UNIVERSIDADE DE GURUPI
CURSO DE DIREITO

DAVID BRYAN DA COSTA

ANÁLISE JURÍDICA SOBRE CRIMES DIGITAIS: FURTO DE DADOS E FALSIDADE IDEOLÓGICA

GURUPI - TO
OUTUBRO - 2024

UNIVERSIDADE DE GURUPI
CURSO DE DIREITO

DAVID BRYAN DA COSTA

ANÁLISE JURÍDICA SOBRE CRIMES DIGITAIS: FURTO DE DADOS E FALSIDADE IDEOLÓGICA

Trabalho de Conclusão de Curso apresentado à Universidade de Gurupi - UnirG, como requisito para obtenção do título de Bacharel em Direito.

Orientador: Prof. Esp. Leonardo Guimarães Torres

GURUPI - TO

OUTUBRO - 2024

ANÁLISE JURÍDICA SOBRE CRIMES DIGITAIS: FURTO DE DADOS E FALSIDADE IDEOLÓGICA, COSTA. David Bryan da[1]. ([1]Acadêmico do Curso de Direito da Universidade de Gurupi - UnirG; TORRES, Leonardo Guimarães[2] ([2]Prof. Orientador do Curso de Direito da Universidade de Gurupi - UnirG).

RESUMO

Com o avanço da internet e dos dispositivos digitais que possuem conexão à ela, vem cada vez mais sendo utilizada essa tecnologia na rotina da maioria dos brasileiros. Esses dispositivos possuem serviços que facilitam a vida de seus usuários podendo evitar atividades como: ir ao supermercado, esperar na fila de bancos, efetuar pagamento de boletos na lotérica, carregar dinheiro físico ou cartão de crédito etc. Com esses dispositivos como o computador ou celular podemos armazenar nossos dados pessoais que são muito importantes e que podem ser utilizados para realizar as atividades que foram citadas anteriormente. Mas os sistemas presentes nos aparelhos digitais possuem falhas que por conta delas ou pela falta de experiência dos usuários podem ser exploradas por criminosos, tendo como objetivo o furto de dados pessoais. Essa situação envolve o direito, já que está se tratando sobre práticas criminosas no meio virtual e na segurança de dados, a pesquisa será produzida a partir de análise bibliográfica de artigos e doutrinas, será usada a linha de pesquisa e cidadania pois tem como objetivo alertar a população brasileira sobre o furto de dados e falsidade ideológica, no âmbito virtual e no âmbito jurídico, as formas que são praticados esses crimes e as formas de se prevenir.

Palavras-chave: Crimes digitais. Furto de dados. Falsidade ideológica. Âmbito virtual e jurídico. Crackers.

LEGAL ANALYSIS OF DIGITAL CRIMES: DATA THEFT AND IDEOLOGICAL FALSEHOOD, AND IDEOLOGICAL FALSEHOOD, COSTA. David Bryan da[1]. ([1]Academic of the Law Course at the University of Gurupi - UnirG; TORRES, Leonardo Guimarães[2] ([2]Professor of the Law Course at the University of Gurupi - UnirG).

ABSTRACT

With the advance of the internet and digital devices that have a connection to it, this technology is increasingly being used in the routine of the majority of Brazilians. These devices have services that make life easier for their users and can avoid activities such as: going to the supermarket, waiting in line at banks, paying bills at the lottery, carrying physical cash or credit cards and so on. With these devices, such as a computer or cell phone, we can store our personal data, which is very important and can be used to carry out the activities mentioned above. However, the systems present in digital devices have flaws that can be exploited by criminals, either because of these flaws or because of the lack of experience of users, with the aim of stealing personal data. This situation involves the law, since it is dealing with criminal practices in the virtual environment and data security, the research will be produced from bibliographical analysis of articles and doctrines, the line of research and citizenship will be used because it aims to alert the Brazilian population about data theft and ideological falsehood, in the virtual and legal spheres, the ways in which these crimes are practiced and the ways to prevent them.

Keywords: Digital crimes. Data theft. Impersonation. Virtual and legal spheres. Crackers.

INTRODUÇÃO

O Estado brasileiro é responsável por garantir a segurança, tanto da pessoa quanto do seu patrimônio. Criminosos sempre buscam uma maneira de cometer seus atos ilícitos no anonimato. Com acesso fácil da internet, esses indivíduos desenvolveram novas técnicas para a prática de crimes virtuais, diferentes dos comuns que são realizados no meio físico.

