OS PRINCIPAIS CIBERCRIMES PRATICADOS NO BRASIL

Jefferson David dos Anjos Silva
Maria Vitória Ribas de Oliveira Lima

Universidade Pernambuco – UPE, jeffersonupeti@gmail.com; ribasolima@gmail.com

Resumo:

Este artigo relata os principais cibercrimes praticados no Brasil, como os criminoso abordam os usuários e quais os riscos que os usuários correm ao utilizar a internet. Os procedimentos metodológicos foram: levantamento bibliográfico, aplicação e análise de questionário online, através da plataforma google forms, com perguntas relacionadas a como o usuário utiliza a internet e quais os crimes que eles conhecem ou já sofreram. A expectativa é que esse resultado mostre a importância desse estudo para professores de licenciatura, pois só no processo educativo podemos formas pessoas mais conscientes e capazes de discernir sobre esses crimes e divulgar tais crimes no seu campo de atuação a educação básica evitando a propagação desses crimes.

Palavras-chave: Cibercrime, Internet, Usuário.

Introdução

Os usuários de internet estão cada vez mais expostos a possíveis cibercrimes, um crime que vem se tornando cada vez mais comum no Brasil. É importante ter conhecimento de como funcionam esses crimes, para que você possa se defender deles. Essa onda de crimes praticadas no Brasil cresceu 197% no ano de 2015, principalmente pelo aumento de usuários de aplicações na rede. O acesso cada vez mais facilitado aos serviços da Internet com o uso de computadores e dispositivos móveis expõem, numa escala jamais vista, os dados pessoais dos indivíduos e das organizações (GARTNER,2014).

Existem várias nomenclaturas utilizadas para designar um crime praticado através de um computador conectado à Internet, dentre elas pode-se citar: crimes virtuais, digitais, informáticos, fraude informática, delitos cibernéticos, cibercrimes, entre outras. (Humberto L. Antonelli; Emerson G. Almeida, 2011). A cibercriminalidade pode assumir muitas formas e pode ocorrer a qualquer hora e lugar. Os criminosos cibernéticos usam métodos diferentes segundo suas habilidades e seus objetivos. Compreender essa ampla variedade de crimes cibernéticos é importante visto que os diferentes tipos de crimes cibernéticos requerem atitudes diferentes para melhorar a segurança do seu computador e de suas informações.

As fraudes bancárias e de cartão de crédito, também geradas pelo roubo de dados pessoais, são os delitos digitais recorrentes no Brasil, mas os crimes cibernéticos se especializam e avançam ao mesmo tempo em que a tecnologia.

Com as recorrentes fraudes bancarias e de cartão de crédito, os atacantes podem vender essas informações no mercado negro, clonar informações, realizar adulteração de conta, contratos, assuntos financeiros, civis e pessoais. Dessa forma, é impossível saber o que o atacante fará com uma identidade roubada, as motivações visam quase que exclusivamente a obtenção de ganhos financeiros. (Agbinya et al., 2008)

O cibercrime (INTERPOL, 2015) é a atividade criminosa ligada diretamente a qualquer ação ou prática ilícita na Internet. Esse crime consiste em fraudar a segurança de computadores, sistema de comunicação e redes corporativas. As práticas associadas ao cibercrime podem ser exemplificadas pelas invasões de sistemas de computação e comunicação, a disseminação de vírus, a falsidade ideológica, a violação de informações confidenciais, as fraudes bancárias, a invasão de sites, hoax (do inglês, embuste ou farsa preparada com intuito de enganar pessoas), o roubo, a violação da propriedade intelectual, dentre outros. Todos esses crimes costumam ser viabilizados apenas por mais um, o RID (roubo de identidades digitais).

O termo cibercrime surgiu no final dos anos 90, em uma reunião do G-8 (composto pelos sete países mais ricos e industrializados do mundo, mais a Rússia). Nessa reunião, o objetivo principal foi encontrar ideias para a contenção de tais crimes, com a aplicação de técnicas e métodos mais eficientes de combate à realização de atividades ilícitas na Internet (o meio cibernético mais popular desde então). Já era evidente que sociedade tornar-se-ia cada vez mais dependente da Internet, aumentando a preocupação com a ocorrência de crimes pela rede mundial de computadores.

