

PANORAMA DA SOCIEDADE DE INFORMAÇÃO E EM REDE: O ESTUDO DE CASO DO *PHISHING* NO E-BAY

PANORAMA OF THE INFORMATION SOCIETY AND NETWORK E-BAY PHISHING CASE STUDY

Karen Cristina Coelho da Silva¹

Graduanda em Direito

Associação de Ensino Barramansense/Centro Universitário de Barra Mansa

Barra Mansa (RJ) – Brasil

RESUMO: A pesquisa trata da rápida evolução da internet e suas implicações incisivas no cotidiano e nas relações sociais estabelecidas pelo novo padrão de vida social iniciado junto ao advento da rede mundial de telecomunicações – sociedade da informação e em rede. O objetivo é o de comprovar o aumento do Phishing – uma típica prática lesiva, altamente qualificada e difundida na Sociedade de Informação em Rede. O Phisher - um criminoso altamente qualificado - se utiliza de seus conhecimentos profundos sobre a rede a fim de tomar para si dados confidenciais que não lhe pertencem. Sendo assim, faz-se mister discutir os parâmetros de proteção da internet e, particularmente, no e-commerce e as lesões que podem ser causadas.

Palavras-chaves: Internet. Prática criminosa. Rede mundial de telecomunicações.

ABSTRACT: The research deals with the rapid evolution of the Internet and its incisive implications in daily life and social relations established by the new pattern of social life started with the advent of the global telecommunications network - the information society and networking. The goal is to prove the increase in Phishing - a typical harmful practice, highly skilled and widespread in the Information Network Society. The Phish - a highly qualified criminal - uses its deep knowledge of the network to take each other confidential data that does not belong to him. Therefore, it is mister discuss the internet protection parameters, and particularly in e-commerce and injuries that may be caused.

Keywords: Internet. Criminal practice. Global telecommunications network.

INTRODUÇÃO

Com o advento da internet iniciou-se mundialmente uma nova era de relações sociais. Um novo mundo, completamente inexplorado e com inúmeras possibilidades de acontecimentos e eventos pouco estudados e analisados. Relações tais como, a troca de informações e conhecimentos gerais ou específicos e ainda relações negociais,

¹ Técnica em Telecomunicações no Ensino Médio. Estudante do 9º período do Curso de Direito do UBM. Estagiária do Núcleo de Prática Jurídica do NPJ. Resenha de Trabalho de final de curso apresentado e aprovado pela Banca Examinadora composta pelos professores: Cláudia Ribeiro Pereira Nunes, Gabriela Quinhones de Souza, Sheila Lyrio Zelma. E-mail: karen.c.coelho@gmail.com

transacionais, como por exemplo o e commerce, que vem crescendo exponencialmente a cada dia. A partir da observância de todo um cenário, de mudança estrutural do ordenamento jurídico com o advento da internet, se torna indispensável uma análise mais aprofundada dos fatos que surgiram com tal revolução; não apenas os da nova vida tecnológica, mas os da vida cívica, jurídica, que acabaram consolidando um acervo de fatos atípicos que pontuam a atualidade.

Essas questões apresentam-se diariamente em um mundo virtual globalizado, extremamente dinâmico que, para muitos, se trata, equivocadamente, de uma miscelânea virtual, de uma internet sem lei e sem parâmetros do que é lícito ou do que é ilícito.

Neste contexto surge o Phishing - golpe online de falsificação, e seus criadores não passam de falsários e ladrões de identidade especializados em tecnologia. Eles usam spam, websites falsos, crimeware e outras técnicas para fazer com que as pessoas revelem informações sigilosas, como detalhes de contas bancárias e de cartões de crédito. Após capturarem informações suficientes sobre as vítimas, eles as usam para enganá-las ou as vendem no mercado negro para obter lucros.

Considerando o atual campo legislativo-punitivo penal brasileiro, levanta-se a questão de que sendo tudo isto muito novo no Estado brasileiro, há lacunas no ordenamento jurídico, impossibilitando a correta punição dos criminosos praticantes de Phishing.