O âmbito virtual é imaterial, um espaço onde pessoas armazenam seus dados e bens imateriais; o estado tem o dever de proteger esses dados e bens. Por se tratar de uma complexidade extrema, existe uma grande dificuldade em rastrear esses indivíduos que praticam crimes virtuais, contra uma vítima de cada vez ou várias vítimas, dependendo da técnica a ser usada.

O estelionato digital e o furto de dados são umas das práticas criminosas comuns do meio virtual que vem se tornando frequente devido a evolução da tecnologia, onde os usuários mantém seu patrimônio imaterial armazenados nos dispositivos eletrônicos com ou sem conexão com a internet, com isso surgem criminosos especializados em tecnologia que usam do conhecimento para cometer delitos, esses popularmente recebem o nome de hackers, mas o termo correto é crackers pois há uma grande diferença entre as práticas destes.

O hacker é um termo usado para quem tem um alto grau de conhecimento sobre os dispositivos digitais e internet, usando somente para descobrir falhas na segurança e reportar às autoridades que o contratou; diferente do cracker, que causam receio nos usuários, deixando-os limitados em suas buscas por não terem conhecimento necessário para detectar quando devem ou não devem abrir um simples link ou usarem seus dados pessoais, sem serem vítimas de algum crime.

Os atos praticados pelos Crackers causam medo nos usuários de internet, deixando-os limitados em sua navegação por não saberem quando poderão sofrer um ataque Cracker, que pode acontecer logo após a simples abertura de um link ou até mesmo um download de um arquivo. Precisa-se esclarecer a diferença entre o hacker e o cracker, são denominações parecidas, mas com práticas opostas. Será abordado a dificuldade do direito em combater as práticas.

O artigo tem objetivo de tratar de crimes cibernéticos e como o direito lida com

isso, o assunto busca trazer benefícios para a sociedade com análises de formas de crimes e como prevenir a fim de ensinar os usuários a se protegerem quando usarem a internet.

O presente artigo irá discorrer sobre crimes de estelionato e furto de dados que acontecem no meio virtual com dispositivos que possuem conexão com a internet, serão apresentados fatos de até 12 anos atrás envolvendo pessoas a partir de 10 anos de idade.

Por fim, o material utilizado é de fontes de confiança sendo elas, leis, doutrinas, site do governo e artigos que são relacionados ao tema; os materiais utilizados foram atualizados ou publicados a partir de 2004 com conteúdos de acordo com as leis vigentes.

1. CRIMES VIRTUAIS

Os crimes digitais são atos ilícitos praticados no meio virtual, onde ocorre acesso não autorizado de dispositivo eletrônico por meio de brechas na segurança do sistema ou por induzimento do usuário ao erro para que forneça o acesso dos seus dados pessoais. Segundo Pinheiro:

> Os crimes digitais podem ser conceituados como sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo entre outro (PINHEIRO, 2010).

Um desses crimes digitais é o estelionato virtual que na sua prática tem o objetivo de enganar os usuários a fim de obter vantagem econômica de forma ilícita, outra prática é o furto de dados decorrente da invasão do dispositivo eletrônico onde o criminoso se apropria de forma indevida dos dados pessoais, essas práticas estão previstas na Lei nº 14.155, de 2021.

Os dados pessoais são um patrimônio que é de grande importância para o usuário de dispositivo eletrônico, pois eles podem conter o número de seu CPF, senha de bancos, obras digitais, arquivos de trabalho etc. Para Tarcísio Teixeira (2022) “Um dos crimes contra o patrimônio de maior alcance é aquele em que, pela internet, os criminosos transferem quantia em dinheiro de contas de terceiros para suas próprias

contas; ou de terceiros (ou mesmo contas fantasmas) e depois se apoderam das quantias".

A prática de crimes virtuais está ocorrendo com mais frequência devido o avanço da tecnologia e as facilidades de serviços fornecidos pela internet, o brasil está no ranking ocupando a vice-liderança mundial e especialistas alertam sobre esses crimes que estão se tornando cada vez mais comuns na internet (GONÇALVES, 2024).

Deve-se dar importância para essas práticas devido estar se tornando cada vez mais comum e por se tratar de crimes contra o patrimônio que podem ter um grande alcance na internet, onde o acesso de seus dados podem trazer prejuízos irreparáveis para a vítima podendo ser uma pessoa física ou jurídica.

2. O QUE É UM HACKER E CRACKER?

Para entender os crimes digitais deve ser esclarecido quem é o agente por trás dessas práticas ilegais, começando pela compreensão de que os termos "Hacker" e "Cracker" não são palavras sinônimas para se referir a um mesmo agente (TEIXEIRA, 2022).

