ESTELIONATO ELETRÔNICO: O INIMIGO DIGITAL[1]

Caroline Batistella[2]
Erivelto Drumond Ponte[3]
Gabrielly Ogawa de Abreu[4]
Iris Portela Gomiero[5]
João Pedro Mendes de Souza[6]
Kallel Filipe dos Santos Araújo[7]
Marcello Carvalho de Araújo[8]
Rosalina Gonçalves da Cunha[9]
Vanderlei Flores de Oliveira[10]

Resumo

A presente pesquisa teórica foi realizada com o objetivo de embasar a atividade extensionista que será realizada no âmbito da disciplina "Direito Digital", sob a orientação do Prof. Dr. Henrique Savonitti Miranda, discorrendo sobre os crimes digitais cometidos nas redes sociails que atingem a sociedade de formas diversas, apresentando medidas que podem ser tomadas para mitigar as vulnerabilidades no uso dos aplicativos sociais.

Inicialmente vale destacar que as tecnologias digitais foram criadas para atender as necessidades da sociedade em tornar mais ágil e eficaz o gerenciamento do tempo em relação às suas obrigações diárias.

Porém o surgimento das redes sociais foi acompanhado pela eclosão de uma nova geração de criminosos agora munidos de uma tecnologia com potencial para aumentar seus ganhos e diminuir os riscos de serem presos, apesar da legislação correr em sentido de tornar mais gravosas as penas por estes tipos de crimes ainda estes ocorrem diariamente nas mais diversas modalidades.

Brasil criou diversos instrumentos próprios para o combate a uso ilegal de dados e informações obrigando tanto o ente público como a pessoa jurídica de direito privado a resguardar e proteger os dados das pessoas não só em ambiente digital como no físico, entre as legislações atual se destaca a Lei Geral de Proteção de Dados (LGPD) nº 13.709/18 que entrou em vigor em setembro de 2020.A legislação é uma forma de mitigar os danos sofridos pelas vítimas dos cyber crimes, contudo a maior defesa para a prevenção contra os crimes se encontra nas mãos dos próprios usuários que ao se depararem com determinadas situações em que se há dúvida da autenticidade do solicitante das informações deve aquele não passar as informações, contudo a plataforma digital deve implementar campanhas de conscientização com o objetivo de alertar aos seus usuários dos perigos de expor sem o devido cuidado e filtro a informações pessoais e aquelas mais sensíveis como dados bancários, pessoais e outros que possam expor sua intimidade.

---

[1] Pesquisa Teórica dede atividade extensionista de aproveitamento da disciplina de Direito Digital do curso *Bacharelado em Direito*, do *Centro Universitário Processus – UniProcessus*, sob a orientação do Professor Doutor Henrique Savonitti Miranda.

[2] Graduanda em Direito pelo Centro Universitário Processus – UniProcessus

[3] Graduando em Direito pelo Centro Universitário Processus – UniProcessus

[4] Graduanda em Direito pelo Centro Universitário Processus – UniProcessus

[5] Graduanda em Direito pelo Centro Universitário Processus – UniProcessus

[6] Graduando em Direito pelo Centro Universitário Processus – UniProcessus

[7] Graduando em Direito pelo Centro Universitário Processus – UniProcessus

[8] Graduando em Direito pelo Centro Universitário Processus – UniProcessus

[9] Graduanda em Direito pelo Centro Universitário Processus – UniProcessus

[10] Graduando em Direito pelo Centro Universitário Processus – UniProcessus

A utilização de ferramentas de segurança e autenticação é uma das formas mais eficazes de evitar o sucesso dos cybers criminosos em relação aos seus objetos de vontade. Atualmente os ambientes de relacionamento virtual são os mais visados pelos criminosos que visam enganar o usuário objetivando os dados destes mesmo que isto leve certo tempo, a exemplo a o WhatsApp onde as vítimas são levadas com maior facilidade a serem o vetor das fraudes que as levam a se tornarem vítimas. Mais comumente as fraudes se realizam por meio de programas que os usuários instalam inconscientemente ou impulsionados pela vontade de ter algum tipo recompensa.

No caso de se tornar vítima deve o usuário tomar providências no sentido de diminuir os danos como identificar o golpe e o tipo de golpe, capturar as evidências dos golpes, divulgação dos golpes nas redes sociais e denúncia às autoridades oficiais competentes pelas investigações em relação aos golpes e seus autores.
Palavras-chaves: crimes digitais, usuários e ferramentas de segurança

1. Introdução

Hodiernamente o uso dos meios eletrônicos tornaram-se imprescindíveis para a vida das pessoas. Diversas ferramentas são disponibilizadas para facilitar a interação, como, por exemplo: *sites*, aplicativos de dispositivos móveis, armazenamento de dados na nuvem, inteligência artificial, entre outros. (BARRETO; BRASIL, 2016).

As tecnologias digitais vieram com o fito de corroborar para a consecução mais dinâmica e eficaz das tarefas diárias das pessoas e das empresas. Por outro lado, tais facilidades geraram um novo nicho para os criminosos praticarem atos delituosos, estes que executam tais práticas criminosas por diferentes formas dentro desse universo tão amplo que a tecnologia digital.