Justifica-se por serem as questões tratadas, atuais e instigantes, pelo fato de a população em geral, partindo do popular não especializado aos capacitados usuários empresariais, não conseguir sequer detectar quando expostos ao golpe online e, ainda, por não haver uma legislação específica para punir os crimes de internet, tais quais a prática de Phishing.

1 DIFERENCIAÇÃO ENTRE HACKERS E CRACKERS

Inicialmente insta trazer à luz conceitos como os de hackers e crackers, no que consiste suas atuações e diferenciações no mundo virtual.

O verbo tohack em inglês possui inúmeras traduções possíveis dependendo do contexto no qual é inserido, cabendo aqui sua utilização quanto aos profissionais da web.

Significado interessante é o explicitado por David Casacuberta, responsável pelo dicionário de Ciber- Direitos:

(...) A princípio, o termo hacker vem do verbo inglês hack que é usado normalmente no contexto dos lenhadores, no sentido de cortar alguma coisa em pedaços ou no sentido de dar pontapés. Segundo a lenda o primeiro uso não “tradicional” do termo se deveu a alguém que sabia dar o pontapé (hack) no ponto exato de uma máquina de refrigerantes para dessa conseguir uma lata (ou garrafa) gratuitamente. Seja nesse sentido, seja no sentido de cortar algo em pedaços, o certo é que o primeiro uso genuíno de hackear no mundo da informática foi de alguém que conhecia de modo muito detalhado um sistema operacional (havia cortado-o em pedaços, por assim dizer) a ponto de poder obter desse o que quisesse (como o senhor da lenda urbana a respeito da máquina de refrigerantes). Deste modo, originalmente, um hacker é simplesmente alguém que conhece os sistemas operacionais (e, logo, os computadores) como a palma de sua mão. Uma vez que, em princípio, para poder entrar num computador sem permissão são necessários grandes conhecimentos(...), rapidamente o termo se difundiu com a nova acepção: a de intruso ou violador informático que acessa o controle de uma máquina na rede, sem permissão.

Os hackers porém, são considerados muito importantes para as empresas que trabalham com tecnologias de informação em rede, visto que, para que possam criar mecanismos de segurança mais eficazes é necessário que alguém descubra suas falhas, seus pontos fracos de defesa e indique a melhor maneira de melhorá-lo. (Vancim e Matioli. 2011: p.94)

Neste contexto surge a denominação cracker que, criada pelos próprios hackers, é utilizada para diferenciar aqueles profissionais, que utilizam de seus conhecimentos informáticos para seu sustento lícito, daqueles que têm intenções criminosas como o cometimento de fraudes online, espionagem com o objetivo ilícito de obter vantagem para si ou para outrem. (Vancim e Matioli. 2011; p.94)

“Os crackers são aqueles que rompem a segurança de um sistema em busca de informações confidenciais com o objetivo de causar danos ou obter vantagens pessoais.”

Donde pode-se concluir que o phisher é um hacker, pois possui imenso conhecimento da rede e da tecnologia informática, tanto de hardware como de software, porém enquadrando-se melhor na categoria de cracker, pois seu objetivo é causar danos ou obter vantagem pessoal, de forma ilícita, caracterizando como um ciber-criminoso.

2 POSSIBILIDADES DE PHISHING NAS COMPRAS NO AMBIENTE E-COMMERCE

O ambiente em rede traz inúmeras vantagens tais como otimização do tempo, liquidação da dificuldade de locomoção, entre inúmeras outras, porém é um ambiente propício à incontáveis tipos de fraudes, que já existem que surgem como inovações a cada dia, e em velocidade recorde.

A informatização está presente no ambiente particular, interligando e modificando relações interpessoais e comerciais, estando também presentes na esfera pública, assim, está presente em todos os setores e em todos os lugares.

2.1 CONCEITO DE PHISHING

Phishing é um golpe online de falsificação, e seus criadores são criminosos especializados em tecnologia. A denominação “Phishing” resulta da união dos vocábulos “Phreak” que significa gênio em computação e “fish” que traduz-se por pesca.