Ao longo dos últimos anos, os criminosos virtuais, armados com malwares sofisticados, roubaram centenas de milhões de dólares de contas bancárias online e de indivíduos em todo o mundo. Em alguns artigos recentes, já descreveram muitas vezes, que os dias de assaltar bancos pessoalmente ficaram para trás e agora isso acontece por detrás da tela de um computador conectado à Internet. Transações bancárias online são seu maior alvo, tornando predominante o malware bancário. Essa tendência consistente com o que relatamos dois anos atrás. (Mercês,2014).

A Internet pode ser uma ferramenta extremamente útil nos negócios, na escola ou no dia-a-dia. Ao mesmo tempo, a Internet pode tornar a vida de alguém um inferno, no caso dessa pessoa se tornar vítima de um crime virtual. Uma grande porcentagem da população

mundial que usa os computadores através da Internet, está ciente do cibercrime e das consequências que eles podem enfrentar se sucumbirem às armadilhas dos criminosos. As outras pessoas que não têm nenhuma pista sobre os perigos que enfrentam todos os dias por usar a Internet, devem ser esclarecidas, antes que seja tarde demais para elas.

Para se proteger contra os crimes cibernéticos você deve em primeiro lugar, saber quais os tipos de crime que existem. A Internet é uma infraestrutura complexa, na qual os cibercriminosos criam cerca de 57 mil sites de scam a cada semana. Em 2008, haviam cerca de 10 milhões de vítimas de roubo de identidade, somente nos Estados Unidos, de acordo com um relatório da agence France Press. Os facilmente evitáveis crimes informáticos, atacam os usuários de computador através de vários métodos, tais como o uso de perseguição cibernética, assédio, invasão de privacidade, phishing e até mesmo sendo impostores online.

Este projeto tem como objetivo apresentar quais são os tipos de crimes praticados no brasil, e apresentar como os criminosos atacam, quais as técnicas que os criminosos mais utilizam, quais os alvos principais dos criminosos e apresentar as principais medidas preventivas ao problema de cibercrime.

Portanto pergunta-se: será que os usuários compreendem os riscos reais que estão correndo e o impacto caso sofram algum ataque cibernético?

Desta forma, nota-se a importância de o usuário entender os riscos que ocorre quando ele utiliza serviços fornecidos da Internet e como se precaver contra esses ataques.

Diante dos aspectos anteriormente delineados, este trabalho teve como objetivo geral evidenciar os principais cibercrimes praticados no Brasil e apresentar a importância desse estudo para professores de licenciatura, para que eles venham formar pessoas mais conscientes sobre isso e reduzir o índice de vítimas de cibercrimes. Para alcançar esta finalidade, os objetivos específicos foram definidos:

- Contextualizar os principais cibercrimes praticados no Brasil;
- Compreender onde os criminosos mais atacam;
- Compreender quais as técnicas e como eles abordam as vitimas;
- Selecionar estratégias para divulgar o estudo junto a professores e estudantes da educação básica em escolas públicas de Garanhuns.

1.Metodologia

No desenvolvimento do trabalho foi feito um levantamento bibliográfico, onde foram consultados os autores: Godoy (1995, 2006); Preti (2010).

De acordo com Preti (2010), fazer pesquisa não é acumular dados e quantificá-los, mas analisar causas e efeitos de maneira contextualizada no tempo e no espaço, dentro de uma concepção sistêmica. O mesmo autor afirma, quando se refere ao uso simultâneo da abordagem qualitativa e quantitativa, que "(...) esses dados são considerados mais ricos, globais e reais" (PRETI, 2010, p. 590).

Para Godoy (1995, 2006), a diversidade existente entre trabalhos qualitativos enumera um conjunto de características essenciais capazes de identificar uma pesquisa desse tipo, a saber, que ela compreende um conjunto de diferentes técnicas interpretativas que visam a descrever e decodificar os componentes de um sistema complexo de significados. Tem por objetivo traduzir e expressar o sentido dos fenômenos do mundo social; trata-se de reduzir a distância entre indicador e indicado, entre teoria e dados, entre contexto e ação.

