CENTRO UNIVERSITÁRIO BRASILEIRO

CURSO DE BACHARELADO EM DIREITO

VICTOR FERREIRA LOPES

INVESTIGAÇÃO E PREVENÇÃO DE CRIMES VIRTUAIS: um estudo sobre phishing como ameaça digital

RECIFE/2023

VICTOR FERREIRA LOPES

INVESTIGAÇÃO E PREVENÇÃO DE CRIMES VIRTUAIS: um estudo sobre phishing como ameaça digital

Monografia apresentada ao Centro Universitário Brasileiro - UNIBRA, como requisito parcial para obtenção do título de Bacharel em Direito.

Professor orientador: Ms. Luiz Luna Neto.

RECIFE/2023

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 2338/ O.

l864i Lopes, Victor Ferreira.
Investigação e prevenção de crimes virtuais: um estudo sobre phishing como ameaça digital/ Victor Ferreira Lopes. - Recife: O Autor, 2023.
52 p.

Orientador(a): Ms. Luiz Luna Neto.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – UNIBRA. Bacharelado em Direito, 2023.

Inclui Referências.

1. Crimes virtuais. 2. Covid-19. 3. Internet. 4. Phishing. 5. Pandemia. I. Centro Universitário Brasileiro - UNIBRA. II. Título.

CDU: 615

Dedico esse trabalho a minha amada esposa,
Lúcia Vitória.

AGRADECIMENTOS

Primeiramente agradeço a Deus por me dar força e motivado em momentos de cansaço, dúvida e desânimo. Sua presença constante me encoraja a perseverar, enfrentar os obstáculos e seguir em frente, mesmo quando as dificuldades parecem insuperáveis.

Agradeço e dedico esta monografia a minha amada e querida esposa, Lúcia Vitória. Você tem sido meu apoio incondicional ao longo dessa jornada acadêmica. Sua paciência, compreensão e incentivo constante foram essenciais para que eu pudesse enfrentar os desafios e alcançar este momento tão importante. Nossos sonhos e realizações são compartilhados, e é com imensa gratidão que reconheço o seu papel fundamental em todas as etapas deste caminho. Suas palavras de encorajamento, seu amor inabalável e sua presença ao meu lado foram a força motriz que me impulsionou a seguir em frente.

Este trabalho é uma pequena demonstração do meu amor e da minha admiração por você. Agradeço por estar sempre presente, por me incentivar a ser meu melhor e por acreditar em mim quando eu mesmo duvidava.

Agradeço também a minha família, aos meus amigos e colegas de curso, que compartilharam suas ideias e experiências, proporcionando um ambiente de aprendizado colaborativo e estimulante. Suas contribuições e discussões enriqueceram meu trabalho e ampliaram minha visão sobre o tema.

Por fim, expresso minha gratidão ao meu orientador, Luiz Luna Neto, por dedicar seu tempo e compartilhar seu conhecimento, enriquecendo o conteúdo deste estudo. Sou imensamente grato por todos os momentos de aprendizado compartilhados.

RESUMO

A Internet tornou-se recentemente uma das ferramentas mais importantes parauma das grandes invenções do século 20. Desde a sua criação, abriu as portas para o desenvolvimento de novas tecnologias e inovações. Esta evolução continua até hoje, mudando a forma como vivemos e interagimos com a maioria das pessoas, tornando os crimes que cometemos ainda mais perfeitos. Continuo**.** O objetivo destetrabalho é apontar crimes que acontecem na Internet especificamente o “PHISHING”.

Este estudo analisa os crimes mais comuns neste cenário. Porém, esse avanço tecnológico, além de certas vantagens, também auxilia na prática de crimes. o chamado cibercrime ou cibercrime; durante a pandemia do COVID-19, os ataques cibernéticos também ocorreram várias vezes. Diante desse aumento da atividade criminosa, este artigo destaca os riscos associados ao desenvolvimento dessa importante ferramenta e o impacto da pandemia do COVID-19 no aumento do acessoa ambientes virtuais relacionados ao cibercrime. Essa constatação mostra a fragilidade do sistema judiciário em termos de legislação e normas legais querepresentam a atividade criminosa em relação ao crime.

Palavras-chave: Crimes virtuais, Covid-19, Internet, Phishing, Pandemia.

ABSTRACT

The Internet has recently become one of the most important tools for one of the great inventions of the 20th century. Since its inception, it has opened the door to the development of new technologies and innovations. This evolution continues today, changing the way we live and interact with most people, making the crimes we commit even more perfect. Continuous. The objective of this work is to point out crimes that happen on the Internet specifically "PHISHING".

This study analyzes the most common crimes in this scenario. However, this technological advance, in addition to certain advantages, also helps in the commission of crimes. the so-called cybercrime or cybercrime; during the COVID-19 pandemic, cyberattacks also occurred several times. In light of this increase in criminal activity, this article highlights the risks associated with the development of this important tool and the impact of the COVID-19 pandemic on increased access to cybercrime-related virtual environments. This finding shows the fragility of the judicial system in terms of legislation and legal norms that represent criminal activity in relation to crime.

Keywords: Cyber crimes, Covid-19, Internet, Phishing, Pandemic.

SUMÁRIO

1 INTRODUÇÃO

A introdução é uma parte crucial de qualquer trabalho acadêmico, pois estabelece o contexto e apresenta o tema de estudo aos leitores. A seguir, segue uma introdução sobre o tema "Investigação e Prevenção de Crimes Virtuais: um estudo sobre phishing como ameaça digital":

No mundo atual, em que a tecnologia desempenha um papel cada vez mais central em nossas vidas, é inegável que a internet trouxe uma série de benefícios e facilidades. No entanto, essa crescente dependência da tecnologia também trouxe consigo uma série de desafios, especialmente no que diz respeito à segurança digital e à proteção de informações pessoais.