É utilizado para intitular os golpes que são aplicados através da internet com a finalidade de obter ilicitamente os dados pessoais e confidenciais dos usuários da rede. Os fraudadores utilizam –se de spams, websites falsos, crimeware e outras técnicas como intuito de induzir as pessoas a revelarem informações sigilosas, como detalhes de contas bancárias e de cartões de crédito. Após capturarem informações suficientes sobre as vítimas, eles as usam para enganá-las, para passar-se por elas ou as vendem no mercado negro para obter lucros. Por exemplo abrindo novas contas usando o nome da vítima, ou esvaziando suas contas bancárias, até mesmo vendendo informações sigilosas de empresas no mercado negro.

Na maioria dos casos, os phishers - que são os propagadores de phishing - enviam uma série de e-mails de spam, às vezes até milhões de mensagens, ou utilizam-se de um website falso. Cada e-mail contém uma mensagem que parece ter sido enviada por uma empresa conhecida e confiável. Já no website falso é solicitado, com urgência, que o visitante forneça informações confidenciais, como números de CPF, números de contas bancárias, senhas, etc.

Usualmente, a mensagem inclui logotipo, nome da empresa e, quase sempre, tenta provocar uma resposta emocional a uma falsa situação. Utilizando uma linguagem comercial e urgente, o e-mail quase sempre solicita informações pessoais e confidenciais do usuário. Algumas vezes, o e-mail direciona o destinatário diretamente para um site falso. O website, assim como o e-mail, parece autêntico e, em alguns casos, o URL pode ter sido mascarado para sugerir que o endereço da Web pareça real. Adicionando alguma letra quase imperceptível ao final do endereço de DNS, ou algum ponto ou traço que um usuário comum da rede é incapaz de perceber que está diante de um e-mail ou um website falso.

Segundo dados na empresa Norton Security após o ano de 2005, os phishers se tornaram muito mais sofisticados e começaram a usar crimeware em conjunto com seus websites falsos, aproveitando as vulnerabilidades comuns dos navegadores da Web, a fim de infectar os hardwares das vítimas. Esta conduta possibilita que com um simples clique em um link contido em um e-mail de phishing para um website falso, a identidade de um usuário pode ser roubada, uma vez que o phisher já não precisará que o próprio usuário insira as suas informações pessoais, mas o vírus inserido por este crimeware se encarregará de coletar as informações confidenciais que forem digitadas posteriormente naquele computador infectado, mesmo que em um site seguro.

O Cavalo de Tróia ou spyware inserido em seu computador irá capturar essas informações da próxima vez que você acessar o site legítimo do seu banco ou outro serviço online.

3 FORMAS TÉCNICAS DE PREVENÇÃO DE PHISHING

Algumas empresas disponibilizam programas preventivos de controle a “softwares maliciosos”, programas que visam detectar e deletar antivírus, possíveis sites maliciosos e ameaças na navegação via Web.

Para que seu computador esteja minimamente protegido basicamente, há que se atualizar o sistema operacional, já que a todo instante é descoberto e explorado falhas na segurança desses sistemas. Igualmente, recomenda-se que se atualize constantemente o navegador da internet (browser). E também é necessário um programa eficaz de antivírus para as atividades de cada usuário, sendo que para usuários particulares é recomendado uma espécie de antivírus e para empresas ou entidades públicas, onde as redes são menos confiáveis, um antivírus mais potente, e muitas vezes caro. O googlechrome atualmente disponibiliza um aplicativo específico de proteção contra ataques de phishing aos usuários do Gmail, que pode ser baixado gratuitamente diretamente como uma extensão do browser, essa extensão protege somente o e-mail do usuário avisando quando aquela página do Gmail, não é a página original do google.

Porém as tecnologias e as artimanhas dos phishers são altamente mutáveis e estes se aproveitam até mesmo dos programas de segurança para passar uma falsa confiança ao usuário.