O instrumento de pesquisa para levantamento de dados foi um questionário online, onde os sujeitos que foram entrevistados são pessoas que já sofreram cibercrime, ou conhecem algum incidente de cibercrime ou ouviram falar sobre. Para que se possa entender, quais são os crimes mais praticados, quais as formas que eles atacam, qual seu principal público alvo e o que as pessoas que sofrem esse tipo de ataque, fazem depois que o crime acontece.

Com os dados coletados do questionário, foi feita uma análise de conteúdo, onde analisamos as respostas dos entrevistados e observamos o que elas têm de semelhantes ou de destaque sobre o tema pesquisado.

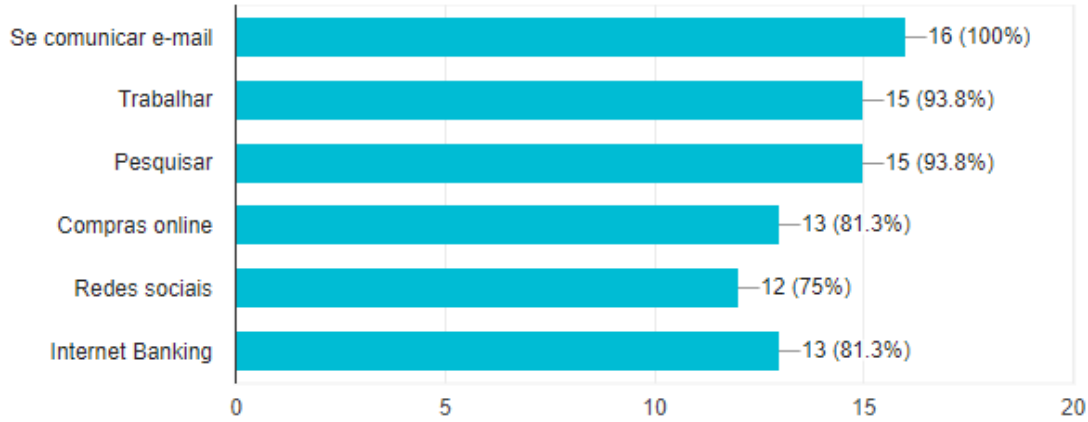
2.Resultados e Discussão

Através dos dados coletados, considerando os pontos levantados, as respostas foram para análise, tendo em mente as questões de pesquisa definidas. Dessa forma, esta seção descreve os resultados obtidos no questionário on-line.

2.1 Respostas da questão de pesquisa 01

Você utiliza a internet para quais finalidades? (Pode marcar mais de uma opção)

Figura 1. Porcentagem dos dados da questão 01



Na figura 1, percebemos que 100% dos entrevistados utilizam a internet para se comunicar via e-mail, 93.8% utilizam para trabalhar, 93.8% para pesquisar, 81.3% para fazer compras online, 75% utilizam para redes sociais e 81.3% para Internet Banking.

O modo em que as pessoas se comunicam e buscam informações mudou muito, principalmente ao que diz respeito à velocidade dessa comunicação.

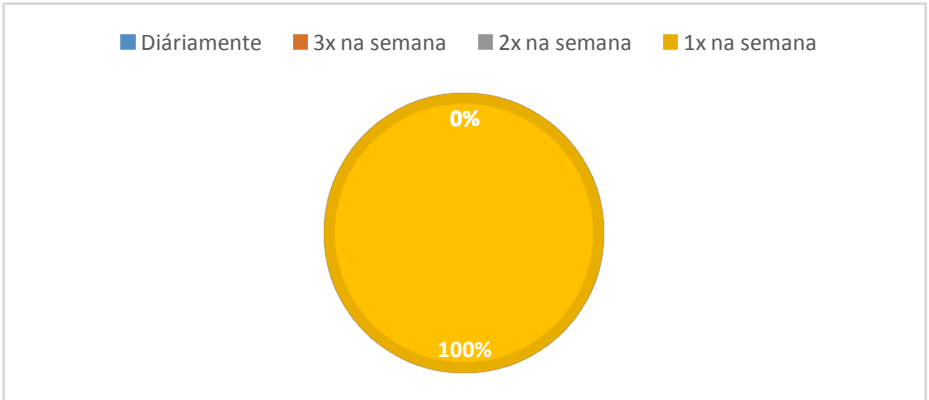
Hoje em dia temos acesso a notícias praticamente em tempo real, o mesmo acontece com conversas on-line, seja através somente de textos como também com o auxílio da webcam. Na internet temos acesso a praticamente tudo: informação imediata, cultura, política, entretenimento diversificado, compras online, internet banking, pesquisas, conteúdos destinados ao público adulto, enfim, inúmeros segmentos.