Os crimes virtuais, ou cibercrimes, emergiram como uma ameaça significativa na era digital. Dentre os diversos tipos de cibercrimes, o phishing tem se destacado como uma das principais estratégias utilizadas pelos criminosos virtuais. O phishing envolve a prática de enviar comunicações fraudulentas, como e-mails, mensagens de texto ou páginas da web falsas, com o intuito de enganar os usuários e obter informações confidenciais, como senhas, números de cartões de crédito e dados bancários.

Diante desse cenário, a investigação e prevenção de crimes virtuais tornaram-se essenciais para garantir a segurança e proteção dos usuários da internet. Compreender o funcionamento do phishing e as técnicas utilizadas pelos criminosos virtuais é fundamental para desenvolver estratégias eficazes de combate e prevenção dessas ameaças digitais.

Este trabalho tem como objetivo aprofundar o conhecimento sobre o tema, focando especificamente no phishing como ameaça digital. Serão explorados os diferentes métodos utilizados pelos criminosos virtuais para realizar ataques de phishing, assim como as principais técnicas de investigação utilizadas para identificar e rastrear os responsáveis por esses crimes.

Além disso, será discutida a importância da conscientização e educação dos usuários da internet como uma estratégia fundamental na prevenção de ataques de phishing. Medidas de segurança e boas práticas serão abordadas, buscando fornecer orientações para minimizar os riscos e proteger-se contra essa ameaça digital cada vez mais sofisticada.

Por meio deste estudo, espera-se contribuir para a compreensão mais ampla do fenômeno do phishing e fornecer insights relevantes para o desenvolvimento de estratégias eficazes de investigação e prevenção de crimes virtuais, garantindo assim a segurança digital dos usuários e promovendo um ambiente virtual mais seguro e confiável.

2 HISTÓRIA DA INTERNET

A Internet, também conhecida como a maior "rede de computadores" do mundo, surgiu durante a Guerra Fria. Graças ao conflito entre os Estados Unidos e a União Soviética, os Estados Unidos e a União Soviética entenderam e souberam da importância dos meios de comunicação para obter vantagem. Vença a guerra e leve-os à vitória.

A Internet foi fundada em 1969, também conhecida como Arpanet nos Estados Unidos e tem como função conectar instituições de pesquisa. Naquele ano, um professor da Universidade da Califórnia encaminhou o primeiro e-mail sobre esse artigo para um amigo da Universidade de Stanford. Os Estados Unidos, temendo um ataque nuclear às suas bases militares, podem comprometer todas as informações e deixar-se vulneráveis aos adversários[1].

Isso criará uma nova rede de troca de informações. ARPANET - Agência de Projetos de Pesquisa Avançada criada pela APA. Lembre-se que o propósito da internet foi criado para defesa em tempo de guerra e que a internet foi criada exclusivamente para proteger e proteger os computadores e informações do governo dos EUA. A partir de 1892, o uso do Arpanet tornou-se mais acadêmico.

O negócio foi inicialmente limitado aos Estados Unidos, mas desde então se expandiu para outros países, como Holanda, Dinamarca e Suécia. Desde então, o termo Internet tem sido usado. Por quase 20 anos, a rede foi acessada apenas pela comunidade acadêmica e científica. Foi introduzida comercialmente nos Estados Unidos em 1987.

No Brasil, a primeira rede nasceu em 1988, em cooperação com várias universidades brasileiras e instituições americanas, e foi aprimorada de forma amigável e aberta ao público ao longo dos anos. No Brasil, a partir dessa época, ainda na década de 1980, o Ministério da Ciência e Tecnologia concebeu a Internet como uma espécie de padrão IP/TCP (Internet Protocol and Transport Control Protocol) que permite a transmissão de informações pela rede para outra pessoa.

Fornece mensagens mais seguras entre redes conectadas a endereços IP na Internet. Em 1990, os Estados Unidos, em conjunto com o Departamento de Defesa,

[1] Âmbito Jurídico. "Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação." Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em: 21 ago. 2022.

mudaram o nome da ARPANET para Network File System (NFS), mais conhecido como "Internet". Este recurso permite acesso remoto a arquivos/pastas de vários computadores dentro do servidor, como um usuário usando o mesmo local.

Assim, a Internet foi se desenvolvendo gradativamente e em 1993, o sistema CERN (Organização Européia para Pesquisa Nuclear), WWW (World Wide Web) era apenas um sistema de documentos, uma espécie de hipermídia relacionada a diversos tipos de mídia. Rede legítima para negócios ou uso pessoal[2].

2.1 A utilização da internet para prática de crimes

Sabemos que a internet trouxe muitos benefícios para a humanidade e é por isso que ela cresceu tremendamente em todo o mundo e aproximou as pessoas do mundo de nós. Este novo mundo virtual trará muitos benefícios para as pessoas, pois promove relacionamentos comerciais, encurta a distância entre as pessoas e realiza relacionamentos sociais e comerciais entre pessoas, pessoas e países online.

O que realmente impulsiona o crescimento fenomenal de todas as nações conectadas é que estamos constantemente interagindo com comércio e relacionamentos sociais e virtuais todos os dias, seja em bancos, pesquisas, enquetes, bate-papos por e-mail e muito mais. É viver com isso. Sala de bate-papo com outras pessoas.

Como a Internet conecta muitas coisas em nosso dia a dia, o ambiente virtual exige uma consciência clara de nossas necessidades diárias. Nesse caso, a Internet dominou negativamente nossas relações sociais, profissionais e econômicas, criando uma série de comportamentos perigosos enquanto aumentava os lucros e ampliava as oportunidades para o crime.

Isso porque, o meio virtual traz uma facilidade enorme de comunicação e desenvolvimento de tecnologias, tornando os crimes praticados por computadores ou via internet mais danosos à sociedade visto a dificuldade de punir ou até mesmo encontrar esse criminoso pois, não existir uma fronteira entre esse “cyberspace”, ou seja, “ciberespaço”[3].