É muito comum ouvir notícias de ataques hackers que usam das habilidades e conhecimento da tecnologia para invadir dispositivos eletrônicos para furtar dados pessoais como senhas de contas bancárias ou fotos pessoais para divulgar podendo estragar a vida de pessoas a distância. Essas notícias acabam usando o termo errado e aderindo a práticas de crimes a um grupo de pessoas que possuem a mesma afinidade com a tecnologia, porém não usam para cometer crimes (LOPES, 2021).

O termo "Hacker" usado na forma generalizada para abordar a prática de crimes digitais, deixa um entendimento raso sobre quem é o agente que faz essas práticas criminosas; portanto para esclarecer os crimes digitais é necessário entender quem são as pessoas por trás.

2.1. Hacker

O termo surgiu em 1960 nos Estados Unidos da América, significa cortar algo

de forma grosseira, na informática o termo é usado para se referir a pessoas que possuem alto nível de conhecimento de programação (CAETANO, [2014]).

A desinformação criou um preconceito em relação ao termo “Hacker” ligando a furtos de dados e outros tipos de crimes virtuais, mas na verdade o Hacker não faz nada relacionado a essas práticas, esse preconceito faz até mesmo com que os profissionais tenham medo de se intitular como hacker, mesmo eles trazendo grandes contribuições com a proteção que eles fornecem no âmbito digital. Segundo BONAGURA:

> A definição correta para este cara é criminoso, não importa se cibercriminoso ou não; é Criminoso. Hackers não são estes caras! O que historicamente os aproximou desta confusão em relação a ter o conhecimento e as ferramentas e, portanto, ser julgado culpado pelo fato, foi exatamente o preconceito fundamentado pela superficialidade como já discutimos anteriormente. É como julgar o dono da pá culpado por todos os buracos do mundo. [...] O que quero reforçar aqui é que o que separa os Hackers dos Criminosos é exatamente o mesmo que separa qualquer outra pessoa ou profissional de fazer o certo ou o errado, ou seja, fatos, ações, finalidades e uma boa dose de caráter (BONAGURA, 2021).

Os hackers são motivados com o objetivo de ajudar os usuários de dispositivos digitais, as suas ações são para o bem das pessoas, sempre estão buscando maneiras de impedir indivíduos com intenções de cometer crimes no âmbito digital. Os hackers são contratados por empresas como Google e outras gigantes da tecnologia, para analisar e encontrar falhas de segurança nos seus produtos sendo aparelhos eletrônicos e softwares (BASTA, 2014).

Os hackers éticos são conhecidos pelo seu trabalho profissional de encontrar falhas em sistemas de empresas utilizando técnicas de ataques controlados a fim de encontrar falhas em sistemas para que os profissionais de TI “tecnologia da informática” possam corrigi-las e poder evitar uma invasão real.

2.2 Cracker

Não é comum escutar o termo “cracker” nas notícias de jornais até mesmo nas comunidades voltadas para tecnologia. Mas o que é o cracker? O cracker é muito parecido com o hacker pois ambos são especialistas em programação de softwares, aparelhos eletrônicos que possuem conexões ou não com a internet.

Mas existe diferença entre eles, enquanto o hacker trabalha ao lado da ética, o

cracker não possui ética; ele busca por falhas nos sistemas e quando as encontram não informa as empresas, ao contrário ele invade e furta informações para poder vender ou injeta programas na rede para fragilizar a segurança permitindo que ele tenha mais acesso às áreas da rede e possa cometer mais crimes.

> No início da computação, indivíduos muito especializados em codificação e na criação de soluções com o uso de computadores eram conhecidos como hackers. Essa era uma maneira típica de reconhecer as realizações da pessoa. Ao longo dos últimos 30 ou 40 anos, porém, "hacker" se tornou um termo mais pejorativo, que se refere a alguém que usa suas habilidades técnicas de forma ilegal ou antiética. Os hackers legais que queriam manter o termo "hackers" responderam a essa tendência divulgando o termo cracker para caracterizar quem está no "lado obscuro" da computação (BASTA,2014).

Os crackers obtêm dados como fotos, informações pessoais como contas bancárias, CPF, senhas de e-mails e etc. Motivados a fazerem práticas ilegais para benefício próprio, seus atos sempre causarão dano a outra pessoa, com o amplo conhecimento de informática eles desenvolvem softwares para quebrar a segurança de sistemas e obter dados.