4 DO ESTUDO DE CASO DO E-BAY

A McAfee divulga o Relatório Trimestral de Ameaças do McAfee Labs: agosto de 2014, revelando que o phishing continua sendo uma tática eficaz de infiltração em redes corporativas. Ao testar a capacidade dos usuários empresariais em detectar golpes online, o Questionário de phishing da McAfee identificou que 80% dos participantes não conseguiram detectar um a cada sete e-mails de phishing. Além disso, os resultados mostraram que os departamentos financeiro e de RH, que armazenam alguns dos dados corporativos mais sigilosos, tiveram o pior desempenho na detecção de golpes, ficando para trás em uma margem de 4 a 9%.

Desde a publicação do Relatório de ameaças do segundo trimestre de 2014 até a divulgação do relatório objeto deste estudo de caso, o McAfee Labs coletou mais de 250 mil URLs de phishing, resultando em um total de quase um milhão de novos sites no último ano. Além do aumento no volume total, os ataques de phishing indetectáveis ficaram mais sofisticados. Os resultados mostraram que o phishing de campanha em massa e o spearphishing ainda predominam entre as estratégias de ataque usadas pelos criminosos virtuais ao redor do mundo. Enquanto isso, os Estados Unidos continuam hospedando mais URLs de phishing do que qualquer outro país.

"Um dos grandes desafios que enfrentamos atualmente é atualização das tecnologias básicas da Internet para torná-las mais adequadas ao volume e à confidencialidade do tráfego que carregam", afirmou Vincent Weafer, vice-presidente sênior do McAfee Labs. "Todos os aspectos da cadeia de confiança foram quebrados nos últimos anos: de senhas à criptografia por chave pública OpenSSL e, mais recentemente, a segurança USB. A infraestrutura com a qual tanto contamos depende de tecnologias que não acompanharam as mudanças e que já não atendem às demandas atuais", explica Weafer.

O relatório da McAfee também revelou novas oportunidades de cibercrime desde a divulgação pública da vulnerabilidade Heartbleed, uma vez que dados roubados de sites ainda vulneráveis estão sendo vendidos no mercado negro. Listas de sites não corrigidos têm rapidamente se tornado um sucesso entre os criminosos virtuais e há ferramentas prontamente disponíveis para plantar armadilhas nesses sites. Com essas ferramentas, é possível montar um sistema automatizado que ataca máquinas confirmadas como vulneráveis e extrai informações confidenciais.

A cada trimestre, a equipe de mais de 400 pesquisadores multidisciplinares do McAfee Labs em 30 países acompanha toda a gama de ameaças em tempo real,

identificando vulnerabilidades de aplicativos, analisando e correlacionando riscos e possibilitando a correção instantânea para proteger as empresas e o público.

Ao analisar tal caso, pode-se notar que mesmo pessoas altamente instruídas, que trabalham nos setores mais sigilosos de grandes empresas não são capazes de detectar um ataque de phishing tamanha esperteza e eficácia de tais criminosos em conseguir mascarar e facilmente ludibriar os usuários com suas avançadas técnicas.

Um segundo estudo de caso foi feito em cima de um teste proposital da Symantec, empresa que administra um grupo de computadores conhecido como honeypots, uma rede de sistemas propositalmente vulneráveis que são usados para capturar e estudar ataques reais. Essas informações são, então, usadas para fins de pesquisa e refinamento dos produtos Symantec. A Symantec capturou recentemente um ataque típico de phishing em sua rede honeypot relacionado ao serviço de leilão on-line eBay. A popularidade e apelo universal do eBay tornou essa marca um dos maiores alvos de ataques de phishing na Internet.

Os eventos começaram com o agressor aproveitando uma falha de segurança antiga que foi disponibilizada propositalmente em um dos servidores do honeypot, visando justamente a ocorrência de eventos como esse. Depois que o agressor obteve acesso total ao sistema através de técnicas adicionais de hacking e uma ferramenta de controle remoto oculta, um website falso do eBay foi estabelecido no servidor. Veja acima a página de login falsa do eBay criada pelo phisher. Ela é extremamente semelhante à versão legítima do eBay e bastante convincente.

