Centro Universitário Processus

Alunos: 10° semestre - Noturno

1- Camila Cristina Gonzaga de Freitas.
2- Lilian Cristina Alves de Souza
3- Bruna Pires Silva
4- Maria Luiza Limeira Pereira Coelho
5- Sandovaldo Belem

DISCIPLINA DE EXTENSÃO: DIREITO DIGITAL

Tema: Prevenção aos Crimes Cibernéticos

Grupo 1: Identidades Fraudulentas no contexto virtual

INTRODUÇÃO

POLÍTICAS PÚBLICAS VOLTADAS AO COMBATE E PREVENÇAO

Mesmo com a chegada positiva da Era digital é preciso mencionar os impactos negativos que acompanharam essa nova realidade, sendo uma situação completamente nova, a sociedade ainda não está preparada para lidar com a proteção virtual.

A Era digital vem ocasionando muitos prejuízos e transtornos para a sociedade, a prática de crimes virtuais se tornaram cada vez mais frequente, surgindo então os crimes no contexto virtual no qual se caracterizam pela prática de delitos cometidos na internet, afirma-se atualmente que a prática desses delitos cresce a cada dia, devido ao aumento de usuários e pela facilidade que as inovações tecnológicas trouxeram para a sociedade. Não restam dúvidas de que a nova era trouxe, além de muitos benefícios, vários malefícios. O anonimato é um problema resultante dos inúmeros malefícios

da Era digital, não podemos ignorar o fato de que todos aqueles que cometem crimes no ambiente digital estão em anonimato, ou seja, se utilizando de falsas identidades para atingir os usuários mais vulneráveis, em frente a um computador há uma pessoa que está realizando atividades incapazes de identificação, isso quando realmente é uma pessoa física, atualmente com a inovação tecnológica existem programas que realizam essas atividades criminosas

A sociedade precisa refletir que os métodos de combate e enfrentamento não consegue alcançar e agir preventivamente elucidando todos os casos existentes. É preciso que sejam operadas formas de proteção para que os usuários se conscientizem dos perigos que a internet proporciona, pois atualmente a rede mundial de computadores oferece informações gratuitas e das mais variadas. Dentro do contexto virtual, todos possuem o livro arbítrio de se relacionar umas com as outras, usando a internet como ferramenta de trabalho ou como diversão, porém infelizmente a sociedade está à mercê de criminosos em ambientes digitais, onde os criminosos estão cada vez mais especializados em condutas ilícitas.

Portanto, é importante enfatizar as informações relacionadas com a segurança tecnológica, criando uma base eficiente para os usuários utilizarem as redes com prevenção, tornando a internet uma opção segura e eficaz para a utilização de todos, atualmente a internet dispõe de ferramentas acessíveis e complexas para prevenção de fraudes, furtos de identidade e invasões financeiras.

Os criminosos utilizam várias técnicas para enganar vítima, oferecendo recursos e fazendo as vítimas acreditarem em suas farsas, os criminosos agem de maneira tão propulsora, ludibriando as vítimas para que ofereçam informações pessoais, concretizando assim a vontade dos criminosos.

INDÍCIOS INVESTIGATIVOS

Após a evolução da internet, em meados dos anos de 1973, descobriu que o apito de plástico, produzia sons exatamente na mesma frequência que era usada para ter acesso ao satélite para ligações à longa distância, então começarão as ligações serem realizadas sem a necessidade de serem pagas, considerando assim o primeiro crime cometido de forma digital.

Os crimes virtuais são ações ilícitas cometidas através do uso de dispositivos eletrônicos e da internet que ofendem direta e indiretamente a segurança informática e a privacidade dos indivíduos em seu aspecto amplo, por meio desses e pela recorrência dos crimes cometidos de formas virtuais, os usuários começaram a buscar medidas para garantir um pouco mais de segurança, usando assim uso de antivírus, por exemplo. Com os passar dos anos, os criminosos virtuais foram evoluindo dia após dia, realizando novas técnicas, aprimorando seus conhecimentos e descobrindo então o mundo que existe por trás da internet, como por exemplo, Deep Web e a Dark Werb, que permitem os acessos por meio de navegadores especiais que impedem o rastreia das atividades dos usuários. Elas são compostas por sites, páginas, que não podem ser localizadas por qualquer meio de busca online, dificultando então os meios de investigação que são utilizados para a busca desses criminosos.