3. ESTELIONATO DIGITAL PARA FURTAR DADOS

Existem outras formas dos crackers obterem informações que eles desejam, quando a segurança do sistema eletrônico é muito forte, uma delas é: usando métodos de manipulação a fim de manter em erro, eles fazem com que a vítima entregue seus dados pessoais sem precisar de fazer uma invasão, basta apenas se passar por alguém de confiança como, um funcionário do banco, fazendo o envio de e-mail falso contendo um link para a vítima, esse link a redirecionará para um site falso idêntico ao do banco pedindo informações pessoais (DINIZ, 2022).

É bem comum e-mails de sorteios que você não participou, dizendo: “Parabéns você ganhou um iphone.” Essas propagandas são falsas e tem o objetivo de furtar seus dados, essa prática é chamada de phishing[1].

> Quando da fraude eletrônica houver a invasão do computador ou celular alheio ocorre o chamado phishing, referente a uma engenharia social que tem como objetivo obter informações relevantes, na modalidade fraude virtual com o intuito de conseguir dados importantes dos particulares (CRESPO, 2011).

Devido essa prática se tornar comum, em 2021 foi promulgada a Lei nº

[1] Phishing. origina da palavra em inglês "fishing", que significa "pescar".

14.155/2021 que altera o Código Penal, tipificando o crime de estelionato cometido no meio virtual. Assim, o artigo 171, § 2º-A do CP preceitua que:

> § 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.

O crime de estelionato digital tem a pena mais gravosa que o crime de estelionato previsto no artigo 171 do código penal:

> 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.

O terror causado pelo cracker afeta os usuários no meio digital tirando a liberdade de navegarem na internet isso afeta tanto quem já foi vítima quanto quem não foi, pois o medo de cair nas armadilhas de um cracker e perder tudo o que tem é muito grande, e isso gera muitas limitações podendo afetar até as empresas que podem perder sua credibilidade por causa de um golpe utilizando o seu nome.

Hoje, muita gente só usa o banco pela internet, por exemplo. Com o aumento de transações virtuais, também aumenta o medo de ter os dados violados, diz Rupak Patitunda, gerente de pesquisas da Ipsos, em matéria do jornal Estadão. (CAPELAS, 2017).

A situação de desconfiança e medo ao usar as tecnologias e facilidades disponíveis no meio digital, afetam também as empresas em seus comércios nas plataformas digitais pois os sites, e-mails e propagandas falsas usam a imagem das empresas que depois sofrem com desconfiança dos consumidores vítimas dessa prática (BRENOL, 2022).

4. COMPLICAÇÕES NA TIPIFICAÇÃO DOS CRIMES

O anonimato é uma das principais complicações em combater as ações de um cracker, esse tipo de criminoso tem a habilidade de navegar através das camadas da internet e conectando de vários pontos assim camuflando seus rastros para tornar seus ataques mais eficazes contra suas vítimas. TEIXEIRA relata que:

> Em boa medida, a internet permite o anonimato, o que dificulta a identificação do autor, haja vista a possibilidade de manipulação dos dados. O flagrante

> também é um problema, uma vez que é quase impossível de acontecer, pois, muitas vezes, o resultado do crime vem muito depois do início da execução, até porque a vítima muitas das vezes só conhece o prejuízo após um lapso temporal razoável, não imediatamente à sua execução. (TEIXEIRA, 2022).

A prática dos crimes virtuais ocorre pela sensação de impunidade que encoraja os criminosos a criarem as mais diversas formas de práticas de atos ilícitos pois sabem que as chances de serem rastreados e punidos são mínimas. os crackers tÊm o conhecimento da existência das leis que punem suas práticas ilícitas, mas não são intimidados por isso, pois seus crimes são praticados a longa distância enquanto a vítima está em outra parte do país e provavelmente nunca verá o rosto do criminoso, além da distância, ainda utilizam ferramentas para esconder sua localização.Segundo GRECO, Para termos uma ideia das dificuldades e da complexidade que o tema dos controles assume, por exemplo, na Internet, basta mencionar que podem existir serviços que poderiam ser denominados de 'serviço de máscara. (GRECO, apud INELAS, 2009, p. 117.)

O que seria serviços de máscara? São chamados de “proxys”, termo usado para definir um servidor intermediário que atende os pedidos do usuário e repassa para outro servidor.

