.1241670. 2013.

- LAFLOUFA, Jacqueline. **Bitcoin: Modinha, Futuro Econômico ou um Péssimo Negócio?** Disponível em: https://tecnoblog.net/140321/bitcoin-moda-futuro-economico-ou-mau-negocio/ 2015 . (acessado em 01/02/2017).
- LEÃO, Celia. **Aprenda a Evitar Saias Justas com Classe.** Disponível em: http://delas.ig.com.br/comportamento/2015-02-12/micos-e-piores-erros-ao-usar-o-whatsapp.html . 2015 (acessado em 01/02/2017).
- SANTOS, Carlos Henrique Aguiar dos; MARCHI, Késsia Rita da Costa. **O Que a Deep Web Pode Oferecer Além da Surface Web.** Unipar Universidade Paranaense. Paranavaí. Disponível em: http://web.unipar.br/~seinpar/2013/artigos/Carlos%20Henrique%20Aguiar%20dos%20Santos .pdf. 2013. (acessado em 30/01/2017).
- SANTOS, Paulo Roberto Vieira Gregorian dos. **Golpes nos Sites de Vendas, Anúncios e Leilões Virtuais.** Disponível em: http://paulorobertogregori.jusbrasil.com.br/noticias/232777316/golpes-nos-sites-de-vendas-anuncios-e-leiloes-virtuais. 2016 (acessadoem 31/01/2017).
- SHESTAKOV, Denis. **Sampling the National Deep Web.** Proceedings of the 22nd. International Conference on Database and Expert Systems Aplications. DEXA. Springer. P. 331 to 340. 2011.
- TOZETTO, Claudia. **Cibercrime faz Bancos Perderem R$ 1,8 Bilhão.** Disponível em: http://link.estadao.com.br/noticias/cultura-digital,cibercrime-faz-bancos-perderem-r-18-bilhao,10000028721 2015. (sic) (acessado em 31/01/2017).

8. NOTAS BIOGRÁFICAS

Renato Nogueira Perez Avila

Graduado em Tecnologia em Processamento de Dados pela Universidade Paranaense FACCAR, possui Graduação em Licenciatura Plena em Informática pela Universidade Tecnológica Federal do Paraná UFTPR, Especialização em Ciência da Computação pela Universidade Estadual de Londrina UEL, Mestrado Profissional em Gestão de Redes de Telecomunicações pela Pontifícia Universidade Católica de Campinas PUCAMP, Doutorado em Ciência da Educação pela Universidad San Carlos USC e Pós Doutorando em educação pela Universidad Iberoamericana. Professor de graduação nas disciplinas de informática aplicada, lógica para o ENADE e métodos e técnicas de pesquisa no Instituto de Ensino Superior de Londrina, professor de Informática para cursos técnicos no Centro de Educação Integrado CEI. Professor Titular de Pós-graduação Lato Senso no Instituto de Ensino Superior de Londrina na disciplina de Metodologia do Artigo Científico, membro do comitê de ética em pesquisa. Professor de Mestrado e Doutorado na Universidad San Carlos nas disciplinas de Técnicas de estatísticas e de Auditoria em Instituições Filantrópicas. Chefe do Departamento de Pesquisa do INESUL. Tem experiencia na área de Ciência da Computação, Informática Aplicada e Inteligência Artificial e atua em Criptografia de Internet e Deep Web, Aprendizado, Educação, mercado de trabalho, comportamento e Informática, Lógica aplicada ao ENADE e Métodos e Técnicas de Pesquisa. Editor Chefe do Periódico Múltiplo Saber e autor de 14 livros pelas editoras Brasport e Ciência Moderna. Membro do CAS e da CPA e pesquisador responsável por provar a existência da Mariana´s Underground Web.

REVISTA CIENTÍFICA DO INSTITUTO IDEIA – ISSN 2525-5975 / RJ / Revista nº 1 – ANO 6 (2017)

Ricardo De Bonis

Cirurgião-Dentista, Doutor em administração pela Universidade Americana – PY, Professor da Disciplina de "Ética na Pesquisa e na Produção Acadêmica" da Universidade Columbia Del Paraguay, Aluno do Programa de Pós-Doutoramento da Universidade Iberoamericana de Asunción – PY, em parceria com o Instituto IDEIA-BR.