E essa diversidade e facilidade da busca de informação, está sob os olhos de atacantes, por isso sempre precisa estar muito atencioso ao que lhe aparece e ao que se busca, para não acabar caindo em algum golpe e sofrendo danos e/ou prejuízos.

2.2 Respostas da questão de pesquisa 02

Você acessa a internet com qual frequência durante a semana?

Figura 2. Porcentagem dos dados da questão 02



Na figura 2, temos 100% dos entrevistados que acessam a internet diáriamente.

A cada acesso estamos expostos a vírus e malware, eles estão espalhados por todos os lugares, onde talvez, menos imaginaríamos. Com apenas um clique você poderá se expor a riscos, como vírus, farsantes e conteúdos impróprios.

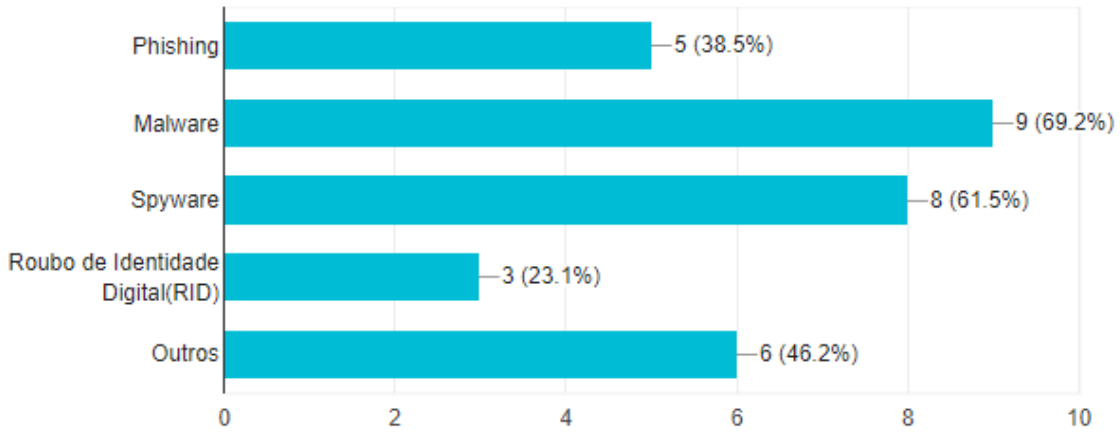
Mesmo com todas as informações que os meios de comunicação passam quase que diariamente, as pessoas parecem ignorar e continuam se expondo aos perigos. O mundo virtual tem o poder de prejudicar a vida de uma pessoa.

Na internet pode-se também haver inúmeras informações totalmente desnecessárias. É possivel publicar comentários sobre uma determinada pessoa, denegrir sua imagem,como também há roubo de identidade, phishing, calúnia, enfim, tantas outras coisas. O que não podemos esquecer é que os crimes virtuais ainda são poucos os solucionados, então, o melhor é se precaver.

2.3 Respostas da questão de pesquisa 03

Você já sofreu alguma tentativa de cibercrime ou conhece alguma? Quais?

Figura 3. Porcentagem dos dados da questão 03



Na figura 3, os 38.5% dos entrevistados relatam que já sofreram alguma tentativa de phisingou conhecem o ataque, 69.2% ja sofreram tentativa de malware ou conhecem, 61.5% ja sofreram tentativa de spyware ou conhecem o ataque, 23.1% com roubo de identidade digital e 46.2% ja sofreram ou conhecem outro tipo de ataque não listado.