---

[2] Wikipedia. Internet. Disponível em: https://pt.wikipedia.org/wiki/Internet. Acesso em: 28 ago.2022.
[3] Wikipedia. Ciberespaço. Disponível em: https://pt.wikipedia.org/wiki/Ciberespa%C3%A7o. Acesso em: 28 ago. 2022.

O ciberespaço é um espaço virtual na Internet que conecta pessoas para criar um novo tipo de mundo virtual onde as pessoas podem se conectar ou se conectar a outros mundos em segundos. Da mesma forma que a Internet beneficia a todos no mundo, também existem vulnerabilidades e atividades que permitem atividades proibidas que podem prejudicar aqueles que estão conectados a esta rede.

Um dos maiores desafios hoje é a promulgação de leis eficazes para limitar ou identificar esses tipos de atividades e práticas ilegais na Internet e para combater o crime nas redes de computadores em todo o mundo. O objetivo é revisar as ações que nosso governo tomou para prevenir esses crimes e encontrar soluções para esses poderes.

2.2 Crimes cibernéticos

Cibercrime inclui cibercrime, cibercrime, e-crime, computador crime, e-crime, etc. Assim, todas essas seitas representam o mesmo tipo de crime - criminosos, suas principais ferramentas serão a tecnologia da informação, a mídia e a própria Internet. Cibercrime é qualquer atividade criminosa que visa ou usa computadores, redes de computadores ou dispositivos de rede.

A maioria, se não todos, os crimes cibernéticos são cometidos por cibe criminosos ou hackers com o objetivo de ganhar dinheiro. No entanto, os cibe criminosos às vezes procuram sabotar computadores e redes por outros motivos que não o lucro. Nesses casos, o motivo pode ser pessoal ou político. O cibercrime pode ser cometido por indivíduos ou organizações. Alguns cibe criminosos são organizados, usam técnicas avançadas e são tecnicamente sofisticados. Alguns hackers são iniciantes.

2.3 Da classificação dos crimes

Bom, como sabemos o que define o crime ou caracteriza de informática são o uso dos computadores ou da internet para prática do ato. Assim podem ser classificados como crimes cibernéticos puros e impuros. As classificações paracrimes cibernéticos não são eficazes, devido a dinâmica e mudança constante da internet e computadores junto a tecnologia. A evolução proporcionada por eles é

muito grande, assim como novas formas delitivas que vão surgindo. Dessa maneira que vão surgindo se tornam obsoletas em pouco tempo.

Segundo Sergio marcos, conceitua sobre crime de informática:

> ´´Sergio Marcos Roque (2007, p. 25), conceitua crime de informática como sendo “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material``[4].

2.4 Crimes cibernéticos puros

Define-se crimes cibernéticos puros como todo ou qualquer tipo de consumo que cause conduta ilícita de computadores, seja por atentado físico ou técnico, inclusive dados e sistemas. Pois o objetivo maior é lograr êxito na tomada de dados de sistema assim sendo fácil alvo de hackers que são pessoas com amplo conhecimento em redes de computadores.

2.5 Crimes cibernéticos impuros

Os crimes cibernéticos impuros ocorrem quando a o uso da internet para determinado crime como meio executivo para prática de um crime tipificado em nossa legislação penal, como divulgar fotos pornográficas de crianças e adolescentes, tipificada no Art. 241 do Estatuto da Criança e do Adolescente.

2.6 Tempo e local de crime

Infelizmente não tem, tempo ou local previsto para isso o crime virtual pode acontecer em minutos ou segundos tendo seu local na casa do cibe criminoso ou invadindo o espaço da vítima sem que ela perceba para ter acesso aos dados ou fotos e vídeos íntimos. No meio, informática é uma dissociação, pois é possível programar a execução de um crime informático no tempo, pois o ato ilícito pode ser feito muito antes da sua programação, devido todo computador de dentro dele ter um relógio

[4] ROQUE, Sergio Marcos. Crimes virtuais. 2022. Disponível em: https://jus.com.br/artigos/72619/crimes-virtuais. Acesso em: 30 ago. 2022.

interno[5].

[5] JUS BRASIL. Competência nos crimes cibernéticos. Disponível em: https://www.jusbrasil.com.br/artigos/competencia-nos-crimes-ciberneticos/514359859. Acesso em: 30 ago. 2022.

O nosso código penal fala que, a teoria da atividade para descrever o momento do crime a prática do crime ocorre no momento da ação ou omissão independentemente do momento ou resultado. No mundo virtual, não existe um espaço físico muito menos geográfico delimitado. Por isso, constatar um crime informático é muito difícil detectar a localização pois será um passo fundamental para saber de onde veio e ocorreu o crime.

Vale ressaltar que o mundo virtual é chamado de “ciberespaço” que é todo local onde ocorre esse fluxo de informações através das redes de comunicações. Por isso, a maioria dos crimes superam o espaço das fronteiras, pois a internet viabiliza esse tipo de crime, pois o mundo está conectado à internet. Como no Brasil, não existe legislação processual penal nacional para esse tipo de matéria, se faz necessário usar alguns princípios do Código Penal Brasileiro, mais precisamente quanto a territorialidade, extraterritorialidade, nacionalidade, defesa e representação.

Bom, com relação à territorialidade no Art. 5° do Código Penal Brasileiro, determina que seja aplicada a lei penal brasileira a todos os crimes executados em território nacional, sem prejuízo das normas, convenções e tratados de Direito internacional.

Com relação aos demais princípios, os quais estão previstos no Art.7° do Código Penal Brasileiro, que conduz a extraterritorialidade da lei penal nacional, que é determinante a aplicação da nossa legislação penal para os crimes praticados fora do nosso território nacional.