Um servidor proxy fica à frente do cliente ou de uma rede de clientes e faz a intermediação do tráfego. Esse servidor proxy é outro computador conectado à internet, como seu computador, e ele tem seu próprio endereço IP. Seu computador se comunica apenas com o proxy e o proxy encaminha toda comunicação à internet. Quando a internet responde, o proxy passa essas respostas ao seu computador. Muitos proxies, mas não todos, podem ocultar o endereço IP do seu computador, para que os sites que você acessar não saibam sua identidade real. Ao usar um proxy com um endereço IP de outra parte do mundo para se conectar, você pode “mudar” sua localização geográfica na internet. (AVAST, 2020).

Se trata de servidores destinados a promover o anonimato de seus usuários. É muito comum serem utilizadas cadeias de proxys para que seja praticamente impossível o seu rastreio no meio virtual, o anonimato é a principal habilidade que o cracker utiliza para cometer os mais diversos crimes de forma eficaz.

O estelionato digital é uma prática que possibilita diversas maneiras do cracker

conseguir pegar o que ele quiser, uma delas é por meio de vírus que servem para controlar o aparelho da vítima, o app tira o controle da vítima sobre seu app do banco e passa para ele, permitindo com que faça transferências bancárias usando o pix para a conta que desejar. MARQUES, explica:

> O golpe é aplicado através de um vírus, que é instalado a partir de aplicativo da Play Store. O app é instalado de forma espontânea após o indivíduo clicar em uma propaganda duvidosa, seja por interesse ou sem querer.Um dos meios também usados pelos golpistas é de uma suposta "atualização do WhatsApp", que faz uma solicitação de uma atualização através de uma notificação falsa. Após a instalação, a conta quase de forma instantânea é esvaziada.Uma característica deste golpe em específico é que, ao acessar seu aplicativo de banco, a tela começa a tremer, além do acesso dificultado à conta. Concluído o golpe, os estelionatários levam pouco mais de 90% do saldo da conta (MARQUES, 2023).

Com a velocidade que surgem novas técnicas para prática de furto no meio virtual, o direito tem dificuldade de acompanhar e combater, se analisarmos o cenário antes da **Lei 12.737/2012** (Lei de invasão a dispositivo informático).

Sem lei específica, os crimes praticados no ambiente de internet dificilmente são punidos, porque a legislação penal não admite analogia. "Se o fato não está definido como crime não há punição; acesso não autorizado a sistema, como aconteceu recentemente na Receita Federal, não é crime, mas passará a ser se o projeto for aprovado", explica (NEVES, 2010).

Houve um tempo sem legislação específica para o combate de invasões de dispositivos, essas práticas eram tratadas de outra forma pela justiça e os crimes cometidos antes dessa lei não sofreram a devida punição.

Também o princípio da anterioridade não permite que a lei alcançasse os crimes consumados antes dela ter entrado em vigor (MENENGUSSI, 2019). Em relação ao ano da chegada da internet no país com a criação da Lei 12.737/2012 pode ser notado a grande demora que o direito teve para tipificar esses crimes, mostrando que tem uma evolução lenta para esse cenário.

5. TIPIFICAÇÃO DE CRIMES PARA COMBATE AO ATAQUE CRACKER

Em 2012 foi promulgada a Lei 12.737/2012 (Lei de invasão a dispositivo informático) que tramitou em caráter de urgência por causa da polêmica que ocorreu com a atriz Carolina Dieckmann, que teve seu computador invadido por um cracker, suas fotos íntimas furtadas e usadas como meio de chantagem, por isso a lei foi

apelidada com seu nome. Ainda no mesmo ano, também ocorreu a promulgação da Lei 12.735/2012 que é responsável pela criação de setores da polícia judiciária especializados em combate de crimes virtuais.

No código penal houve alterações no artigo 154-A pela Lei 14.155/21 que revogou a antiga Lei 12.737/12 trazendo um aumento de pena para crime de invasão de dispositivo informático, envolvendo o ataque cracker que tem o objetivo de violar a segurança, como mostra sua redação:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
>
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. (Redação dada pela Lei nº 14.155, de 2021).

Nos atos praticados pelo cracker para furtar dados ele rompe barreiras, invade e uma vez dentro pega o que quiser, como uma pessoa quebra um cadeado para furtar objetos de uma casa (BELCIC, 2020). Isso gera um grande prejuízo para a vítima que tem seus dados furtados. analisando as práticas nota-se que há uma semelhança ao crime de furto qualificado, tipificado pelo artigo 155,§ 4º,I, do Código Penal:

> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
>
> Pena - reclusão, de um a quatro anos, e multa.
>
> § 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido:
>
> **I** - com destruição ou rompimento de obstáculo à subtração da coisa;

As práticas parecem ser da mesma proporcionalidade ao comparar um furto de dados com um furto qualificado onde o indivíduo quebra a janela de uma carro para levar uma bolsa, mas comparando a facilidade e a taxa de sucesso dos dois crimes, um indivíduo capaz de realizar os dois tipos de crimes optaria pelo furto de dados por ser mais difícil de ser pego e pela facilidade de não precisar estar no local para praticar.

