Modalidade do trabalho: Relatório técnico-científico
Evento: XXIII Seminário de Iniciação Científica

CRIMES CIBERNÉTICOS: PHISHING - PRIVACIDADE AMEAÇADA[1]

Grasiele Giusti Morgenstern[2], Tania Regina Gottardo Tissot[3].

[1] Artigo científico realizado no Curso de Direito da FEMA, na matéria eletiva Direito e Informática.
[2] Acadêmica do Curso de Direito – 6º semestre. Faculdades Integradas Machado de Assis (FEMA) - Santa Rosa/RS. grasygm@hotmail.com
[3] Acadêmica do Curso de Direito – 6º semestre. Faculdades Integradas Machado de Assis (FEMA) - Santa Rosa/RS. tania.tissot@hotmail.com

1.INTRODUÇÃO

A sociedade caminha para a globalização como consequência da revolução tecnológica e da explosão da comunicação que se relaciona com o desenvolvimento de sociedades mais livres, igualitárias, sociedade da informação, que universaliza hábitos, culturas e formas de produção e consumo. Os meios de comunicação de massa, potenciados por novas tecnologias, rompem fronteiras culturais, políticas, religiosas e econômicas .

A internet é vista como um meio de comunicação que interliga dezenas de milhões de computadores no mundo inteiro e permite o acesso a uma quantidade de informações praticamente inesgotáveis, anulando toda distância de lugar e tempo .

Vivemos em uma sociedade informatizada onde as Tecnologias da Informação (TICs) fazem parte do dia-a-dia, sendo um meio de ampliação e praticidade da comunicação e informação, auxiliando no desenvolvimento da globalização com informações instantâneas, invadindo a sociedade e se tornando necessária às transformações do mundo atual.

Segundo Emerson Wendt:

A internet tem sido utilizada para inúmeras finalidades, seja para realizar negociações comerciais, buscar conhecimento, conhecer pessoas, manter relacionamentos, produzir atividade de marketing pessoal, buscar diversão e, em alguns casos, promover transtornos para outras pessoas, incluindo prejuízos financeiros das vítimas .

A difusão desta tecnologia representa um avanço considerável em se tratando de propagação de conhecimento, informações que antes não chegavam a certos lugares, hoje, com a internet, chega a qualquer lugar, basta que haja estrutura para tanto. Para as TICs, não há espaço nem tempo, ambos se perderam, pois não há barreiras para se conectar com o mundo tornando o usuário um disseminador e coletor de informações, sejam estas verdadeiras ou não.

Em virtude dessa crescente expansão do uso da internet, a exposição dos usuários é cada vez maior, gerando interesse e possibilitando a prática de crimes. Estes crimes podem acontecer de maneiras e lugares diferentes, sendo uma ação criminosa envolvendo computadores e redes. Destinada a tipificar estes crimes, entrou em vigor no dia 2 de abril de 2013, a Lei dos Crimes Virtuais – Carolina Dieckmann, Lei 12.737.

Modalidade do trabalho: Relatório técnico-científico
Evento: XXIII Seminário de Iniciação Científica

A Lei 12.965, de 23 de abril de 2014, Marco Civil da Internet, veio para auxiliar no que dizem respeito aos princípios, garantias, direitos e deveres para o uso da internet no Brasil, determinando as diretrizes para atuação de cada esfera em relação à matéria (art. 1º, Lei 12.965/2014).

2.METODOLOGIA

Este trabalho é resultado de uma investigação bibliográfica, por meio de um procedimento qualitativo, a qual discutiu sobre a modalidade de pesquisa utilizando como suporte teóricos autores que discorrem sobre a proposta.

3.RESULTADOS E DISCUSSÃO

O presente trabalho exibe uma pesquisa, sem esgotar o tema, sobre os crimes cibernéticos, especificamente sobre o phishing. A utilização desenfreada dos meios eletrônicos e o desenvolvimento das novas tecnologias de informação têm aumentado à insegurança e a falta de privacidade de quem utiliza estes meios. Cada vez mais cedo as pessoas têm acesso à internet ficando expostas aos riscos oferecidos e em muitos casos repassando informações da privacidade de familiares e conhecidos.

Esse acesso irrestrito e exposição da privacidade e de dados pessoais, documentos eletrônicos, transações bancárias, provoca interesse em outros usuários, é o que se percebe com os crimes virtuais ou cybercrimes, que são realizados de várias maneiras interferindo na segurança digital do usuário, invadindo sua privacidade e de seus conhecidos. Há a necessidade de proteção da intimidade, privacidade e informações pessoais, a fim de que o cidadão não seja transformado em números, tratado como se fosse mercadoria, com seus dados sendo comercializados ao ponto de causar prejuízos.

O termo phishing é originado da palavra inglesa fishing, que significa pescar, ou seja, é a conduta daquele que pesca informações sobre o usuário de computador . É um tipo de fraude eletrônica, onde o golpista busca obter informações pessoais do usuário como senhas, dados financeiros, números de cartões de crédito e outros dados pessoais .