2.7 Da escassa previsão legal como condutas ilícitas na internet

O direito penal brasileiro, que evoluiu rapidamente nos últimos anos, está adaptado aos tempos modernos, mas este estudo busca analisar se esses desenvolvimentos são suficientes para garantir a segurança jurídica no Brasil. Embora a maioria desses delitos fictícios possa ser tratada pela lei penal aplicável, ainda é necessário criar legislação adicional com foco em tópicos relacionados à Internet (por exemplo, Lei 12.735/2012, 12.737/2012). "lei". Carolina Dieckmann" e Lei 12.965/2014 "Marco Civil da Internet".

Mas o documento também descreve os desafios que o Departamento de Estado enfrenta ao processar criminosos cibernéticos, dado o aumento dramático no número de casos nos últimos anos. O estudo bibliográfico realizado neste artigo tem

como base o princípio “Nullum Crimen nulla poena sine praevia lege” do artigo 1º do Código Penal Brasileiro de 1940.

Não há como negar que diferentes formas de tecnologia desenvolvidas nas últimas décadas moldaram a maneira como as pessoas interagem hoje. A globalização da Internet representa uma nova dimensão na sociedade atual que tem um impacto direto em muitas formas de relações humanas e, à medida que a cibercultura continua a evoluir, será difícil lidar com o impacto dessas mudanças, essa mudança para a humanidade. Isso é um grande problema.

Damásio de Jesus e José Antônio Milagre descrevem uma ideia interessante em seu Infotipos (2016) Handbook of Crime. O crime existe por causa da riqueza, assim como não falta a Internet. Assim como a internet evoluiu para melhor, ela também evoluiu para pior. Na última década, a Internet se tornou um ponto de acesso para criminosos se esconderem atrás de redes criptografadas e aproveitarem todas as oportunidades para cometer crimes cibernéticos[6].

Pode ser porque você confia em sua identidade para ser protegida por trás da tela do computador com criptografia moderna. Não acho que tenha qualquer significado legal, seja porque é um software ou apenas porque é um crime imaginário e não um crime físico.

Embora a maioria dos crimes fictícios possa ser caracterizada de alguma forma por sua semelhança com os tipos de crimes previstos no Código Penal, é necessário promulgar legislação específica. Primeiramente, a Lei 12.737/2012. A chamada "Lei Karolina-Dieckmann", promulgada em 2012 para descrever certos tipos de crimes cibernéticos, faz parte do código penal existente que anteriormente não visava os cibe criminosos.

A tecnologia é atualizada a cada segundo, a Internet se expande a cada segundo e o Congresso não pode impedir essas expansões. Porque são essas consoantes que determinam como isso acontece. Ação para a sociedade antes de todos os avanços tecnológicos que estamos testemunhando no século 21. Agora, mais do que nunca, é necessário desenvolver a legislação penal existente em um

[6] JESUS, Damásio de; MILAGRES, José Antônio**.** Manual de Crimes Informáticos. 1ª Edição. ed. São Paulo: Saraiva, 2016. 231 p. ISBN 978850262724-6. Disponível em https://docero.com.br/doc/ecv5ns. Acesso em 30 ago.2022

grau que promova certeza sobre os aspectos legais e desenvolver novos caminhos para a polícia e o Departamento do Interior para fornecer meios legais. Pode ser processado, processado em tribunal. Combater o cibercrime e o crime.

,

3 EVOLUÇÃO LEGISLATIVAS DOS CRIMES CIBERNÉTICOS

A legislação brasileira relacionada aos crimes cibernéticos tem passado por uma evolução significativa ao longo dos últimos anos. A abordagem legislativa tem sido fundamental para enfrentar os desafios emergentes no mundo digital e proteger os cidadãos contra os crimes cometidos por meio da tecnologia. A principal legislação brasileira relacionada aos crimes cibernéticos é a Lei nº 12.737, de 2012, conhecida como "Lei Carolina Dieckmann".

Essa lei foi promulgada após o caso de uma famosa atriz brasileira que teve suas fotos íntimas vazadas na internet. A Lei Carolina Dieckmann tipifica como crime a invasão de dispositivos informáticos alheios, com o intuito de obter, adulterar ou destruir dados ou informações sem autorização. Posteriormente, em 2013, foi sancionada a Lei nº 12.965, também conhecida como "Marco Civil da Internet".

Embora o Marco Civil não se concentre exclusivamente em crimescibernéticos, ele estabeleceu princípios, direitos e deveres para o uso da internet no Brasil. Além disso, o Marco Civil estabelece a responsabilidade dos provedores de internet e de serviços online em relação aos conteúdos ilícitos compartilhados por seus usuários[7].

Em 2018, entrou em vigor a Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados (LFPD). Embora seu objetivo principal seja regulamentar a proteção e o tratamento de dados pessoais, a LGPD também aborda a segurança das informações e estabelece penalidades para o vazamento de dados e outras violações relacionadas à proteção de informações pessoais[8].

Outro marco importante na evolução legislativa dos crimes cibernéticos no Brasil foi a promulgação da Lei nº 14.155, em 2021. Essa lei criou o tipo penal de "furto qualificado mediante fraude eletrônica", que inclui, por exemplo, o roubo de informações financeiras e bancárias por meio de técnicas de engenharia social.

Além dessas leis específicas, o Código Penal brasileiro foi alterado para incluir diversos tipos de crimes cibernéticos, como estelionato eletrônico, falsificação de cartões de crédito, violação de segredo empresarial, entre outros.

[7] Wikipedia. Internet. Disponível em: https://pt.wikipedia.org/wiki/Internet. Acesso em: 28 ago.2022.
[8] Wikipedia. Internet. Disponível em: https://pt.wikipedia.org/wiki/Internet. Acesso em: 28 ago. 2022.