Algumas das formas mais comumente utilizadas na atualidade são os crimes de estelionato digital. Como supracitado, estas práticas podem ser aplicadas por variados *modus operandis*. Muito em voga está a modalidade de Phishing, *fakes sites*, apresentação de falsas ofertas na internet, roubo de identidade digital para uso em caso de estelionatos nos aplicativos de mídias sociais e de mensagens, entre outros.

Tendo em vista este cenário, percebe-se a necessidade de divulgar para a sociedade a importância da utilização de mecanismos e padrões de segurança para evitar as vulnerabilidades a que estamos expostos.

2. Desenvolvimento do tema pesquisado

2.1. Estelionato eletrônico

Atualmente vivemos na era digital, cercados de tecnologia, que nos conecta quebrando fronteiras, com informações em tempo real, otimiza o nosso tempo, facilita o trabalho. Ao mesmo tempo em que nos beneficia, traz consigo muitos riscos, pois os cibercriminosos também se aprimoram para praticar seus crimes e lograr êxito com os mesmos.

As redes sociais possuem milhões de usuários ao redor do mundo, e esse grande número é um atrativo para os cibercriminosos que enxergam essa quantidade de usuários como alvos para possíveis ataques.

O estelionato eletrônico ocorre quando um criminoso aplica golpes patrimoniais através das redes sociais, contatos telefônicos, correio eletrônico, entre outros. Eles

conseguem obter dados confidenciais, como senhas, por exemplo, com o intuito de obter vantagem ilícita (BARRETO; BRASIL, 2016).

A justiça, até poucos anos atrás, não tinha ferramentas para combater esse tipo de crime que passou a ser previsto em lei. Em 2021 foi promulgada a lei 14.155, alterou o Decreto-lei nº 2.848/1940 – Código Penal – em seu artigo 155, tornando mais gravosos os crimes cometidos por meio de dispositivo eletrônicos ou informáticos, com auxilio ou não da internet. (BRASIL, 1940).

A disposto legal do art. 155 do CP teve acrescido o parágrafo 4º-B, com a seguinte redação:

> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
> Pena - reclusão, de um a quatro anos, e multa.
>
> [...]
>
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.

O art. 171 do CP nos parágrafos 2º-A, § 2º-B e § 3º do Código Penal descreve o tipo penal do crime de estelionato e suas peculiaridades definido a pena a ser imputada aos agentes infratores, com a seguinte redação:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.
>
> [...]
>
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. (Incluído pela Lei nº 14.155, de 2021)
> § 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

A lei 14.155 no artigo 2º alterou a redação do artigo 70 do Código de processo Penal que inseriu a competência jurisdicional legal para julgar tais crimes.

> Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.
> [...]
> § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de

> valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.

2.2. Lei de proteção de dados

A Lei n° 13.709, de 14 de gosto de 2018 – Lei Geral de Proteção de Dados (LGPD), inspirada pelo Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, reconhece a relevância intrínseca de cada dado pessoal, ampliando sua compreensão de acordo com a legislação europeia (TEFFÉ; VIOLA, 2020).

A definição de dado pessoal engloba informações associadas a indivíduos identificáveis ou identificados, enfatizando que dados inicialmente insignificantes ou aparentemente irrelevantes podem se tornar específicos após processamento (TEFFÉ; VIOLA, 2020).

Conforme a LGPD, a manipulação de dados pessoais requer justificação legal, aplicável a entidades públicas e privadas, incluindo contextos digitais (TEFFÉ; VIOLA, 2020). A base legal é fundamental, não apenas para exceções sob o Art. 4º da LGPD (TEFFÉ; VIOLA, 2020).

Dentre as opções legais, destaBca-se o consentimento do titular, regulamentado pelo Art. 7º da LGPD. Consentimento, definido como manifestação livre, informada e inequívoca do titular, é central na LGPD para proteger direitos e liberdades individuais (TEFFÉ; VIOLA, 2020).

> [...]
>
> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;

Dados sensíveis, por outro lado, são minuciosamente listados no Art. 5º, II, da LGPD, abrangendo categorias como origem racial e opiniões políticas. Lidar com esses dados requer precaução, devido ao potencial risco aos direitos do titular.

> [...]
>
> Art. 5º Para os fins desta Lei, considera-se:

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

A LGPD busca instituir um referencial legal que assegure privacidade e direitos individuais na era tecnológica. Define bases legais para tratar dados, regulamenta o consentimento e aborda dados sensíveis. Seu objetivo é evitar riscos à privacidade, garantir informações seguras e responsáveis, levando em conta as necessidades contemporâneas (TEFFÉ; VIOLA, 2020).

Examinando exemplos práticos concretos de aplicação da LGPD, notamos situações como a necessidade de empresas que enviam e-mails de marketing aos clientes obterem consentimento claro e prévio dos destinatários, comunicando a finalidade, a forma e a duração do tratamento dos dados, bem como os métodos para exercer os direitos dos titulares.

Em relação à segurança, um aplicativo que coleta dados biométricos dos usuários deve garantir que essas informações sejam usadas somente para fins específicos e legítimos, armazenando-as com segurança e confidencialidade, prevenindo vazamentos ou acessos não autorizados. No ambiente online, um site que utiliza cookies para personalizar a experiência dos visitantes deve esclarecer quais tipos de cookies são utilizados, para quais finalidades e por quanto tempo, enquanto solicita o consentimento dos usuários antes de ativá-los, permitindo que possam recusar ou retirar o consentimento a qualquer momento.