O e-mail de "isca", como a mensagem exibida abaixo, é então enviado pelo phisher a uma lista de e-mail das vítimas potenciais. Esta mensagem, extraída de um ataque de phishing real, segue a fórmula típica de linguagem que deseja parecer oficial, aliada a um aviso ameaçador, alertando o destinatário a agir imediatamente para que a sua conta permaneça ativada. Todos os links incluídos na mensagem remetem ao website real do eBay, com a notável exceção do convite falso, "clique aqui para reinserir as informações sobre a sua conta." O link para essa seção leva o usuário para a página de login falsa do <http://signin.ebaay-com.us/> ao invés da página genuína de login do eBay: <http://signin.ebay.com/>.

Transcrição da página da Internet:

Assunto: Aviso! Atualização de cartões de débito ou crédito [1] Registrar no eBay [2] [poweredByLogo_112x22.gif] Prezado cliente, [3] [SYIStart_LiveHelp_75x20.gif] Sentimos informar que a sua conta do eBay poderá ser suspensa, se você não atualizar novamente as informações da sua conta. Para resolver esse problema, [4] clique aqui para reinserir as

informações da sua conta. Se seus problemas não puderem ser solucionados, a sua conta será suspensa por um período de 24 horas, sendo que após esse período a conta será encerrada. De acordo com o Contrato do Usuário, seção 9, devemos emitir um aviso imediatamente, suspender temporariamente, indefinidamente ou encerrar sua afiliação e recusar o fornecimento de nossos serviços, se acreditarmos que as suas ações poderão causar perda financeira ou responsabilidade legal para você, para nós ou para nossos usuários. Deveremos também executar essas ações, caso não seja possível verificar ou autenticar qualquer informação que você nos forneça. Devido à suspensão desta conta, você estará proibido de usar o eBay para qualquer propósito. Isso inclui o registro de uma nova conta. Observe que essa suspensão não cancela nenhuma obrigação de pagamento de tarifas à eBay, com a qual você tenha se comprometido. Atenciosamente, Safeharbor DepartmenteBay, Inc, Equipe do eBay. Esta é uma mensagem automática. Favor não responder. [5]Sobre o eBay | [6]Notificações | [7]Centro de segurança | [8]Políticas | [9]Mapa do site [10]Ajuda Copyright © 1995-2005 eBay Inc. Todos os direitos reservados. Nomes e marcas comerciais designados são propriedades de seus respectivos proprietários. O uso deste website constitui a aceitação do [11]Contrato do Usuário e da [12]Política de privacidade do eBay. [13]TrustE

Após clicar no link falso da mensagem de e-mail de phishing, as vítimas fazem o login no site falso do eBay usando seu nome e senha (este site de phishing não fazia nenhuma restrição, aceitava todos os nomes de usuários e senhas). A vítima era então encaminhada para uma página onde poderia supostamente atualizar seu perfil de cobrança, o que enviaria por e-mail informações altamente confidenciais sobre a vítima, como informações do cartão de crédito, número de RG e CPF, endereço residencial e nome de solteira da mãe, diretamente para o phisher.

Figura 1

The figure displays two side-by-side screenshots of eBay's login interface. The left screenshot is the original eBay sign-in page, featuring the eBay logo, a 'Sign In' button, and fields for 'eBay User ID' and 'Password'. It includes links for 'Forgot your password?' and 'Sign In', and a 'Register' button. The right screenshot is a phishing page titled 'Comece a usar o eBay' (Start using eBay). It contains fields for 'Nome' (Name), 'Sobrenome' (Surname), 'E-mail', and 'Criar sua senha' (Create your password). It also has a 'Confirmar senha' (Confirm password) field and an 'Enviar' (Send) button. The phishing page includes a 'Já tem uma conta?' (Already have an account?) link and a 'Entrar' (Enter) button. The phishing page also contains a 'TrustE' logo and a 'Copyright © 1995-2005 eBay Inc. All Rights Reserved' notice.