Essas alterações visam adequar a legislação aos avanços tecnológicos e garantir a punição adequada aos criminosos cibernéticos. Vale ressaltar que a evolução legislativa dos crimes cibernéticos no Brasil ainda está em curso, uma vez que o cenário digital é constantemente transformado por novas tecnologias e ameaças. É possível que haja a necessidade de atualizações e aprimoramentos adicionais para enfrentar os desafios futuros relacionados à segurança cibernética e proteção de dados.

Os primeiros casos de crimes virtuais foram em meados do ano de 1960, onde infratores manipulam dados contidos em computadores, praticando vários atos ilícitos como, sabotagem, espionagem e abuso de forma legal em computadores, naquela época era bastante difícil de detectar.

A partir de 1980, houve uma grande mudança sobre esse assunto, pois foram divulgados diversos crimes referentes ao mundo virtual piratarias de programas, divulgação de dados, manipulação de dinheiro em caixas eletrônicos, abuso em telecomunicações.

Assim, como foi crescendo bastante a prática de crimes nesse âmbito virtual foi se criando uma necessidade de legislações para tais atos para regulamentar a prática desses respectivos atos ilícitos. Por mais uma vez, os Estados Unidos da América foram pioneiros nesse assunto, criando as primeiras legislações sobre o crime virtual em 1894.

3.1 Da lei n.°12.965/2014 - Marco Civil da Internet

A Lei n.°12.965/2014, também conhecido como Marco Civil da Internet, é uma legislação brasileira que estabelece princípios, direitos e deveres para o uso da internet no país. Foi sancionada em abril de 2014 e entrou em vigor em junho do mesmo ano[9].

O Marco Civil da Internet tem como objetivo garantir direitos fundamentais dos usuários, promover a privacidade, a liberdade de expressão e o acesso à informação. Além disso, a lei busca regular as atividades na internet, estabelecendo

[9] Brasil. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 ago. 2022.

responsabilidades para os provedores de internet e definindo regras para a coleta, o armazenamento e o compartilhamento de dados pessoais dos usuários.

Os principais pontos do Marco Civil da Internet, previstos na Lei 12.965, são os seguintes. Neutralidade da rede que estabelece o princípio da neutralidade, garantindo que os provedores de acesso à Internet tratem todos os dados de forma isonômica, sem discriminação, restrição ou bloqueio de conteúdos, serviços, aplicativos, dispositivos ou formas de uso[10].

Privacidade e proteção de dados assegura a inviolabilidade e o sigilo das comunicações dos usuários, bem como a proteção de seus dados pessoais, estabelecendo que a coleta, armazenamento, tratamento e compartilhamento de informações só podem ocorrer mediante o consentimento livre, expresso e informado do usuário.

Responsabilidade dos intermediários de determina que provedores de conexão à Internet e provedores de aplicações devem respeitar a liberdade de expressão e não podem ser responsabilizados pelo conteúdo gerado pelos usuários, exceto em casos específicos definidos na legislação, como a violação de direitos autorais.

Direito à privacidade reconhece o direito à privacidade e à inviolabilidade da intimidade, assegurando que as informações pessoais dos usuários não sejam acessadas, divulgadas ou utilizadas de forma indevida.

Armazenamento de dados determina que os provedores de conexão e aplicações devem manter registros de conexão dos usuários por um período de no mínimo seis meses, resguardando a privacidade das comunicações. Liberdade de expressão garante o direito à liberdade de expressão e o acesso à informação, vedando a censura e a restrição ao fluxo de informações na Internet.

Judicialização de conteúdos estabelece regras para a retirada de conteúdos da Internet, exigindo que sejam fundamentadas em decisão judicial. Esses são algunsdos principais pontos do Marco Civil da Internet, que busca garantir os direitos dos usuários e estabelecer princípios para o uso da Internet no Brasil.

3.2 Da lei n.°12.737/2012 - Lei Carolina Dieckmann

[10] Oficina da Net. O Marco Civil da Internet foi aprovado - Entenda o que é e o que muda na sua vida. Disponível em: https://www.oficinadanet.com.br/post/12558-o-marco-civil-da-internet-foi-aprovado-entenda-o-que-e-e-o-que-muda-na-sua-vida. Acesso em: 29 ago. 2022.

A Lei n° 12.737/2012, popularmente conhecida como "Lei Carolina Dieckmann", é uma legislação brasileira que trata dos crimes cibernéticos, em especial a invasão de dispositivos eletrônicos e a divulgação não autorizada de dados pessoais na internet. A lei recebeu esse nome em homenagem à atriz Carolina Dieckmann, que foi vítima de um crime virtual em 2012, quando fotos íntimas suas foram hackeadas e divulgadas na internet[11].

A lei foi criada para preencher uma lacuna legal relacionada aos crimes cibernéticos, estabelecendo penalidades para a invasão de computadores, a obtenção e divulgação não autorizada de informações e dados pessoais, e a interrupção ou perturbação de serviços de computadores ou sistemas informatizados. Antes dessa lei, não existia uma legislação específica para tratar desses crimes no Brasil.

Um dos principais pontos da Lei Carolina Dieckmann é a tipificação dos chamados "crimes cibernéticos", que incluem a invasão de dispositivos eletrônicos, a obtenção, divulgação ou comercialização de informações privadas sem autorização, e a interrupção ou perturbação de serviços de computadores ou sistemas informatizados.

A lei prevê penas de detenção de três meses a um ano, além de multa, para quem obtiver, divulgar ou comercializar dados pessoais sem autorização. A pena pode ser aumentada se o crime for cometido contra autoridades públicas, em razão de suas funções, ou se envolver o uso de informações para obtenção de vantagem ilícita.