No âmbito das atualizações mais recentes sobre a LGPD, destaca-se a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por supervisionar e orientar as atividades relacionadas à LGPD no Brasil. Além disso, as sanções administrativas previstas na LGPD entraram em vigor a partir de agosto de 2021, impondo penalidades por infrações à lei. Adicionalmente, o Projeto de Lei nº 500/2021 foi aprovado, introduzindo modificações em dispositivos da LGPD e estabelecendo novas regras para o tratamento de dados pessoais pelo setor público.

> Art. 65. Esta Lei entra em vigor:
> I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e
> I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54;
> II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos.

Por fim, é válido ressaltar aspectos menos conhecidos da LGPD. Ela não é aplicável aos dados pessoais empregados exclusivamente para fins jornalísticos, artísticos ou acadêmicos, o que visa proteger a liberdade de expressão e a pesquisa. Além disso, a LGPD não se aplica aos dados pessoais transferidos de ou para outros países, desde que não haja comunicação, compartilhamento ou transferência internacional desses dados. Uma particularidade interessante é que a lei autoriza o compartilhamento de dados pessoais entre órgãos e entidades públicas para executar políticas públicas, sempre que os princípios e garantias da legislação forem mantidos.

Essa legislação, fundada em princípios robustos e orientada pela proteção da privacidade e dos direitos individuais, estabelece uma base sólida para lidar com os desafios do cenário digital atual. A LGPD não apenas influencia a forma como empresas e instituições coletam e tratam dados pessoais, mas também fomenta uma

cultura de responsabilidade, transparência e respeito às liberdades individuais em um mundo cada vez mais conectado.

2.3. Medidas de segurança para evitar o estelionato

A segurança nas redes sociais assume uma relevância cada vez maior, dada a escalada dos incidentes de estelionato eletrônico. De acordo com Sousa (2021), a conscientização dos usuários desempenha um papel crucial na mitigação dos golpes nas redes sociais. A rápida evolução das estratégias utilizadas por cibercriminosos exige que os usuários estejam bem informados sobre os riscos e sejam capazes de identificar e evitar possíveis ameaças.

O termo "phishing" se refere a um tipo de ataque cibernético que busca enganar os usuários de internet para que revelem informações pessoais, financeiras ou sensíveis, como senhas, números de cartão de crédito e dados de identificação. Os cibercriminosos que realizam ataques de phishing frequentemente se fazem passar por entidades confiáveis, como bancos, empresas legítimas ou organizações governamentais, usando mensagens falsas por e-mail, mensagens instantâneas ou outros canais de comunicação eletrônica.

Essas mensagens costumam conter links maliciosos ou direcionar os usuários a sites falsos que imitam a aparência de sites autênticos. O objetivo final é convencer os usuários a compartilhar informações confidenciais, que são posteriormente usadas para atividades fraudulentas, como roubo de identidade, fraude financeira e até mesmo acesso não autorizado a sistemas sensíveis (MONTAGNER; WESTPHALL, 2022)

A prevenção contra phishing envolve a conscientização dos usuários sobre os sinais de alerta e a adoção de medidas de segurança, como não clicar em links suspeitos, verificar cuidadosamente os remetentes de e-mail, evitar compartilhar informações sensíveis em resposta a mensagens não solicitadas. É fundamental que os usuários sejam educados sobre os indicadores comuns de risco, nesse sentido, Mitnick e Simon (2017) destacam a importância das plataformas de redes sociais em promover campanhas de conscientização, oferecer guias de segurança e facilitar o acesso a recursos de denúncia para atividades suspeitas.

A educação também deve abordar a relevância de manter senhas robustas e únicas para cada plataforma. Nesse contexto, Oliveira (2022) enfatiza que os usuários devem ser incentivados a não compartilhar senhas, bem como habilitar a autenticação de dois fatores (2FA) e revisar regularmente suas configurações de privacidade.

A autenticação de dois fatores (2FA) emerge como uma medida essencial para fortalecer a segurança online. Conforme discutido por Oliveira (2022), a 2FA requer uma segunda forma de autenticação, como um código enviado via SMS, um aplicativo autenticador ou uma impressão digital, além da senha tradicional. Esse método cria uma barreira adicional que impede o acesso não autorizado, mesmo no caso de comprometimento da senha.

Ao adotar a 2FA, os usuários garantem que apenas eles possam efetuar o login, uma vez que a etapa adicional de autenticação está vinculada ao seu dispositivo pessoal. Isso proporciona proteção contra tentativas de invasão, mesmo no cenário em que terceiros obtenham acesso à senha.

As plataformas de redes sociais frequentemente oferecem suporte à 2FA e incentivam os usuários a ativá-la. A configuração desse método é geralmente simples e acrescenta uma camada extra de segurança sem gerar complexidade excessiva ao processo de login (SILVA; ARAÚJO; AZEVEDO, 2013)

A conscientização dos usuários e a implementação da autenticação de dois fatores são medidas eficazes para combater os golpes nas redes sociais. Ao compreender os riscos e seguir práticas de segurança robustas, os usuários podem melhor proteger-se contra ameaças virtuais e manter uma presença segura no ambiente online.