O cracker é um problema sério para o meio virtual que vem limitando as pessoas de utilizarem as facilidades que os serviços virtuais oferecem, por causa do medo de cair em golpes ou sofrem uma invasão e serem expostos em público, está claro que furto de dados deve ter pena maior que o furto qualificado, pois além de

oferecer um prejuízo maior, ainda é mais chamativo para o criminoso por ser mais fácil.

6. MÉTODOS DE PREVENÇÃO AOS ATAQUES CRACKERS

A característica mais comum de uma vítima de crimes cibernéticos é a falta de conhecimento sobre a maneira que são realizados, um conhecimento básico pode evitar muitos desses golpes. No *Guia sobre golpes virtuais e dicas de como preservar seus dados na internet* fornecido pelo Núcleo de Defesa do Consumidor - Defensoria Pública do Estado de Tocantins, mostra alguns cuidados que devem ser tomados na hora de fazer compras online:

> • Procure validar os dados de cadastro da empresa no site da Receita Federal;
>
> • Verifique se a página da empresa nas redes sociais contém o selo de verificação;
>
> • Todas as transações devem ser feitas por meio do site oficial;
>
> • Pesquise na internet sobre o site, antes de efetuar a compra, para ver a opinião de outros clientes;
>
> • Acesse sites especializados em tratar reclamações de consumidores insatisfeitos, para verificar se há reclamações referentes a essa empresa;
>
> • Sempre verifique os dados do boleto que está pagando.

O ataque cracker é um assunto que também interessa às empresas voltadas a tecnologias como Apple e Google que oferecem suporte com guias de como evitar ser vítima desses crimes.

Nelas podem ser encontrados guias com dicas sobre segurança de senhas, redes sociais, como evitar ataque phishing e explicações sobre softwares nocivos, essas dicas podem ser encontradas na *Avast Academy*[2]*, Apple suporte*[3] e *Central de segurança Google*[4]*.*

Mesmo havendo leis para combater os crackers, o usuário deve ter a consciência de que ser cauteloso na hora de navegar na internet diminui as chances de ser vítima desses crimes, caso seja vítima deverá informar imediatamente para uma delegacia ou uma delegacia especializada em crimes virtuais para que tomem as

---

[2] Avast Academy. **Segurança:** Como descobrir se seu smartphone foi hackeado. Disponível em :<https://www.avast.com/pt-br/c-phone-hacking-signs>. Acesso em 10 out. 2023.

[3] Apple Suporte. **Suporte:** Reconhecer e evitar e-mails de phishing, chamadas de suporte falsas e outras fraudes**.** Disponivel:<https://support.apple.com/pt-br/HT204759>. Acesso em 10 out. 2023.

[4] Google. **Central de Segurança:** A maneira mais segura de pesquisar. Disponível em:<https://safety.google/intl/pt-BR_br/>. Acesso em: 10 out 2023.

providências necessárias.

CONSIDERAÇÕES FINAIS

O combate ao cracker é um problema que ainda está longe de ser solucionado e que continua gerando danos e alguns até irreparáveis, tanto para usuários comuns quanto para empresas que têm seus aparelhos invadidos e suas informações vazadas e isso impede que a sociedade desfrute dos avanços tecnológicos. O anonimato é utilizado pelo criminoso como uma arma dando a sensação de impunidade na hora de realizar seus crimes.

Nossa legislação dispõe penas que tratam da mesma forma os crimes de furto de dados como o crime de furto qualificado, mas comparado a facilidade de não precisar estar no local e a taxa de sucesso torna o crime de furto de dados uma opção mais atrativa para o criminoso que consegue realizar os dois tipos de crimes.

Com o avanço da tecnologia a sociedade está cada vez mais conectada e ao mesmo tempo que surgem novas tecnologias para facilitar a vida dos usuários, também surgem novos métodos de crimes cibernéticos e a legislação não consegue acompanhar, restando o usuário garantir a sua própria proteção.

Manter o software atualizado, softwares de segurança e ficar informado sobre novas práticas de crimes virtuais é a melhor forma de se proteger dos ataques crackers. A legislação deve reconhecer que o crime no âmbito virtual tem uma maior proporção de danos do que o mesmo no âmbito físico, por isso deve haver penas mais rigorosas a fim de desmotivar a atividade cracker.