O mundo, como sabemos, está cada vez mais conectado. Atualmente, a vida das pessoas está interligada à internet. As redes sociais, por exemplo, contam com milhares de usuários em todo o planeta. Há também quem não faz uso das famosas redes, porém, acessa a internet para outros serviços, como transações bancárias, compras online, entre outros.

Com o crescente número de usuários web há cada vez mais espertalhões tentando tirar proveito da situação para roubar alguma informação. Os meios mais comuns para isso é através do phishing (conversas ou mensagens falsas com links fraudulentos), spam (mensagens enviadas sem o consentimento do usuário) e malwares (softwares maliciosos instalados sem permissão do usuário, como vírus.

A prática de crimes virtuais ainda é muito comum justamente pela ilusão que o computador não poderá revelar a identidade dos evolvidos, além disso, muitos acreditam que a punição ainda é muito branda, ou mesmo inexistente.

Os usuários, por sua vez, ainda estão despreparados para reconhecer possíveis tentativas de fraudes, e assim acabam caindo em algum golpe. Por fim, por não saberem de seus direitos, acabam ficando calados perante os crimes praticados.

2.4 Respostas da questão de pesquisa 04

Você já foi lesado através de algum cibercrime? Quais foram seus prejuízos?

Quadro 1. Tabulação representativa das principais respostas da questão 04

	Descrição
Resposta 1	Sim, Roubaram dinheiro conta bancaria.
Resposta 2	Não, porque procuro acessar sites confiáveis.
Resposta 3	Já. Compras indevidas com meu cartão de crédito. Em valores baixos, mas ainda assim causando transtornos, pois tive que bloquear os cartões e ficar dias sem ter como fazer compras, aguardando o banco enviar nova via.
Resposta 4	Não, pois foi identificado de imediato.
Resposta 5	Não.

De acordo com os resultados apresentados no quadro 1, percebemos que uma maioria não sofreram prejuízos através de algum tipo de ataque cibernético, porem os que ja foram lesados, tiveram como prejuízo roubo de dinheiro em conta bancaria e compras indevidas com o seu cartão de crédito.

Primeiramente devemos lembrar que todo e qualquer crime praticado na internet possui leis que os representam. Deste modo, em nenhuma hipótese a melhor alternativa é ficar calado. Se você caiu, mesmo sem querer, em qualquer golpe pela web, ou mesmo foi vítima de qualquer situação desfavorável em uma rede social, lembre-se há leis que amparam a sua situação. Muitas pessoas também são chantageadas porpessoas, no geral, conhecidos, ex-

namorados, ex-maridos com a divulgação de fotos íntimas na rede, saiba que, mesmo que a divulgação não seja feita, o crime está estabelecido, então, o melhor é denunciar.

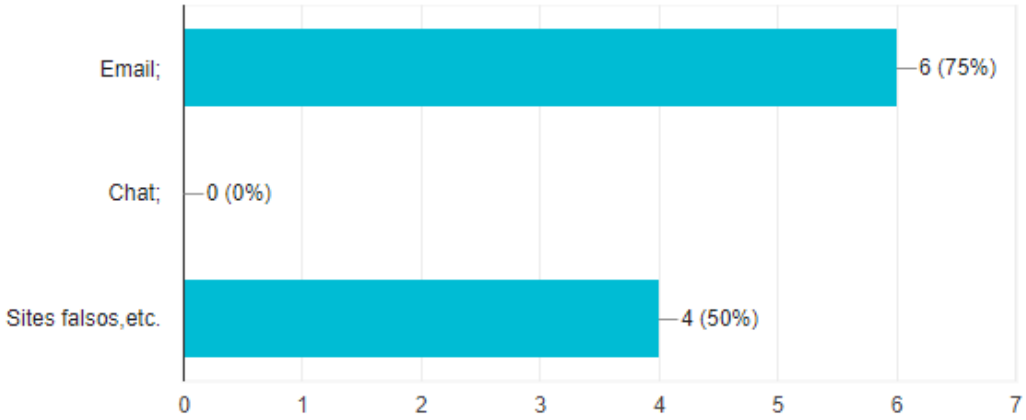
O primeiro passo, após ser vítima de qualquer crime virtual, seja qual for a modalidade, é procurar uma Delegacia Especializada em Crimes Eletrônicos. Caso não exista em sua cidade, a denúncia pode ser feita em qualquer outra Delegacia.