2.4. Whatsapp

Atualmente os aplicativos de mensagens instantâneas se tornaram ferramentas essenciais no dia a dia das pessoas.

Com tamanha importância, alcance e facilidade de uso, seria inevitável o aparecimento dos mais variados tipos de golpes com o intuito de causar prejuízo aos usuários.

De acordo com o site globo.com, um levantamento da empresa de segurança digital PSafe, feito em 2020, estimou que, só em outubro daquele ano, 453 mil pessoas tiveram o WhatsApp clonado ou tiveram a conta falsificada - uma média de 15 mil vítimas por dia. (G1, 2022).

Qualquer pessoa pode ser vítima desses golpes, porém os mais vulneráveis são os que têm pouca familiaridade com os aplicativos.

Entre esses aplicativos, o WhatsApp é um dos mais utilizados no mundo e consequentemente o que mais atrai os golpistas. Se aproveitando de momentos de distração do usuário, criminosos praticam roubos de senhas e dados pessoais para tirar alguma vantagem ilícita. (ESET, 2023).

É imprescindível conhecer as estratégias utilizadas pelos golpistas para identificar e minimizar os riscos inerentes desses aplicativos de mensagens instantâneas. (ESET, 2023).

Em um dos golpes, o criminoso utiliza um número novo, mas com foto roubada de um conhecido da vítima. O objetivo é se passar por esse conhecido para solicitar alguma vantagem financeira. O criminoso usa alguma desculpa e se nega a aceitar ligação por voz ou vídeo, argumentando que está impossibilitado no momento de receber tais ligações. Demonstra urgência na transferência para não dar muito tempo à vítima para perceber o golpe e assim conseguir a transferência. (ESET, 2023).

O Auxílio econômico falso. Neste tipo de golpe, os criminosos se passam por representantes de benefícios governamentais. As vítimas recebem uma mensagem com a informação de que tem algum auxílio do governo e que precisam fazer um cadastro para terem acesso ao direito. O objetivo é conseguir informações pessoais que podem ser vendidas ou utilizadas para invasão das contas bancárias. (ESET, 2023).

O phishing se refere a golpes em que o criminoso se passa por uma entidade confiável e se apodera também de informações pessoais. Utilizam mensagens com arquivos infectados, com falsas mensagens de promoções, serviços, ofertas e cobranças de sites conhecidos. Porém os links redirecionam para páginas falsas e novamente para fornecer dados pessoais. (ESET, 2023).

A Clonagem do número de WhatsApp da vítima é mais um golpe muito utilizado. O usuário recebe ligações ou mensagens com um conteúdo atrativo e convincente. O objetivo é conseguir o código de seis dígitos. Com esse código clona o mensageiro, acessa os contatos, conversas, grupos e informações pessoais no aplicativo. (ESET, 2023).

É mais um golpe que põe em risco os contatos do número clonado, pois o criminoso tenta dar golpes se passando pela vítima. (ESET, 2023).

Aplicativos de spyware, conhecidos como aplicativos espiões, são utilizados também por criminosos no WhatsApp para dar golpes. É uma forma semelhante ao golpe de phishing. Os links encaminhados na mensagem direcionam o usuário para baixar programas maliciosos, que dão acesso às informações do seu celular, inclusive aos códigos de verificação do WhatsApp. (ESET, 2023).

Golpe do falso emprego. A vítima recebe uma mensagem com uma suposta vaga de emprego. Geralmente atrativas e com salários ótimos e outras vantagens. Os criminosos solicitam quantias em dinheiro para garantir a vaga. Nesse golpe também podem enviar links e arquivos maliciosos. (ESET, 2023).

Falsas atualizações do WhatsApp. Os usuários recebem mensagens com links, informando sobre falsas atualizações do aplicativo, normalmente se referindo a uma nova versão com recursos diferentes do aplicativo. Esses links direcionam a vítima para versões alternativas, não oficiais, como WhatsApp Rosa ou WhatsApp Plus. Ao clicar, vírus são instalados no celular. (ESET, 2023).

2.5. Como Relatar Golpes às Plataformas de Redes Sociais

Diante dessa intensa organização de crimes de estelionato eletrônico, isso tem gerado crescente preocupação entre os usuários. Relatar tais atividades fraudulentas é de extrema importância para diminuir a disseminação desses crimes e proteger a comunidade, principalmente para aquelas pessoas que possuem dificuldade em utilizar celulares, computadores ou tablets, tendentes a se tornarem alvo ainda mais fácil para essas organizações criminosas, tornando-se assim, alvos vulneráveis. Segundo Alexandre Armellini, diretor de Red Team da Cipher, as crianças, jovens, adolescentes e idosos são mais vulneráveis a crimes digitais e fraudes e golpes digitais. De acordo com Armellini:

> “Os bandidos se aproveitam da ingenuidade, impulsividade ou dificuldade com o mundo digital de suas vítimas, para elaborar golpes cada vez mais ousados e sofisticados”.

Dessa forma, apresentamos um passo a passo sobre como relatar golpes às plataformas de redes sociais e denunciar as atividades fraudulentas às autoridades competentes.

