1 INTRODUÇÃO

Com o avanço da globalização, na qual ficou possível a conexão entre o mundo todo, ficou cada vez mais fácil a interação tanto econômica, social, cultural e politica entre a sociedade e com esse advento se faz presente a conexão em redes socias permitindo que todos se conectem independe de distância. Desta forma, o que entra em pauta, a cerca do nosso tema, é a questão dos crimes em redes sociais, que essa facilidade de acesso vem possibilitando. Esse processo só é possível, devido ao avanço das tecnologias dos meios de telecomunicação, que permitem o rápido fluxo de informação, pessoas e golpes.

Para tanto, é crucial examinar que as redes sociais não apenas facilitam a comunicação global, mas são utilizadas como ferramentas por indivíduos envolvidos em atividades criminosas tais como: roubo de identidade e senha, cobrança fraudulenta, fraude via e-mail, falsa identidade induzindo o individuo a determinado golpe. Em nosso tema iremos frisar a respeito desses crimes diante das redes sociais.

Diante dos crimes em relação ao roubo de identidade destaca-se ser um dos tipos mais comuns de crimes virtuais, os roubos de identidade e de senha podem servir para alavancar outros muitos delitos, como compras indevidas, transações financeiras, realizar empréstimos pessoais em nome da vítima, dentre outros delitos. Nas cobranças fraudulentas, fraude via e-mail acontece na maioria das vezes com acessos pessoais da vítima e também em golpes via link, caso muito comum a cerca do tema debelado.

“Segundo dados do Instituto Brasileiro de Geografia e estatística, 82,7 % dos domicílios nacionais possuem acesso à internet, sendo o Brasil o terceiro país que mais utiliza as redes sociais. As redes sociais de um modo geral, possibilitam a interação de pessoas e possuem recursos abrangentes com inúmeras funcionalidades. Muitos usuários utilizam as redes de forma “correta”, entretanto para alguns, estar encoberto por uma tela gera uma falsa impressão de impunidade, e leva em alguns casos a prática de crimes”. Diante do exposto, feito pela autora no site do jus Brasil Joice Pio, a internet possibilita o fácil acesso e ao mesmo tempo gera crimes e isso se faz presente ao não uso correto das vias de rede, ocasionando o prejuízo futuro a quem se utiliza de maneira correta e por alguma circunstância acaba caindo em determinado golpe.

2 TIPIFICAÇÃO DOS CRIMES DE ACORDO COM OS INSTRUMENTOS LEGAIS E ARGUMENTOS

"Os crimes em questão, variam de menor potencial ofensivo a maior, e normalmente são geradores de danos morais, financeiros e até mesmo físico a depender do caso concreto, sendo tipificados em alguns instrumentos legais, dentre eles a Constituição Federal, Código Penal e também leis esparsas como a Lei Geral de Proteção de Dados e o Marco Civil da Internet (Lei nº 12.965/2014).

A Constituição Federal trata dos direitos fundamentais e determina que seu maior bem a ser tutelado é a pessoa humana, possuindo assim seus direitos que estão discriminados pelo texto legal. Em cada título da Constituição, temos as garantias que o Estado deve fornecer ao cidadão. O artigo 5º, por exemplo, indica que todos são iguais perante a lei, e dispõe sobre questões como direito à vida, liberdade, segurança, igualdade, e a propriedade.

O artigo 5º, inciso x, da Constituição Federal (BRASIL,1988), diz: Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; Baseados no artigo 5º da Constituição Federal, podemos determinar que embora temos o direito à informação e a liberdade de expressão, nada justifica a utilização desses conteúdos para cometer crimes.

Além da Constituição Federal, temos outros dispositivos legais pertinentes, como a Lei 12.735/2012 que alterou o Código Penal tipificando as condutas realizadas mediante uso de sistema eletrônico, digital ou semelhantes, que sejam praticadas contra sistemas informatizados e similares, bem como a Lei 12.737/2013, conhecida como Lei Carolina Dieckman que dispõe sobre a tipificação criminal de delitos informáticos, determinando os crimes digitais propriamente ditos, como a criação e disseminação de vírus computacional, e não aqueles comuns praticados por meio do computador. Não podemos deixar de citar a Lei Geral de Proteção de Dados, que estabelece o tratamento de dados pessoais por empresas públicas e privadas, objetivando a segurança jurídica. Temos também a Lei 14.155 de 2021, que dispõe sobre os crimes de violação de dispositivo informático, furto e estelionato, tornando mais graves os crimes cometidos pela internet.