Após,o ideal é procurar um advogado especializado em Direito Digital, para que o profissional possa guiar da melhor forma a vítima desse tipo de crime.

2.5 Respostas da questão de pesquisa 05

Como o criminoso lhe abordou?

Figura 4. Porcentagem de dados da questão 05



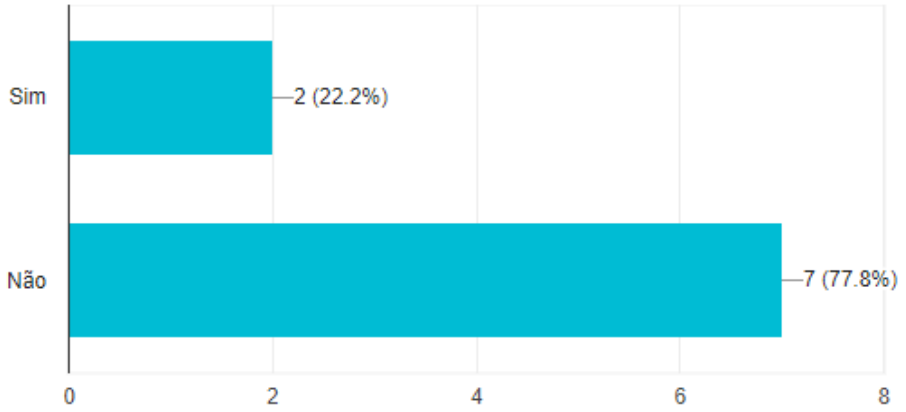
Na figura 4, os 75% dos entrevistados alegam que os criminoso lhe abordaram através de emails e 50% dos entrevistados dizem que foram abordados através de sites falsos.

Eles estão por toda parte: programas maliciosos (cavalos de troia, worms, spywares) e golpes virtuais (phishing, pharming, fraudes). Ao perceber algo estranho em sua máquina, a primeira coisa a fazer é desconectá-la da internet. Se o dispositivo for pessoal, entre em contato com o seu provedor. Se for no trabalho, alerte o departamento de Tecnologia da Informação (TI).

2.6 Respostas da questão de pesquisa 06

Você registrou boletim de ocorrência?

Figura 5. Porcentagem de dados da questão 06



Na figura 5, os 22.2% dos entrevistados que sofreram algum cibercrime registram boletim de ocorrência e 77.8% dos entrevistados alegam que não fazem boletim de ocorrência quando sofrem algum cibercrime.

Em todos os casos, é de extrema importância registrar um boletim de ocorrência, para que a denúncia seja apurada. Além de ajudar a prevenir ações do tipo no futuro, você tem mais chances de ser ressarcido. Mesmo que no Brasil haja poucas delegacias de polícia especializadas em crimes eletrônicos, qualquer DP é obrigada a atender os casos ou encaminhá-los aos postos apropriados.

2.7 Respostas da questão de pesquisa 6.1

Porque?

Quadro 2. Tabulação representativa das principais respostas da questão 6.1

	Descrição
Resposta 1	Recebe devolução.
Resposta 2	Não precisou , porque busquei esclarecimentos com instituições para nada responder , visto serem improcedentes comunicações realizadas pelas referidas instituições e cessaram os emails.
Resposta 3	Não houve danos e/ou prejuízos.
Resposta 4	Não houve realização do fato com sucesso.
Resposta 5	Porque consegui sustar os pagamentos junto ao banco e a central de segurança do Bradesco disse que iria cuidar de tudo.

De acordo com os resultados apresentados no quadro 2, percebemos que os entrevistados que registraram boletim de ocorrência, o fizeram porque conseguem sustar os pagamentos, com o seu banco lhe dando suporte e até porque podem receber devolução do

prejuízo. E os entrevistados que não fizeram boletim de ocorrência alegam que não sofreram danos e/ou prejuízos.