<u>Passo 1: Identificação do Golpe</u>

Talvez seja esse o passo mais difícil, pois para muitas pessoas, essa identificação do golpe ocorre quando a pessoa se torna vítima dele. Nesse sentido, observe mensagens suspeitas ou fraudulentas, como por exemplo aquelas costumeiras mensagens recebidas pelo SMS, pedindo para acessar um link, ou pedindo para dar a confirmação de um código, etc. (Neon, 2022).

Observe também a criação de perfis falsos, procure verificar se aquela página possui muitos seguidores, e até mesmo se esses usuários que seguem a página são verdadeiros, analisando por meio de fotos no perfil e nome comum. Verifique se essa página possui comentários ativados, bem como se existem críticas nesses comentários falando do produto ou do envio e chegada deste produto, de modo que, normalmente, os golpistas tendem a apagar tais mensagens para que nenhuma pessoa leia e saiba que aquela página é fake.

Desconfie de produtos e / ou serviços com valores muito abaixo do mercado, bem como de sites que transferem a forma de pagamento para aplicativos de conversa. (Neon, 2022).

Segundo o site Neon (2022), sempre desconfie se alguém solicitar informações pessoais, como por exemplo informações bancárias, dados de cartões, código de segurança do cartão, senha de aplicativos, etc. Na dúvida, procure sempre o site oficial da empresa ou do aplicativo e verifique como é feito o correto procedimento, procure o Serviço de Atendimento ao Consumidor (SAC) ou ligue diretamente com o número oficial da empresa para se resguardar de possíveis fraudes.

Se ainda assim, não conseguir identificar se a empresa é fruto de um golpe, a empresa Time BL Consultoria (2023), informa para fazer uma verificação mais detalhada. Verifique se a loja disponibilizou as informações obrigatórias por lei como, CNPJ, Razão Social, Endereço da sede da empresa, telefone, e-mail ou formulário para contato.

Consulte se o CNPJ da loja consta no site da Receita Federal, bem como se a loja consta na lista do Procon. Verifique ainda se a loja protege seus dados e se possui certificado SSL e fique atento ao endereço (URL) de sites. (Time BL Consultoria, 2023).

Passo 2: Captura de Evidências

Se você verificar que tal mensagem ou página é fruto de um golpe, ótimo, você não se tornará vítima desse crime. Porém, é importante alertar os outros usuários a não caírem nesse golpe. Dessa forma, tire screenshots dessas interações suspeitas, perfis envolvidos ou qualquer evidência relacionada ao golpe. Essas evidências servirão de provas para relatar a situação e serão essenciais. (MPMG, 2021).

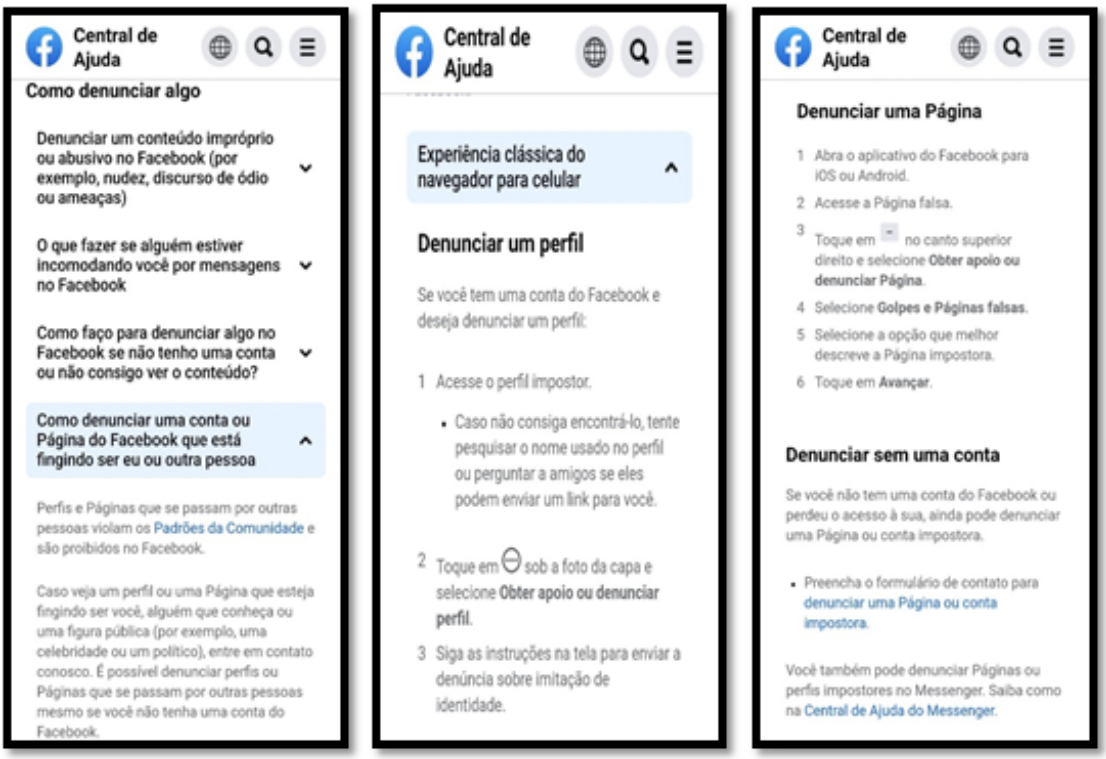
Passo 3: Relatório à Plataforma de Rede Social

Acesse as configurações de ajuda ou suporte da plataforma e siga os procedimentos para denunciar o perfil ou postagem fraudulenta. Forneça todas as evidências capturadas e descreva detalhadamente o ocorrido.Quando um post é reportado, as empresas analisam e firmam uma decisão de acordo com a política da plataforma, evitando fraudes e estelionatos, entre outros conteúdos inadequados (G1, 2023).