Analisar o desenvolvimento desfreado da tecnologia, bem como o dinamismo das redes sociais acaba por muitas vezes não sendo acompanhado pela burocracia da máquina do judiciário. Além do mais, a falta de ferramentas adequadas para buscar e identificar os autores é um assunto a ser discutido. Consequentemente, todos esses fatores acabam perpetuando para que os crimes sejam cometidos." Em suma, fica evidente que o Brasil tem leis e artigos que garantem o cidadão tanto em liberdade de fazer determinado ato, quanto de garantia de sigilo em redes socias, no entanto, fica claro a dificuldade de conciliação de ambos e que não da para fiscalizar tudo e todos mesmo com leis.

Verificar o avanço das redes sociais e apresenta tanto desafios quanto oportunidades significativas para o direito penal. À medida que a tecnologia evolui rapidamente, é crucial adaptar constantemente as leis e as práticas de aplicação da lei para proteger efetivamente indivíduos e a sociedade em geral. Uma abordagem eficaz requer leis atualizadas, cooperação internacional e o uso adequado das ferramentas digitais disponíveis para combater as redes criminais que emergem nas plataformas de mídia social.

Na investigação dos crimes em redes sociais dentro da esfera do direito penal, várias abordagens são empregadas para garantir uma análise abrangente e eficiente. Primeiramente, a análise forense digital desempenha um papel crucial ao identificar e coletar provas eletrônicas, permitindo reconstruir a sequência de eventos e estabelecer a autoria dos delitos. Isso envolve o uso de ferramentas especializadas para examinar dispositivos e plataformas online, assegurando a integridade das evidências.

Além disso, a pesquisa jurídica e legislativa desempenha um papel fundamental na interpretação das normativas aplicáveis aos crimes cibernéticos, avaliando como essas leis se aplicam em contextos específicos e quais medidas legais podem ser adotadas. Paralelamente, a cooperação internacional entre autoridades é essencial para investigações que transcenderem fronteiras, exigindo protocolos eficientes de troca de informações e colaboração entre países.

Por fim, análises detalhadas, ou seja, um método aplicado das tendências criminais em redes sociais oferece insights sobre os comportamentos dos criminosos virtuais e suas estratégias, orientando o desenvolvimento de políticas públicas e estratégias de aplicação da lei mais eficazes. Essas metodologias combinadas estabelecem uma base sólida para lidar com os crescentes desafios relacionados aos crimes digitais nas redes sociais. Destaca também método indutivo, com analises descritivas e procedimento técnico com base em bibliografia, documentos.

3 TIPOS DE GOLPE EM REDES SOCIAIS E COMO PREVINIR

Os cybers crimes têm se tornado cada vez mais sofisticados e frequentes, especialmente com a evolução da tecnologia e a crescente dependência das pessoas pela internet. Um dos métodos mais comuns utilizados por criminosos digitais é o golpe por meio de compartilhamento de links maliciosos. Este tipo de ataque pode assumir várias formas, mas geralmente visa roubar informações pessoais, financeiras ou distribuir malware.

Tipos de Golpes por Compartilhamento de Links

Phishing: O phishing é uma técnica em que o criminoso envia um e-mail, mensagem de texto ou mensagem em redes sociais que aparenta ser de uma fonte confiável, como um banco, uma loja online ou até mesmo um conhecido. O link na mensagem direciona a vítima para um site falso que imita o original. Seu é coletar informações sensíveis, como nomes de usuário, senhas, números de cartão de crédito e outras informações pessoais.

Spear Phishing: Uma variação mais direcionada do phishing, onde o criminoso personaliza a mensagem com informações específicas sobre a vítima para aumentar a credibilidade do golpe. Geralmente utilizado para obter acesso a sistemas corporativos ou informações confidenciais de indivíduos de alto perfil.