Vale ressaltar que a lei também estabelece a competência da Polícia Federal para investigar esses crimes e a possibilidade de cooperação internacional para a persecução penal. No entanto, é importante mencionar que a Lei Carolina Dieckmann tem sido alvo de críticas e debates desde sua criação.

Alguns argumentam que a legislação é muito ampla e imprecisa, podendo gerar interpretações subjetivas. Além disso, há preocupações sobre a efetividade da aplicação da lei, a capacidade dos órgãos de investigação em lidar com crimes

[11] Brasil. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 29 ago. 2022.

cibernéticos e a necessidade de atualização constante para acompanhar a evolução tecnológica.

Em resumo, a Lei n° 12.737/2012, conhecida como "Lei Carolina Dieckmann", representa um importante avanço na legislação brasileira ao tipificar os crimes cibernéticos e estabelecer penas para invasão de dispositivos eletrônicos e divulgação não autorizada de dados pessoais. No entanto, sua efetividade e aplicação continuam sendo objeto de discussão e aprimoramento[12].

3.3 Da lei n.°13.709/2018 - Lei Geral de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais (LGPD) é uma legislação brasileira que visa garantir a proteção dos dados pessoais dos cidadãos e estabelecer regras claras sobre como essas informações devem ser tratadas por empresas e organizações.

A LGPD foi aprovada em agosto de 2018 e entrou em vigor em setembro de 2020, após um período de adaptação. Ela é amplamente inspirada no Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês) da União Europeia, buscando trazer o Brasil em conformidade com as melhores práticas internacionais de proteção de dados.

A lei define dados pessoais como informações relacionadas a uma pessoa natural identificada ou identificável. Ela se aplica a todas as entidades públicas ou privadas que realizam o tratamento de dados pessoais, independentemente do meio ou do país em que estejam localizadas.

A LGPD estabelece uma série de princípios que devem ser seguidos pelas organizações no tratamento de dados pessoais, tais como. Finalidade para dados pessoais devem ser coletados para propósitos legítimos, específicos e informados aos titulares dos dados.

Necessidade o tratamento dos dados pessoais deve ser limitado ao mínimo necessário para a realização das finalidades estabelecidas. Transparência as organizações devem fornecer informações claras e acessíveis sobre como os dados

[12] Defensoria Pública do Estado do Ceará. Lei Carolina Dieckmann: 10 anos da lei que protege a privacidade dos brasileiros no ambiente virtual. Disponível em: https://www.defensoria.ce.def.br/noticia/lei-carolina-dieckmann-10-anos-da-lei-que-protege-a-privacidade-dos-brasileiros-no-ambiente-virtual/. Acesso em: 29 ago. 2022.

serão tratados. Qualidade dos dados sobre dados pessoais devem ser precisos, atualizados e completos.

Segurança medidas de segurança adequadas devem ser adotadas para proteger os dados pessoais contra acessos não autorizados, perdas ou vazamentos. Além dos princípios, a LGPD também prevê os direitos dos titulares dos dados, tais como o direito de acesso, retificação, exclusão e portabilidade de seus dados pessoais. Os titulares também têm o direito de revogar o consentimento dado para o tratamento de seus dados, quando este for a base legal para o tratamento.

A lei estabelece ainda a necessidade de uma base legal para o tratamento de dados pessoais, tais como o consentimento do titular, o cumprimento de obrigação legal, o exercício regular de direitos, a proteção da vida, a execução de contrato, o legítimo interesse ou o interesse público.

A LGPD também prevê sanções para o não cumprimento de suas disposições, incluindo advertências, multas que podem chegar a 2% do faturamento da empresa, limitação do funcionamento do banco de dados e até mesmo a proibição parcial ou total do exercício das atividades relacionadas ao tratamento de dados.

Em resumo, a LGPD é uma legislação que visa garantir a proteção dos dados pessoais dos cidadãos brasileiros, estabelecendo regras claras e princípios fundamentais para o tratamento dessas informações pelas organizações. Ela busca promover a privacidade e a segurança dos dados, empoderando os indivíduos em relação ao controle de suas informações pessoais.

3.4 Da convenção Européia sobre crimes cibernéticos – Convenção de Budapeste

A Convenção Europeia sobre Crimes Cibernéticos, também conhecida como Convenção de Budapeste, é um tratado internacional elaborado pelo Conselho da Europa para combater a criminalidade cibernética. Foi adotada em 23 de novembro de 2001 e entrou em vigor em 1º de julho de 2004. Atualmente, mais de 60 países, incluindo países não europeus, são signatários ou aderiram à Convenção.

O objetivo principal da Convenção de Budapeste é fornecer uma base jurídica para a cooperação internacional na prevenção e combate a crimes cibernéticos, bem como para a proteção dos direitos humanos no contexto digital. Ela abrange uma ampla gama de atividades criminosas, incluindo fraudes online, roubo de identidade,

pornografia infantil, ataques cibernéticos, violações de direitos autorais e outros delitos relacionados à tecnologia da informação.

A Convenção estabelece uma série de medidas e diretrizes para facilitar a cooperação entre os Estados signatários. Isso inclui disposições para a troca rápida de informações entre autoridades competentes, a investigação e a coleta de evidências eletrônicas transfronteiriças, a facilitação do acesso a dados armazenados no exterior, a criminalização de certas condutas cibernéticas e a promoção da conscientização e educação sobre segurança cibernética[13].

Além disso, a Convenção de Budapeste estabelece a criação de pontos de contato nacionais, que são órgãos responsáveis pela cooperação e assistência mútua entre as partes. Também prevê a criação de uma instância de monitoramento, conhecida como Grupo de Peritos sobre Crime Cibernético (C-PROC), que é responsável por auxiliar os Estados na implementação efetiva da Convenção.