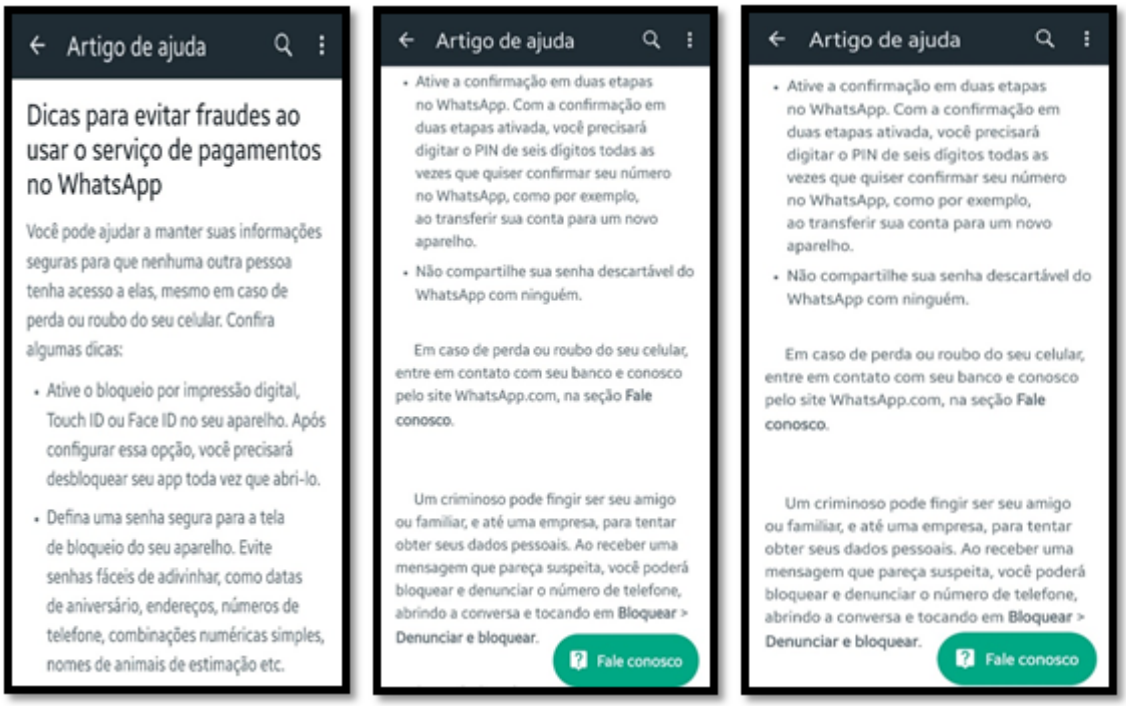
Abaixo, estão exemplos de alguns aplicativos informando seus usuários de como denunciar uma página ou publicação que desconfiem ser golpistas ou fraudulentas.

- Instagram:

- Facebook:



- WhatsApp:



<u>Passo 4: Compartilhe com sua Rede</u>

Alerte amigos e familiares sobre esse golpe, evitando que mais pessoas caiam nessa armadilha. Lembre-se, quanto mais o compartilhamento e a informação acerca

de um golpe, mais protegidas e menos propensas a se tornarem vítimas estarão, especialmente os mais vulneráveis, como os idosos e as crianças, explicando como vem acontecendo esses golpes de estelionato eletrônico e ensiná-los a se protegerem. (MPMG, 2021)

Nota-se que, ao aprender como se proteger e denunciar esses crimes de estelionato eletrônico, aprende-se diversas outras informações importantes como, o ativamento do bloqueio por meio de impressão digital, Touch ID ou Face ID, ou a criação de uma senha para a tela de bloqueio do aplicativo. Tudo isso contribui para a segurança no aparelho do usuário, prejudicando ainda mais a consumação deste crime.

Passo 5: Denúncia às Autoridades Competentes

Se o golpe envolver atividades criminosas, como roubo de dados pessoais ou fraudes financeiras, denuncie à Polícia Civil ou ao Ministério Público. Entregue todas as evidências disponíveis.

Ao adotar medidas proativas e denunciar golpes, contribuímos para a segurança e integridade das redes sociais. A conscientização e a ação coletiva são essenciais para reduzir o impacto do estelionato eletrônico em nossa sociedade digital.

Faça um Boletim de Ocorrência, levando as evidências a uma delegacia para formalizar a denúncia do caso, fazendo com que sejam investigadas. O ideal é que esta denúncia seja formada em uma delegacia especializada em crimes cibernéticos, presente em algumas cidades do Brasil somente, porém essa denúncia pode ser levada a qualquer delegacia. Para verificar a existência de uma delegacia personalizada, recomenda-se acessar o site Safernet, possibilitando consultar a localização e acesso a informações atualizadas com enfoque em crimes virtuais.