REFERENCIAL BIBLIOGRÁFICO

AMARIZ, Luiz Carlos. Hackers e Crackers. InfoEscola: Navegando e aprendendo. Disponível em:<https://www.infoescola.com/informatica/hackers-e-crackers/>. Acesso em: 20 set. 2022.

APPLE SUPORTE. Suporte: Reconhecer e evitar e-mails de phishing, chamadas de suporte falsas e outras fraudes. Disponivel:<https://support.apple.com/pt-br/HT204759>. Acesso em 15 out. 2023.

AVAST ACADEMY. Segurança: Como descobrir se seu smartphone foi hackeado.

Disponível em :<https://www.avast.com/pt-br/c-phone-hacking-signs>. Acesso em 13 out. 2023.

ARAUJO, Claudio Rodrigues. ANÁLISE DA APLICAÇÃO DO DIREITO PENAL NOS CRIMES VIRTUAIS. Pensar Acadêmico, v. 19, n. 2, p. 494-511, 2021.

AVAST SOFTWARE S.R.O. O que é phishing, exatamente? Avast. Disponível em:<https://www.avast.com/pt-br/c-phishing>. Acesso em 2 out. 2022.

AVAST SOFTWARE S.R.O. O que é um servidor proxy e como ele funciona? Avast. Disponível em:<https://www.avast.com/pt-br/c-what-is-a-proxy-server>. Acesso em 19 mar. 2023.

BRENOL, Marlise. Saiba como identificar um site falso. Serasa. Disponível em:<https://www.serasa.com.br/premium/blog/saiba-como-identificar-um-site-falso/>. Acesso em 07 abr. 2024.

BASTA, Alfred; BASTA, Nadine; BROWN, Mary. Segurança de computadores e teste de invasão. 2ª edição, 2014.

BELCIC, Ivan. O que é cracking? É hacking, mas do mal. Avast. Disponível em:<https://www.migalhas.com.br/depeso/349148/tempos-modernos-preconceitos-antigos>. Acesso em 15 abr. 2024.

BONAGURA, Jordan M. Tempos modernos, preconceitos antigos. Migalhas. Disponível em:<https://www.migalhas.com.br/depeso/349148/tempos-modernos-preconceitos-antigos>. Acesso em 11 abr. 2024.

BRASIL. Lei nº 12.737, DE 30 DE NOVEMBRO DE 2012. Lei de Invasão de dispositivo informático. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 23 de ago. 2023.

CAETANO, Érica. O que é hacker?. Brasil Escola. Disponível em: https://brasilescola.uol.com.br/informatica/o-que-e-hacker.htm. Acesso em 10 de ago. 2023.

CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro: Brasport, 2014.

CANALTECH. Roubo de contas no Instagram: usuários pagam serviços para

recuperarperfis.Disponível em: <https://canaltech.com.br/seguranca/roubo-de-contas-no-instagram-usuarios-pagam-servicos-para-recuperar-perfis-206898/> Acesso em: 17 de ago. 2023.

CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. São Paulo: Saraiva, 2011.

DINIZ, F. F.; CARDOSO, J. R.; PUGLIA, E. H. P. O crime de estelionato e suas implicações na era contemporânea: o constante crescimento dos golpes via internet. LIBERTAS DIREITO, [S. l.], v. 3, n. 1, 2022, p-13. Disponível em:<https://periodicos.famig.edu.br/index.php/direito/article/view/215. Acesso em: 19 abr. 2024>.

ESTADÃO. 7 em cada 10 brasileiros temem ser hackeados, revela pesquisa. DIsponivel em:<https://www.estadao.com.br/link/cultura-digital/7-em-cada-10-brasileiros-temem-ser-hackeados-revela-pesquisa/> Acesso em: 09 de Set. 2023

FAORO, Roberta Rodrigues; JESUS, Betina Ribeiro de; ABREU, Marcelo Faoro de. UM ESTUDO SOBRE CRIMES DIGITAIS: DETECÇÃO E PREVENÇÃO. Anais do IV SINGEP. 2015, p. 1-17.

GONÇALVES, Rafaela. Crimes cibernéticos avançam no Brasil e aceleram com a tecnologia. Correio Braziliense. Disponível em:<https://www.correiobraziliense.com.br/economia/2024/03/6824212-crimes-ciberneticos-avancam-no-brasil-e-aceleram-com-a-tecnologia.html>. Acesso em 10 abr. 2024.