A Convenção de Budapeste é amplamente considerada um marco importante no combate à criminalidade cibernética, pois promove a cooperação internacional e a harmonização das leis em matéria de crimes cibernéticos. No entanto, é importante destacar que nem todos os países adotaram ou ratificaram a Convenção, e ainda existem desafios significativos para lidar com a crescente sofisticação e alcance global dos crimes cibernéticos. Portanto, esforços contínuos são necessários para fortalecer a segurança cibernética e combater efetivamente esses tipos de crimes.

Brasília, 17/04/2023 o Governo Federal promulgou a Convenção sobre o Crime Cibernético, firmada em Budapeste. O Brasil, ao aceitar o convite do Conselho da Europa, passou a ser um dos países que aderiram a tal instrumento internacional multilateral, fortalecendo, assim, os laços de cooperação com parceiros estratégicos no enfrentamento aos crimes cibernéticos. O Decreto nº 11.491, que traz a decisão, foi publicado no Diário Oficial da União (DOU), no dia 12 de abril de 2023.

Graças à chamada Convenção de Budapeste, assinada em 23 de 2001, as autoridades brasileiras poderão contar com uma fonte adicional para investigar crimes cibernéticos, bem como outras infrações penais que exijam a coleta de provas

[13] MPF - Ministério Público Federal. MPF e Conselho da Europa promovem encontro internacionaldas redes de Ministérios Públicos sobre cibercriminalidade e provas digitais. Disponível em: https://www.mpf.mp.br/pgr/noticias-pgr2/2023/mpf-e-conselho-da-europa-promovem-encontro-internacional-das-redes-de-ministerios-publicos-sobre-cibercriminalidade-e-provas-digitais. Acesso em: 30 ago. 2022.

eletrônicas/digitais. Armazenados em outros países. Espera-se uma cooperação "mais forte, mais rápida e mais eficiente".

Para André Zaca Furquim, coordenador-geral de Cooperação Jurídica Internacional em Matéria Penal do Ministério da Justiça e Segurança Pública (MJSP), há uma expectativa de que a Convenção de Budapeste irá, gradativamente, elevar o número de pedidos de cooperação jurídica internacional. “Considerando que as investigações operadas no Brasil demandam, cada vez mais, provas eletrônicas que se encontram em outros países, esta Convenção irá facilitar e, portanto, encorajar os investigadores brasileiros a utilizar tal estratégia”. completou.

A diretora do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) do MJSP, Carolina Yumi diz que: "A integral implementação da Convenção de Budapeste no Brasil trará resultados positivos ao país, uma vez que ensejará a modernização de normativos e políticas adotadas na temática de enfrentamento aos crimes cibernéticos, assim como na coleta e preservação das provas digitais."

Além de fortalecer a cooperação internacional para enfrentar e explicar crimes no ambiente virtual, a Convenção incentiva o Brasil a continuar desenvolvendo sistemas jurídicos e políticos que levem em conta a evolução do crime no ambiente virtual. O equilíbrio certo deve ser encontrado entre o aumento da ação penal e a proteção de dados pessoais[14].

[14] Governo Federal. Convenção de Budapeste é promulgada no Brasil. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: 30 ago. 2022.

4 O QUE É PHISHING?

A fraude online é a forma mais simples de cibercrime, na qual criminosos ("golpistas") enganam as vítimas para que revelem informações confidenciais, como números de cartão de crédito e senhas. E-mail ou SMS são as táticas mais comuns usadas para enganar as pessoas. Os criminosos se fazem passar por indivíduos confiáveis ou entidades legais, como instituições financeiras.

Ao abrir uma mensagem SMS ou e-mail, a vítima encontrará uma mensagem que cria um senso de urgência. Este é o caso se você deseja pagar sua dívida o mais rápido possível ou redefinir uma senha comprometida. Isso permitiu que ele clicasse em um comando que acessava um site que imitava o site legítimo ao qual ele estava conectado. Atualmente, essas informações são enviadas a criminosos que as utilizam para fins ilícitos. Você entende o que é phishing? Em caso afirmativo, deixe claro que não é o mesmo que spam.

Spam e phishing são a mesma coisa? não. Spam é simplesmente lixo eletrônico, publicidade não solicitada que não tem a intenção de prejudicar o destinatário. Na tentativa de phishing, os criminosos querem roubar dados e utilizá-los contra você ou sua empresa. Vamos ver então como funciona este tipo de crime cibernético!

Um ataque de phishing consiste em três elementos específicos. Isso é feito por meio de comunicação eletrônica. Criminosos se passando por indivíduos ou entidades confiáveis o objetivo da fraude é obter informações pessoais ou comerciais confidenciais. Portanto, antes de aprender a solucionar ataques de phishing, é necessário perceber que o mecanismo de operação é o mesmo.

Os golpistas enganam as vítimas para que baixem anexos, cliquem em links e enviem dados confidenciais. Quanto mais habilidoso for um phisher, mais danos ele pode causar ao seu negócio isso é feito por meio de comunicação eletrônica. O agente faz-se passar por pessoa singular ou coletiva credível.

Como o phishing pode prejudicar sua empresa?

O impacto negativo desses ataques cibernéticos vai muito além do prejuízo financeiro. O foco do golpe é o retrato de uma pessoa ou organização em quem a vítima confia. Não é incomum que os hackers criem perfis falsos de mídia social para

construir relacionamentos com alvos em potencial. Se a tentativa for bem-sucedida, a vítima pode perder a confiança na empresa.

Afinal, como confiar em uma organização que vazou dados? Assim, os ataques não roubam apenas dinheiro, informações pessoais e outros dados. Mais motivos para aprender mais sobre golpes e diferentes tipos de golpes. Quais os diferentes tipos de phishing?