Endereço Eletrônico para encontrar delegacias especializadas:
https://new.safernet.org.br/content/delegacias-cibercrimes

Acesse por QR CODE direcionando a câmera de celular para o código abaixo:

3. Considerações Finais

Este trabalho cientifico se destinou a análise de crimes relacionados a estelionatos cometido pelos conhecidos cybers criminosos no âmbito do mundo virtual considerando os meios utilizados pelo qual furtam dados pessoais das vítimas e a forma que as utilizam.

Inicialmente foi discutido relevância das tecnologias digitais com filem de trazer benefícios pessoais para os usuários e tornando a vida destes mais ágil e eficaz no sentido de poder realizar mais com o mesmo tempo que se possui.

Entretanto com a tecnologia digital veio a necessidade de se ampliar a definição criminal de alguns crimes, no caso, o estelionato em meio digital (fraude eletrônico) conhecido como estelionato digital e a criação de marcos para a proteção de dados pessoais e sensíveis, vinculando as pessoas jurídicas tanto as de direito público e as de direito privado a atendimento destes marcos.

Sendo levantada que as ações criminosas podem ser mitigadas por contra ações de iniciativas públicas ou privadas realizadas por meio de trabalho de conscientização de combate aos crimes virtuais capitaneada pelos usuários uma vez que estes são as partes mais vulneráveis e que detém o poder de decisão no momento de disponibilização ou não dos seus dados.

A presente preposição acadêmica busca a demonstração de fatos que transmutam os limites da teoria e apresenta a realidade enfrentada no mundo real e no virtual onde os crimes cometidos neste se concretiza naquele.

Não se estagnando no problema identificado amplia-se a visão para a solução que se consubstancia nos próprios usuários que são as vítimas e passam a fazer parte da resolução para a trama criminosa.

Como ferramentas estatais foi destinado o conceito raiz da Lei Geral de Proteção de Dados a sua inspiração, a sua formação e por fim a concretização, porém é claro que a falta de comprometimento poderá arruinar o intuito da Lei.

Por fim o trabalho apresentado tem como finalidade a demonstração da relevância nos campos sociais, acadêmico e do direito uma vez que a primeira é beneficiada por trazer a sociedade um estudo técnico provido de informações relevantes no que tange às fraudes virtuais e as possibilidade de combate a estas espécie criminosa, no campo acadêmico o estudo por ser mais um norte da forma que para a orientação de acadêmicos interessados no assunto de tão vultuoso campo para estudo e discursão e por fim não menos importante a relevância do tratado em relação ao campo do direito se fixa na importância trazida do estudo para ampliar de forma assertiva do interesse da legislação ao assunto de interesse intersocial e multidisciplinar.

Referências

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à Luz do Marco Civil da Internet**. 1. ed. São Paulo: Brasport, 2016.

BRASIL. Decreto-Lei 2.848, de 7 de dezembro de 1940. **Código Penal**. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 19 ago. 2023.

BRASIL. Decreto-Lei 3.689, de 3 de outubro de 1941. **Código de Processo Penal**. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acessado em: 19 ago. 2023.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 19 ago. 2023.

BRASIL. Lei n. 14.155, de 27 de maio de 2021. **Alteração do Código Penal e Código de Processo Penal**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 19 ago. 2023.

Como Bloquear e Denunciar Contatos. **Whatsapp. Central de Ajuda**. Disponível em: <https://faq.whatsapp.com/1142481766359885/?locale=pt_BR&cms_platform=android> Acesso em: 22 ago. 2023.

Como denunciar posts em Facebook, Instagram, TikTok, Kwai e outras redes sociais. **G1.Globo**. 20/04/2023. Disponível em: <https://g1.globo.com/tecnologia/noticia/2023/04/20/como-denunciar-posts-em-facebook-instagram-tiktok-kwai-e-outras-redes-sociais.ghtml> Acesso em: 25 ago. 2023.

Como surgiu a Lei Geral de Proteção de Dados (LGPD)?. **Acervo 30**. Disponível em: https://acervonet.com.br/blog/como-surgiu-a-lei-geral-de-protecao-de-dados-lgpd/. Acessado em 20 ago. 2023.

CORÁGEM, Ana Carolina Corágem Campos. LGPD: 13 conceitos básicos para começar a entender. **Conhecimento**. Acesso em: 18/08/2023. Disponível em <https://institutolegado.org/blog/lgpd-13-conceitos-basicos-para-comecar-a-entende/> Crianças e Adolescentes são mais vulneráveis a golpes na internet. Estado de Minas. 2023. Disponível em: https://www.em.com.br/app/noticia/saude-e-bem-viver/2023/02/14/interna_bem_viver,1457282/criancas-e-adolescentes-sao-mais-vulneraveis-a-golpes-na-internet.shtml. Acesso em: 25 ago. 2023.

Denunciar perfis falsos do Facebook. Facebook. **Central de Ajuda**. Disponível em: <https://pt-br.facebook.com/help/306643639690823/?helpref=related_articles> Acesso em: 22 ago. 2023.

Dicas e curiosidades sobre a LGPD. UPLexis. 2020. Disponível em: https://uplexis.com.br/blog/artigos/lgpddicas-e-curiosidades-sobre-a-lgpd/. Acessado em 20 ago. 2023.