Legenda: comparação entre a página fake e a página original do ebay.

Fonte: Disponível em: <eBay:http://signin.ebay.com>/. Acesso em 15 de mai. 2015.

Neste estudo de caso esse phisher específico preferia que as informações fossem enviadas a sua conta de e-mail gratuita, onde poderiam acessar e ler as informações

pessoais de cada vítima como desejassem, apesar de alguns phishers terem predileção por coletar todas as informações da vítima em um servidor conhecido como "deaddrop" ou "eggdrip",

A maioria dos ataques de phishing como esse dura somente alguns dias, com o maior número de vítimas respondendo dentro das primeiras 24 horas.

Através da análise deste segundo estudo de caso é possível mostrar como o phishing está presente no cotidiano dos usuários da rede e principalmente do e-commerce. O e-bay é um site muito popular altamente utilizado por inúmeros compradores ao redor do mundo, acessível por todos, de todas classes sociais, usuários instruídos e capazes de evitar contaminações por vírus ou se deixar levar por spams, e, também aqueles que são ingênuos e caem em todo e qualquer tipo de fraude.

Porém fazendo uma análise conjunta dos dois estudos de caso fica evidente a dificuldade de detectar-se os golpes de phishing, seja por pessoas comuns ou mesmo por pessoas instruídas neste sentido. E como ninguém está livre desta prática que é altamente crescente na sociedade atual.

CONSIDERAÇÕES FINAIS

O advento da internet proporcionou a superação das conhecidas limitações fronteiriças, territoriais e temporais, em especial, as práticas delituosas foram potencializadas devido a facilidade de acesso à informações de todo gênero, a qualquer momento e local. A virtualização da sociedade trouxe em seu seio além de inúmeros benefícios, aspectos negativos, atingindo cada vez mais, maiores setores sociais.

Com a revolução tecnológica, acelerou-se o processo conhecido como globalização tornando acentuado o grau de realidade atribuído à virtualidade, como nunca havia se vivenciado antes. Trazendo à evidência novas práticas delituosas significativamente potencializadas com o advento da sociedade de informação em rede, mostrando a necessidade da disponibilização de novas formas de proteção à bens jurídicos, com a finalidade de que o direito não ande descompassadamente com o avanço tecnológico-social, devendo tomar para si os moldes das novas demandas da sociedade.

Em contraposição a tamanha e rápida evolução tecnológica já alcançada, pode perceber-se uma lacuna nas formas de proteção e punição no direito penal material, no que consiste à aplicabilidade deste aos crimes cometidos via internet, o que acaba impondo ao direito processual copiosa barreira na solução dos casos concretos, tanto

sua persecução, quanto na produção probatória ou até mesmo na aplicação das medidas cautelares. Isto posto estender o tratamento de crimes comuns já tipificados no direito pátrio, a crimes que se dão de maneiras peculiares, bem como a expedição de leis, como o Marco civil da internet, que não satisfazem a premência da realização da persecução penal adequada.

A fase de investigação de um cibercrime não pode avançar sem o instrumento correto e capacitação dos agentes investigadores, sendo preciso também previsão concreta no que diz respeito à procedimentalidade.

O Brasil apresenta importantes progressos no que concerne a pesquisas sobre os crimes realizados no ambiente virtual, o que deixa perceptível a capacidade de instalação direito penal brasileiro, de maneira que tal aprendizagem não permaneça somente no plano ideológico e possa ser colocada em funcionamento, para a proteção dos usuários da internet, mantendo ainda a subordinação aos princípios constitucionais brasileiros. Porém, tal aprendizagem continua a não ter previsão de concretização em uma regulação procedimental.

Tem-se como solução à problemática penal a assinatura do Brasil à Convenção de Budapeste, já aderida por vários Estados europeus, que traz o cibercrime, sua tipificação e normas procedimentais, colocando enfoque à cooperação jurídica penal internacional, quanto à persecução penal, na fase investigativa e na produção probatória.