Ataques de Ransomware: Neste tipo de ataque, a vítima é induzida a clicar em um link que baixa automaticamente um malware no dispositivo. Esse malware criptografa os arquivos da vítima e exige um pagamento (resgate) para que o acesso aos dados seja restabelecido. Tem o objetivo de extorquir dinheiro da vítima em troca do desbloqueio dos dados criptografados.

Malvertising: Este golpe envolve a inserção de links maliciosos em anúncios online. Os anúncios podem parecer legítimos e podem estar em sites respeitáveis, mas ao clicar neles, a vítima é direcionada para sites que instalam malware ou coletam informações pessoais. Distribui malware ou coletar dados de forma furtiva.

Golpes de Redes Sociais: Criminosos utilizam plataformas de redes sociais para compartilhar links que prometem conteúdo interessante, como vídeos virais, ofertas de emprego, prêmios ou notícias chocantes. Estes links podem levar a sites de phishing ou baixar malware. Espionam as atividades da vítima, roubar informações ou distribuir malware.

Como se Proteger de Golpes por Links Maliciosos

Desconfie de Mensagens Não Solicitadas: Evite clicar em links em e-mails, mensagens de texto ou mensagens de redes sociais de remetentes desconhecidos ou não solicitados.

Verifique o Endereço do Link: Passe o mouse sobre o link (sem clicar) para ver o URL real. Se o endereço parecer suspeito ou diferente do esperado, não clique.

Use Ferramentas de Segurança: Utilize software antivírus e antimalware atualizado para detectar e bloquear ameaças. Extensões de navegador que verificam links também podem ser úteis.

Autenticação de Dois Fatores (2FA): Habilite a autenticação de dois fatores em suas contas online para adicionar uma camada extra de segurança.

Educação e Conscientização: Mantenha-se informado sobre os tipos mais recentes de golpes e compartilhe esse conhecimento com familiares e amigos para que todos estejam cientes dos riscos.

Verificação em Múltiplos Níveis: Ao receber um link de um contato conhecido, confirme com a pessoa se ela realmente enviou o link antes de clicar. Pode ser que a conta dela tenha sido comprometida.

Os golpes por meio de compartilhamento de links são uma ameaça crescente no mundo digital. A sofisticação desses ataques exige que os usuários da internet estejam cada vez mais atentos e informados sobre as melhores práticas de segurança. Com medidas preventivas adequadas e uma mentalidade crítica, é possível reduzir significativamente o risco de cair em golpes desse tipo.

4 CONCLUSÃO

A globalização e a evolução tecnológica trouxeram benefícios, mas também facilitaram crimes nas redes sociais, como roubo de identidade e fraudes. A legislação brasileira oferece uma base para combater esses crimes, mas enfrenta desafios devido à rápida evolução tecnológica e à complexidade das investigações. Crimes como phishing, ransomware e golpes

online exigem medidas preventivas, análise forense, cooperação internacional e conscientização dos usuários. Uma abordagem integrada e adaptável é necessária para garantir a segurança digital.

REFERENCIAS

Cybercrime The Cyber Threat. Disponível em: https://www.fbi.gov/investigate/cyber. Acesso em: 23 de jun. de 2024

Crimes cibernéticos: o que são, tipos, como detectar e se proteger. Disponível em: https://fia.com.br/blog/crimes-ciberneticos/ . Acesso em: 23 de jun. de 2024

Kapersky O que são crimes cibernéticos e como se proteger deles? Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 23 de jun. de 2024

MARQUES, Vinicius; **GLOBALIZAÇÃO**, disponível em: https://www.todamateria.com.br/globalizacao/. Acesso em: 18 de jun. de 2024

PIO, Joice; **redes sociais, avanço tecnológico e crimes virtuais, disponível em :** https://www.jusbrasil.com.br/artigos/redes-sociais-avanco-tecnologico-e-crimes-virtuais/1463978222. Acesso em: 18 de jun. de 2024

TRECSSON, Business school: **crimes virtuais: o que são? Como detectar? Dicas para se proteger, disponível em:** https://www.trecsson.com.br/blog/tecnologia-e-ciencia-de-dados/crimes-virtuais. Acesso em: 18 de jun. de 2024