GOOGLE. Central de Segurança: A maneira mais segura de pesquisar. Disponível em:<https://safety.google/intl/pt-BR_br/>. Acesso em: 10 out 2023.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). PNAD TIC Internet já é acessível em 90,0% dos domicílios do país em 2021. Agência de notícias IBGE,16 de set. 2022. Disponível em: <//agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021#:~:text=Na%20%C3%A1rea%20rural%2C%20a%20propor%C3%A7%C3%A3o,com%20acesso%20%C3%A0%20grande%20rede>. Acesso em: 1 out. 2022.

MARQUES, Caynã. Fraude do Pix: novo vírus facilita golpes; entenda. OPOVO. Disponível em:<https://www.opovo.com.br/noticias/economia/2023/09/14/fraude-do-

pix-novo-virus-facilita-golpes-entenda.html>. Acesso em 13 abr. 2024.

MEU POSITIVO. Hackers do bem-Quem são eles e como podem ajudar empresas?. Disponível em: <https://www.meupositivo.com.br/panoramapositivo/hackers-do-bem/> Acesso em 12 de ago. 2023.

NEVES, Maria. Falta de lei sobre crimes digitais leva à impunidade, diz especialista. Agência Câmara de Notícias. Disponível em:<https://www.camara.leg.br/noticias/208500-falta-de-lei-sobre-crimes-digitais-leva-a-impunidade-diz-especialista/>. Acesso em 14 abr. 2024.

NÚCLEO DE DEFESA DO CONSUMIDOR (NUDECON).Guia sobre golpes virtuais e dicas de como preservar seus dados na internet. Disponível em: <https://static.defensoria.to.def.br/postify-media/uploads/post/file/51817/044_Guia_-_Golpes_Virtuais_30x21cm.pdf> Acesso em: 20 de Set. 2023.

LOPES, Fabio Juliate. É Crime ser 'Hacker'? Jusbrasil. Disponível em:<https://www.jusbrasil.com.br/artigos/e-crime-ser-hacker/1154055636>. Acesso em 15 abr. 2024.

PINHEIRO, Patrícia Peck. Direito digital / Patrícia Peck Pinheiro. – 6. ed. rev., atual. e ampl. – São Paulo: Saraiva, 2016.

PINHEIRO, Patrícia Peck. Direito digital global e seus princípios fundamentais. Revista Jurídica , São Paulo, p. 46-47, 2016.

GRECO, Marco Aurelio apud INELAS, Gabriel Cesar Zaccarias de. Crimes na Internet. 2ª edição, 2009, p. 117.

ROCHA, LILIAN ROSE LEMOS; BINICHESKI, PAULO. Crimes digitais. repositório. uniceub. disponível em: <https://www.google.com/url?sa=t&source=web&rct=j&url=https://repositorio.uniceub.br/jspui/bitstream/prefix/14602/1/Crimes%2520digitais.pdf&ved=2ahUKEwio_dKKvoz7AhUimZUCHQ8IDcAQFnoECBcQAQ&usg=AOvVaw1DT18l7LATKAnqMDmeUHX0> acesso em: 25 de out. 2022.

SANTOS CABETTE, Eduardo Luiz. Crime de Invasão de Dispositivo Informático (artigo 154 - A, CP). Jusbrasil Artigos. Disponível em: <https://eduardocabette.jusbrasil.com.br/artigos/153070617/crime-de-invasao-de-

dispositivo-informatico-artigo-154-a-cp>. Acesso em: 18 set 2022.

TEIXEIRA, Tarcísio. Direito digital processo eletrônico. 6ª edição, 2022, p. 224.

TEIXEIRA, Tarcísio. Direito digital processo eletrônico. 6ª edição, 2022, p. 230.

TEIXEIRA, Tarcísio. Direito digital processo eletrônico. 6ª edição, 2022, p. 237.

VARELLA, G; SOPRANA, P. Pornografia de Vingança: crime rápido, trauma permanente. São Paulo, 16 Fev 2016. Época. Disponível em: <http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/02/pornografia-de-vinganca-crime-rapido-trauma-permanentee.html>. Acesso em 25 de out. 2022.

VERAS, Ricardo Régis Oliveira. Roubo de dados e crackers / Delitos via internet: violação de propriedade intelectual por crackers. DireitoNet, 14 de jan. 2004. Disponível em: <https://www.direitonet.com.br/artigos/exibir/1434/Roubo-de-dados-e-crackers>. Acesso em: 18 de set. 2022.