Cabe ainda salientar, que a convenção de Budapeste proporciona aos Estados signatários a criação de suas próprias legislações preventivas e repressivas dos crimes virtuais. Mantendo assim a soberania de qualquer país que venha a assinar tal tratado.

Portanto pode o Brasil como ato inicial à repressão de crimes no ambiente virtual, aumentar seus esforços em demonstrar ânimo em ser convidado a ser signatário da Convenção de Budapeste e em concomitância iniciar a preparação de seu sistema jurídico penal para inserir nestas normas regenciais que tipifiquem os crimes cibernéticos trazendo o direito para mais perto do avanço tecnológico.

REFERÊNCIAS

AZEVEDO, Mauricio Maia Vinhas. **Algumas considerações acerca da democracia direta eletrônica**. Revista de Informação. v.13, n.14. Agosto 2012. Disponível em: http://www.dgz.org.br/ago12/F_I_art.htm. Acesso em: 15 de maio 2015.

BOTELHO, Fernando. **A Internet brasileira e seus marcos regulatórios**http://ftp.tjmg.jus.br/institucional/discursos_artigos/desembargadores/internet_brasileira_fernando_botelho.pdf - Acesso em 13 de abril de 2015

BUDAPESTE. **Convenção de Cibercrimes.** Disponível em: http://www.wirelessbrasil.org/wirelessbr/secoes/crimes_digitais/texto_convencao.pdf. Acesso: 12 maio 2015.

CARNEVALE, Ubirajara; DUARTE, Solange. **O uso legal da Internet: ética e valores para jovens da era digital.** – São Paulo: 2011.

CASTELLS, Manuel. **A sociedade em rede - a era da informação: economia, sociedade e cultura**, vol. 1. São Paulo: Paz e Terra, 2000.

Centro de Estudos, **Resposta e Tratamento de Incidentes de Segurança no Brasil** – www.cert.br – Acesso em 12 de maio de 2015.

COASE, Ronald H. **O problema do custo social.** Tradução Francisco Kümmel F. Alves e Renato Vieira Caovilla. Original publicado em 1960. Disponível em: <http://www.pucpr.br/arquivosUpload/5371894291314711916.pdf> Acesso em 10 maio 2015.

CRESPO, Xavier de Freitas. **Diretivas Internacionais e Direito Estrangeiro.** In:_. Crimes Digitais. São Paulo: Saraiva, 2011.. P.120-155.

DELGADO, Vladimir Chaves. **Cooperação internacional em matéria penal na convenção sobre o cibercrime.** Dissertação (mestrado) Centro Universitário de Brasília: Brasília, 2007. p.57-58, 153-154.

GOMES, Luiz Flávio. Artigo. **Limites do “jus puniendi” e bases principiológicas do garantismo penal.** Busca legis.ccju.ufsc.br. p.3.

Crimes na internet: interpretados pelos tribunais: repertório de jurisprudência e legislação. Supervisão editorial: Jair Lot Vieira. Bauru, São Paulo. Edipro, 2009.p.97

GOOGLE, **História sobre os sites de busca.** Disponível em: <https://sites.google.com/site/historiasobreossitesdebusca/>. -Acesso em 05 de maio de 2015.

GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet.** Revista de Direito Mackenzie. Disponível em: <http://editorarevistas.mackenzie.br/index.php/rmd/article/viewFile/4811/3692> - Acesso em 10 de maio de 2015.

HATA, Fernanda Yumi Furukawa. **Direito Penal Internacional.** Revista SJRJ, Rio de Janeiro, V.17, n.29. p. 117-141, dez 2010. P. 117.