No início a palavra phishing era utilizada para definir a fraude que consistia no desvio de e-mail não solicitado pela vítima, que era estimulada a acessar sites fraudulentos. Os sites tinham a intenção de permitir o acesso às informações eletrônicas da pessoa que lhe acessava, como por exemplo, número da conta bancária, cartão de crédito, senhas, e-mails e outras informações pessoais .

Uma característica destas mensagens é que simulavam ser originadas de uma instituição conhecida, como por exemplo, banco, órgão governamental, empresa etc. . Estas mensagens procuram sempre chamar a atenção do usuário com a possibilidade de obter vantagem ou pela curiosidade, apresentando diferentes temas de campanhas publicitárias, serviços, imagens de pessoas famosas, assuntos em destaque .

Nestes casos o criminoso criava uma falsa história para atrair os usuários de computadores e com isso acessar as informações nas quais tinha interesse, principalmente visando obter lucros ou causar prejuízos para as vítimas .

Atualmente esta palavra é utilizada para definir também a conduta das pessoas que encaminham mensagens com a finalidade de induzir a vítima a preencher formulários com seus dados privados

ou a instalar códigos maliciosos, capazes de transmitir para o criminoso cibernético as informações desejadas .
De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, os principais tipos de ações envolvendo phishing utilizados pelos autores destes crimes são :
- mensagens que contêm links para programas maliciosos;
- páginas de comércio eletrônico ou internet banking falsificadas;
- mensagens contendo formulários para o fornecimento de informações importantes.

4.CONCLUSÕES

O ser humano tem como atributo natural, a busca incontinente do meio mais fácil para conseguir seus objetivos, sejam eles materiais ou morais. A Rede Mundial de Computadores e demais equipamentos de Informática, são meios mais ágeis, úteis e eficazes para obtenção de objetivos inerentes a cada pessoa, talvez, inimagináveis por um leigo no século XX .
No entanto, ao mesmo tempo em que os meios eletrônicos trazem para a sociedade uma facilidade para progressão financeira e moral de forma lícita, infelizmente, também trazem as mesmas progressões para os criminosos, principalmente em relação aos crimes contra o patrimônio .
O Brasil, segundo diversas fontes de pesquisa, alcança os primeiros lugares no ranking de "crackers" (tipo de Hacker que utiliza seus conhecimentos para prática de ilícitos) e cybercrimes no mundo .
Esse tipo de constatação só nos leva a concluir que nosso Poder Judiciário deve agir coercitivamente com criminosos que utilizam os meios em comento, enquadrando-os em normas penais já previstas com severas sanções.
As Pessoas Jurídicas devem harmonizar-se nos mais autos níveis de segurança para os serviços que prestam pela Internet, sob pena de sofrerem indenizações por negligência, imprudência ou pelo próprio risco do negócio. As Pessoas Físicas, da mesma forma, devem utilizar todos os produtos e dicas de seguranças para não terem seus dados e senhas capturados .
Diante do exposto, urge a necessidade de constatarmos que apesar da matéria em testilha ser nova, principalmente no mundo jurídico, podemos apontar que a doutrina e a jurisprudência estão concluindo que quase todos atos ilícitos cometidos por meios eletrônicos já têm previsão legal .

5.PALAVRAS-CHAVE: Crimes Cibernéticos; Usuários; Internet; Phishing.

6.REFERÊNCIAS

CARTILHA DE SEGURANÇA PARA INTERNET, UNIVERSO ON LINE SA. Disponível em: <https://sac.uol.com.br/info/cartilha/fraudes/sec2.jhtm>. Acesso em: 13 dez. 2014.

CARTILHA DE SEGURANÇA, GOLPES NA INTERNET. Disponível em: <http://cartilha.cert.br/golpes/>. Acesso em: 13 dez. 2014.

MONITOR DAS FRAUDES. Disponível em: <http://www.fraudes.org/buscasite.asp?Src=phishing>. Acesso em: 13 dez. 2014.

OPICE BLUM. Disponível em: <http://www.opiceblum.com.br/lang-pt/02_artigos_a001.html?ID_ARTIGO=46>. Acesso em: 13 dez. 2014.

OPICE BLUM. Disponível em: <http://www.opiceblum.com.br/lang-pt/02_artigos_a001.html?ID_ARTIGO=28>. Acesso em: 13 dez. 2014.

PAESANI, Liliana Minardi. Direito e Internet. 6. ed. São Paulo: Atlas, 2013, p.10.

PHISHING. Disponível em: <http://pt.wikipedia.org/wiki/Phishing>. Acesso em: 13 dez. 2014.

WENDT, Emerson. JORGE, Higor Vinicius Nogueira. Crimes cibernéticos: ameaça e procedimentos de investigação. 2 ed. Rio de Janeiro: Brasport, 2013, p. 12.