A nível processual ou puramente investigativo, em casos de ataques realizados sobre ou através de uma rede informática, distribuição de conteúdos ilícitos ou utilização de uma rede informática como meio de comunicação entre criminosos, não seria realista recorrer apenas aos meios tradicionais de investigação. Pelo contrário uso de novas tecnologias É importante encontrar e coletar evidências. Para identificar a origem do ataque ou destinatário da mensagem ou na prevenção de infrações graves contra um interesse legítimo coletivo substancial.

O escopo da investigação, antes de tudo, é instaurar um inquérito policial, e conduzir uma investigação após a denúncia do caso à delegacia especializada em crimes cibernéticos, portanto, começa a fase da apuração de provas. Todo ato feito por algum aparelho eletrônico, deixa algum tipo de rastro codificado em alguma rede de dados, até mesmo na Deep Web, em mensagens criptografadas, ou nos IPs das máquinas utilizadas para cometer os crimes.

Conforme o exposto, para que seja realizada a linha de investigação sobre os crimes cometidos, é necessário um cuidado muito maior que os demais delitos, pois além de existir uma grande dificuldade na investigação, os metodos utilizados são mais especificos.

Vale salientar, que as pessoas que são vitimas desses tipos de crimes, acabam trazendo para si um abalo psicológio, pois além de se sentir totalmente indefesa, grande parte das vezes, acabando tendo um impacto financeiro em sua vida e até em suas empresas, quando não são cometidas a diversas ameaças e extorsões com o receio de ter mais a sua vida exposto por estes criminosos.

Diante das dificuldades na quais as autoridades encontram ao realizar

as investigações, existem então alguns métodos principais que são utilizados, como: a interceptação das comunicações telefônica, quebra de sigilo telefônico e de dados e quebra de sigilo telemático, que são considerados os métodos mais corriqueiros nos crimes cibernéticos, vale salientar que para a autoridade policial conseguir utilizar-se desses meios investigativos, é obrigatória a autorização judicial, como também, comprovar que todos os outros meios de prova restaram ineficazes para elucidação do delito, pois a regra é a proteção dos dados.

O objetivo da investigação desses crimes é identificar na mídia os endereços IP utilizados pelos criminosos durante suas operações. Para Teixeira (2013, p.43) "O endereço IP, também conhecido como endereço lógico, é um sistema de identificação universal onde cada computador possa ser identificado exclusivamente, independente da rede em que esteja operando". Entre as evidências que podem ser obtidas na investigação de crimes cibernéticos, o endereço IP é, sem dúvida, a evidência mais importante para resolver o caso.

Caso, perceba que foi vítima desses determinados crimes, é necessário que realize a comunicação na delegacia, tanto virtual ou presencialmente, com isso irá ajudar as autoridades policiais para que posso realizar os meios de investigações.

COMO OCORRE O ROUBO DE IDENTIDADE

O furto online normalmente costuma ocorre por meio do phishing (tentativa de frauda para obter ilegalmente informações como número da identidade, senhas bancárias, número de cartão, entre outros, através de um e-mail com conteúdo duvido) ameaças virtuais enviadas com o objetivo de roubar informações ou dados pessoais por meio de mensagens falsas.

O furto ou roubo de identidade que ocorre quando alguém consegue as informações através do que foi citado anteriormente, como ocorre normalmente ao atender uma ligação e acreditar que o link ou pagina que foi enviada é verídica e confiável.

COMO SE PROTEGER

Para se proteger é recomendado algumas orientações

1- Ative a verificação em duas etapas para proteger os dispositivos contra malwares (software malicioso usado para causar prejuízo);

2- Não acessar contas pessoais em dispositivos de terceiros;

3- Evite usar a rede WiFi grátis, pública ou privada;

4- Senhas fortes e diferenciadas;

5- Não use o perfil pessoal de rede social para outros cadastros;

6-Ficar atento a solicitação de mensagens eletrônicas;

7- Cuidado ao receber mensagens via SMS, WhatsApp, ou redes sociais e ou outros meios de comunicação digital;

8-Observe selos e certificados de segurança;

9-Tente contato pelos canais de atendimento;

10- Cheque sites de reputação e comentários nas redes sociais.