HERSCOVICI, Alain. **A sociedade em redes e a universalização do mercado: elementos de análise.** In: Revista Electrônica Internacional de Economia de las Tecnologías de laInformación y de loComercio, Volume 2, Jul./Ago. 2000, p.5-6. Disponível em <<http://www.eptic.he.com.br>> Acesso em: 30 de maio 2015

TECHTUDO, pesquisa. **80% dos brasileiros já sofreram ataques de phishing.** Disponível em: <http://www.techtudo.com.br/noticias/noticia/2011/09/80-dos-brasileiros-ja-sofreram-ataque-de-hackers-na-rede.html> - Acesso em 14 de maio de 2015

MCAFEE, **pesquisa de Campo,** - Disponível em: <http://convergecom.com.br/tiinside/seguranca/mercado-seguranca/05/09/2014/pesquisa-mostra-que-80-dos-usuarios-corporativos-nao-sao-capazes-de-detectar-golpes-de-phishing> – acesso em 10 de maio de 2015

LÉVY, Pierre. **O que é virtual?** Tradução: Paulo Neves. E-book. Disponível em:http://www.mom.arq.ufmg.br/mom/arq_interface/6a_aula/o_que_e_o_virtual_-_levy.pdf. Acesso em: 05 mai. 2015. p.82-83

MACHADO, André Augusto Mendes. **A investigação criminal defensiva.** 2009. Dissertação (Mestrado), Faculdade de Direito de São Paulo, São Paulo. p.101-103

MELLO, Celso Albuquerque. **Curso de Direito Internacional Público.** Rio de Janeiro: Renovar, 2004. P.96-97.

NUNES, RadamNakai. **A cooperação jurídica penal internacional à luz do garantismo penal**. Tese (mestrado), Universidade Católica de Brasília, Brasília, 2006. p.100-101

OLIVEIRA, Liziane Paixão silva. **O Conceito de Soberania Perante a Globalização**. Revista CEJ, Brasília n.32, p.80-88, jan/mar. 2006 Pag 82.

ORTON, Frank. **Algumas características especiais do Processo Civil Sueco**. Tradução: Alexandre Freitas Câmara.R.EMERJ, Rio de Janeiro, v.14, n.54 p.7-14. Disponível em: http://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista54/Revista54_7.pdf. Acesso em: 15 mai. 2015.

SANTOS, Coriolano Aurélio Camargo. **Atual cenário dos Crimes Cibernéticos no Brasil**. Disponível em:<http://pt.scribd.com/doc/41224053/Crimes-Ciberneticos>. Acesso em: 10 maio 2015. p. 13-14

SILVA, Ana Karolina Calado da. **O estudo comparado dos crimes cibernéticos: uma abordagem instrumentalista-constitucional acerca da sua produção probatória em contraponto à jurisprudência contemporânea brasileira**. In: **Âmbito Jurídico**, Rio Grande, XVI, n. 109, fev 2013. Disponível em: http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=12778&revista_caderno=17 - acesso em 06 de maio de 2015.

STJ, NOTÍCIAS ESPECIAIS - **Justiça usa Código Penal para combater crime virtual**
http://stj.jus.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=90108 – Acesso em: 14 de maio de 2015

SOUZA, Márcia Cristina Pereira de. **Proteção Jurídica do software**. Disponível em: <<http://www.cjf.jus.br/revista/numero3/artigo18.htm>> Acesso em: 08 de maio de 2015.

DADOS, **ferramentas de busca**. United States of American, apelle, Robert Tappan Morris, defendant-apellant. Disponível em: http://www.loundy.com/CASES/US_v_Morris2.html. Acesso em: 20 mai. 2015.

VANCIM, Adriano; MATIOLI, Jefferson. **Direito & Internet - Contrato Eletrônico e Responsabilidade Civil na Web** . – 1ª Ed. Leme: Lemos &Cruz :2011

WACHOWICZ, Marcos. **O programa de computador e sua proteção no Brasil**. Jus Navigandi, Teresina, 6, boletim 53, 2002. Disponível em: < <http://www1.jus.com.br/doutrina!texto.asp?id=2530> >. Acesso em: 13 de maio de 2015

YOUTUBE. **Saiba mais- soberania nacional**. Disponível em: <http://www.youtube.com/watch?v=nMKwPSaygOE> Acesso: em: 10 de maio 2015.