O B.O serve como “pontapé inicial” dado à Polícia pelo comunicante para a investigação dos fatos comunicados. Presta-se fielmente à descrição do fato, registrando horários, determinados locais, relacionando objetos, descrevendo pessoas envolvidas, identificando partes entre inúmeras outras informações relevantes juridicamente.

De outro lado, o brasileiro tem por costume lavrar boletins para o registro de fatos atípicos, isto é, fatos que, muito embora, não se revistam de tipicidade penal - não configurando, portanto, infração penal - servem para “preservar direitos” ou prevenir a prática de possível infração.

O B.O também serve para resguardar a própria ação policial, demonstrando de onde partiu aquela série de ações investigativas que se o órgão de polícia está realizando.

Tal documento, que para muitos parece simples e de pouca valia, pode acarretar consequências irreversíveis para a pessoa apontada como "autor dos fatos" ou “comunicado”.

3.Conclusões

Cumprimos o nosso objetivo, ao contextualizar os principais cibercrimes praticados no Brasil e compreender onde os criminosos mais atacam. Fazendo com que os usuários conheçam os riscos que correm ao utilizar a internet. É de muita valia que os professores das licenciaturas tomem conhecimento sobre esse assunto, pois é um assunto muito sério, para que eles possam formar outros profissionais da educação básica, para que sejam mais conscientes e preparados sobre os riscos que a internet oferece.

Referente à pesquisa,ressalta-se que o estudo foi realizado no estado de Pernambuco, onde os sujeitos entrevistados são discentes e docentes da Universidade de Pernambuco. E sabemos que é de extrema valia que novos estudos ocorram, abrangendo um número maior de entrevistados para se ter uma dimensão mais ampla do objetivo estudado: os principais cibercrimes praticados no Brasil.

Sobretudo, a pesquisa realizada é de grande importância para os estudos acadêmicos, em busca de melhores resultados para uma segurança maior dos usuarios, levando em conta a importância de mostrar quais os principais cibercrimes mais praticados no Brasil, como os criminoso atacam, quais são as técnicas mais utilizadas de cibercrimes e consequentemente como se prevenir desses ataques.

Referências

AGBINYA, J. I., Islam, R., & Kwok, C. **Development of digital environment identity (deity) system for online access.** In Proceedings of the 2008 Third International Conference on Broadband Communications, Information Technology & Biomedical Applications, BROADCOM '08, IEEE Computer Society, Washington, DC, USA, pages 1–8, 2008.

Fernando Mercês. (2014). Trend Micro Security Intelligence. **"O Submundo do Crime Digital Brasileiro: Um Mercado de Aspirantes a Cibercriminosos?"**. Disponível em:<http://www.trendmicro. com.br/cloud-content/br/pdfs/141117_mercadosubmundobr.pdf>. Acesso em: 09 junho.2018.

GARTNER. **Gartner Says More than 75 Percent of Mobile Applications will Fail Basic Security Tests Through 2014**.Disponível em: < http://www.gartner.com/newsroom/id/2846017>. Acesso em: 27 maio.2018.

GODOY, A. S. **A pesquisa qualitativa e sua utilização em administração de empresas.** RAE, São Paulo, v. 35, n. 4, p. 65-71, 1995.

GODOY, A. S. **Estudo de caso qualitativo.** In: GODOI, C. K.; BANDEIRA-DE-MELLO, R.; SILVA, A. B. Pesquisa qualitativa em estudos organizacionais. São Paulo: Saraiva, 2006.

Humberto L. Antonelli & Emerson G. Almeida. (2011). EGOV. **A Internet e o Direito: Uma abordagem sobre cibercrimes.** Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/a_internet_e_o_direito_uma_abordagem_sobre_cibercrimes.pdf>. Acesso em: 08 maio.2018.

INTERPOL. **Cybercrime.** Disponível em: <http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>. Acesso em: 07 maio. 2018.

PRETI, O. **Produção de material didático impresso:** orientações técnicas e pedagógicas. Cuiabá: UAB/UFMT, 2010.