Estelionato Digital: MPMG intensifica atuação para combater golpes pelo WhatsApp em MG. **MPMG**. 2021. Disponível em: https://www.mpmg.mp.br/portal/menu/comunicacao/noticias/estelionato-digital-mpmg-intensifica-atuacao-para-combater-golpes-pelowhatsappem-mg-8A9480687CEBDB46017CF0ECEB305789-00.shtml. Acesso em: 25 ago. 2023.

FEITOSA, Larissa Saiba como identificar golpes de estelionato eletrônico e como se proteger. **O Popular**. 2023. Disponível em: <https://opopular.com.br/cidades/saiba-como-identificar-golpes-de-estelionato-eletronico-e-como-se-proteger-1.3051269> Acesso em: 22/08/2023.

GARRETT, Filipe. Crimes cibernéticos: entenda o que são e como denunciar. Techtudo, 2021.Disponível em: https://www.techtudo.com.br/noticias/2021/08/crimes-ciberneticos-entenda-o-que-sao-e-como-denunciar.ghtml. Acesso em: 19 ago.2023.

Golpes em rede social: conheça os mais comuns e saiba como evitá-los. **Security Report**. Disponível em: https://www.securityreport.com.br/golpes-em-rede-social-conheca-os-mais-comuns-e-saiba-como-evita-los/. Acesso em: 19 ago. 2023.

Golpes no Instagram: conheça e evite as ciladas mais comuns. **Time Neon**. 2022. Disponível em: <https://neon.com.br/aprenda/seguranca-digital/golpe-no-instagram/> Acesso em: 22 ago. 2023.

Golpe na Internet: O que fazer caso seja vítima de um Estelionato Virtual. **Time BL Consultoria**. 2023. Disponível em: <https://blconsultoriadigital.com.br/golpe-na-internet-estelionato-virtual/> Acesso em: 22 ago. 2023.

Golpe do Whatsapp: os principais tipos e como funcionam. **ESET**. 2023. Disponível em: https://www.eset.com/br/artigos/golpe-do-whatsapp/. Acesso em: 21 ago.2023.

Golpes no Whatsapp: como se proteger e o que fazer se for vítima. **G1-Tecnologia**. 2022. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/02/24/golpes-no-whatsapp-como-se-proteger-e-o-que-fazer-se-for-vitima.ghtml. Acesso em: 21 ago.2023.

GONÇALVES, Jonas Rodrigo. **Como escrever um Artigo de Revisão de Literatura. Revista JRG de Estudos Acadêmicos**, Ano II, Vol. II, n.5, 2019.

GONÇALVES, Jonas Rodrigo. **Manual de Artigo de Revisão de Literatura**. 3.ed. Brasília: Processus, 2021.

GONÇALVES, Jonas Rodrigo. **Metodologia Científica e Redação Acadêmica**. 8. ed. Brasília: JRG, 2019.

LGPD: 13 conceitos básicos para começar a entender. **Legado**.2021. Disponível em: https://institutolegado.org/blog/lgpd-13-conceitos-basicos-para-comecar-a-entender/. Acessado em 20 ago. 2023.

MITNICK, Kevin D.; SIMON, William L. A Arte de Enganar: Ataques de Hackers: **Controlando o Fator Humano na Segurança da Informação**. 2. ed. São Paulo: Alta Books, 2017.

MONTAGNER, Antônio S.; WESTPHALL, Carla Merkle. Uma breve análise sobre phishing. **Revista ComInG - Communications and Innovations Gazette**. 2022. Disponível em: https://periodicos.ufsm.br/coming/article/view/71731. Acesso em: 20 ago. 2023.

O que são crimes cibernéticos: Como se proteger dos crimes cibernéticos. **Kaspersky**, 2022. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybere . em: 19 ago.2023.

OLIVEIRA, Wellington Antério de. Os crimes cibernéticos e a prática de estelionato por meios eletrônicos. **Ânima Educação**. 2022. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/32940 . Acesso em: 20 ago. 2023.

Policia Civil do Rio Grande do Norte. Golpes do Whatsapp. **Blog Meu Sistema,** 2022. Disponível em: https://blog.meusistema.com.br/wp-content/uploads/2022/11/CARTILHA-POLICIA-CIVIL-GOLPES-WHATSAPP.pdf . Acesso em: 19 ago. 2023.

SILVA, N. B. X.; ARAÚJO, W. J. De; AZEVEDO, P. M. de. Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. **Revista Ibero-Americana De Ciência Da Informação**, 2013. Disponível em: https://periodicos.unb.br/index.php/RICI/article/view/1782/1573. Acesso em: 20 ago. 2023.

SOLINI, Isadora Solini. Dicas e curiosidades sobre LGPD. **UPLexis**. 2023. Disponível em <https://uplexis.com.br/blog/artigos/lgpddicas-e-curiosidades-sobre-a-lgpd/>. Acesso em: 20 ago. 2023.

SOUSA, Rafaela. Educação. **Brasil Escola**, 2021. Disponível em: https://brasilescola.uol.com.br/educacao. Acesso em: 20 ago. 2023.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**. 2020. http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/. Acessado em 20 ago. 2023.

20 exemplos práticos e reais de aplicação da LGPD. **GET Privacy**. Disponível em: https://getprivacy.com.br/exemplos-praticos-e-reais-de-aplicacao-da-lgpd/. Acessado em 20 ago. 2023.