PREVISÃO LEGAL

Alguns dos crimes descritos, tem previsão no ordenamento jurídico brasileiro:

No crime de falsidade ideológica o sujeito pretende alterar a verdade dos fatos que têm relevância jurídica, criar obrigações, ou, prejudicar direitos, através da fraude de informações em documentos públicos ou privados. Essa fraude se dá pela inserção de uma falsa declaração ou pela omissão de dados que essencialmente deveria constar. Art-299 do Código Penal.

No crime de estelionato o sujeito que obtém vantagem ilícita para ele ou para outrem, em prejuízo alheio, induzindo ou mantendo alguém em erro, seja mediante artifício, ardil ou qualquer outro meio fraudulento,pratica o crime de estelionato. Art-171 do Código Penal.

No crime de falsidade ideológica, o que vem à mente das pessoas é um indivíduo que altera documentação se fazendo passar por outra. Art-307 do Código Penal**.**

OBJETIVO

Alertar os operadores comerciais, pessoas físicas, pessoas jurídicas, financeiras dentre outras para diminuição dos casos de golpes. Esses roubos acontecem por meio de phishing. O phishing opera através de e-mail, sites enganosos, falsas operações, como empréstimos, lotéricas, prêmios e muito mais.

Eles visam obter acessos a dados confidências de futuras vítimas. À

medida que os avanços da tecnologia aumentam, as gestões de risco aumentam também. O objetivo principal é a orientação dos meios utilizados pelos fraudadores para cometer crimes. Utilizam vazamento de dados, os crimes são cometidos quando os fraudadores têm acesso aos dados pessoais verídicos. Após os dados serem vazados (dados biométricos, imagens de documentos, informações pessoais) uma pessoa pode se passar pela outra por meio de uma fraude de identidade.

Outra forma recorrente de aplicação de golpes é o uso do chip de celular, com a intenção de juntar dados pessoais das vítimas, tendo assim acesso aos aplicativos das vítimas, inclusive os dos bancos. Os criminosos não roubam necessariamente os aparelhos telefônicos, roubam as linhas telefônicas, que podem ser feitos a distância. Reunindo dados pessoais das vítimas, depois entram em contato com a operadora telefônica da vítima, e solicitam a portabilidade do número para outro chip. Eles solicitam o envio de token do banco para ter acesso aos aplicativos. O setor de telefonia é a área mais atingida pelos golpistas, em seguida os bancos e outras instituições financeiras. Isso porque, apenas com alguns dados pessoais e o número de telefone é possível fraudar aplicativos e serviços de autenticação em dois fatores, e-mails, telefone, mensagens de texto são etapas comuns no processo de verificação. Sendo assim as apropriações podem acontecer em qualquer conta vinculada ao telefone. Munir a população de informações de como são esses crimes de roubo de identidade virtual e consequentemente fornecer informações úteis para a proteção dos seus dados virtuais

A busca de segurança e métodos seguros é uma constante, já que as fraudes são criadas na medida em que a tecnologia evoluí.

Com o aumento dos crimes cometidos de forma virtual, principalmente, com a evolução dos golpes aplicados pelos criminosos, invasão das informações dos usuários como informações de banco, acesso aos dados pessoais, conseguimos identificar uma falha internet de informar aos seus usuários formas primordiais que poderiam ser utilizados frequentemente para evitar esses tipos de furto de identidade.

REFERÊNCIAS

CÓDIGO PENAL BRASILEIRO. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848. Acesso em 29 de março de 2023.

FREITAS, C. C. G. de; GONÇALVES, J. R.; TORRES, M. G. A evolução do direito penal brasileiro relacionado aos crimes cibernéticos. **Revista JRG de Estudos Acadêmicos**, Brasil, São Paulo, v. 6, n. 12, p. 296–311, 2023. DOI: 10.5281/zenodo.7760710. Disponível em: http://revistajrg.com/index.php/jrg/article/view/520. Acesso em: 3 abr.

2023.

LIMA, Adriano Gouveia; DUARTE, Adrienne..Crimes virtuais: conceito e formas de investigação. **Boletim Jurídico**, Uberaba/MG, a. 19, nº 990. Disponível em *https://www.boletimjuridico.com.br/artigos/direito-penal/10382/crimes-virtuais-conceito-formas-investigacao*. Acesso em 21 de março de 2023.

TEIXEIRA, Ronaldo de Quadros. **Os Crimes Cibernéticos no Cenário Nacional.** Escola superior aberta do Brasil – ESAB, 2013 (Curso de pós-graduação lato sensu em engenharia de sistemas)