Por e-mail método mais comum deste golpe, que servirá de isca para o ataque. Em geral, a mensagem escrita aos destinatários contém anexos com malware ou links que levam a sites maliciosos, feitos para roubar dados. Esses e-mails fraudulentos costumam ter uma aparência legítima, com logotipos e design semelhantes aos das organizações reais. Eles geralmente tentam induzir as pessoas a clicar em links maliciosos, fornecer informações pessoais ou baixar anexos infectados por malware.

Os ataques também podem vir de sites falsos que imitam sites genuínos e confiáveis. Imagine que você tem uma conta no Banco Beta, o maior banco dos Estados Unidos. Somos uma instituição financeira confiável e comprovada. No entanto, os hackers geralmente imitam seu site, colam suas informações de login e as confundem com o site oficial. Você pode usar essas informações para fazer login em sua conta real. Esse tipo de golpe também pode ser facilitado por pop-ups comuns em sites.

Vishing é a versão em áudio, o phishing de voz. Na prática, o criminoso tentará obter seus dados por telefone, com o fim de roubar sua identidade. Fique atento com as chamadas automatizadas, que são exemplos de tentativa de phishing. O termo é uma combinação das palavras "voice" (voz) e "phishing" (pescaria), referindo-se à prática de pescar informações confidenciais dos usuários.

Nesse tipo de golpe, os criminosos se passam por representantes de instituições confiáveis, como bancos, empresas de cartão de crédito ou serviços governamentais, e entram em contato com as vítimas por telefone. Eles geralmente usam técnicas de engenharia social para obter informações pessoais, financeiras ou outras informações confidenciais das pessoas. Os golpistas são altamente persuasivos e usam táticas para induzir as vítimas a revelarem dados sensíveis, como números de cartão de crédito, senhas, códigos

Smishing é um golpe feito por SMS. Smishing é uma forma de fraude que combina as palavras "SMS" (Short Message Service) e "phishing" (pescaria). Nesse tipo de golpe, os criminosos enviam mensagens de texto falsas para os telefones

celulares das vítimas, com o objetivo de obter informações pessoais, financeiras ou induzi-las a realizar ações indesejadas.

Os golpistas se passam por instituições legítimas, como bancos, empresas de cartão de crédito, empresas de telecomunicações ou serviços online populares, e enviam mensagens que parecem autênticas. Essas mensagens geralmente solicitam às vítimas que forneçam informações confidenciais, como números de conta.

4.1 Phishing nas Redes Sociais

Você sabe o que são golpes no Instagram e no LinkedIn? As redes sociais são fonte de muitas informações pessoais e são acessadas por milhões de pessoas em todo o mundo. Com isso em mente, os golpistas adaptam seus ataques nas mídias sociais aos desejos e necessidades de suas vítimas.

Finalmente, você terá acesso fácil a informações sobre seu estilo de vida e trabalho. Mas é os ataques de mídia social, por exemplo, os invasores podem criar perfis falsos para cometer crimes. Outra forma de ataque cibernético envolve obter acesso à conta de um usuário e enganar amigos para que enviem links maliciosos. Com tantas possibilidades, é importante entender as estratégias utilizadas pelos hackers. Esta é a melhor maneira de se proteger de ataques.

As técnicas de phishing são diversas e incluem técnicas simples e complexas. A propósito, muitos deles trabalham no Brasil. A Coreia do Sul lidera a lista de usuários mais afetados por ataques de phishing (12,39%), de acordo com as estatísticas de 2022. Tem certeza de que entende bem esses tipos de golpes na prática? É importante conhecer algumas estratégias que podem ajudar seu programa de segurança a resolver esses problemas. Confira alguns a seguir.

4.2 Tipos de phishing

"Whaling", que é uma forma específica de ataque de phishing direcionado a indivíduos de alto perfil, como executivos de empresas ou figuras de destaque.

Whaling, também conhecido como spear phishing, é um tipo de ataque que envolve a personalização e direcionamento de e-mails fraudulentos para indivíduos específicos, com o objetivo de obter informações confidenciais ou acesso não autorizado a sistemas corporativos. OS golpistas por trás do whaling conduzem uma

pesquisa minuciosa sobre suas vítimas, coletando informações de fontes públicas, como redes sociais e sites de empresas. Com base nessas informações, eles criam e-mails altamente convincentes e personalizados, que podem se passar por colegas de trabalho, parceiros de negócios ou até mesmo altos executivos da empresa.

Esses e-mails geralmente parecem legítimos e são projetados para enganar a vítima e fazê-la agir de acordo com as instruções do atacante. Os e-mails de whaling podem solicitar informações confidenciais, como senhas, números de cartão de crédito ou detalhes de contas bancárias, ou podem conter links ou anexos maliciosos que, quando abertos, infectam o sistema do usuário com malware.

Para se proteger contra ataques de phishing whaling, é essencial estar ciente dos sinais de alerta, como e-mails não solicitados ou inesperados, erros gramaticais ou ortográficos, endereços de e-mail suspeitos ou solicitações incomuns. Além disso, é importante manter-se atualizado sobre as práticas recomendadas de segurança cibernética, como nunca fornecer informações confidenciais por e-mail e verificar cuidadosamente a autenticidade das solicitações antes de tomar qualquer ação. Utilizar software antivírus atualizado e manter-se informado sobre os métodos mais recentes de ataques de phishing também é recomendado.

O phishing fraudulento é um tipo de ataque cibernético que manipula psicologicamente os usuários para revelar informações confidenciais ou realizar ações indesejadas. Ao contrário do phishing tradicional, que pode ser mais comum, o phishing é projetado para parecer muito persuasivo e persuasivo, explorando a confiança e a credibilidade da vítima.

Os golpistas que realizam ataques de phishing enganosos geralmente fingem ser uma organização ou entidade confiável, como um banco, empresa de comércio eletrônico, rede social ou serviço de e-mail. Eles fazem cópias exatas dos sites legítimos dessas organizações, incluindo logotipos, designs e conteúdo, para enganar as vítimas.

Ataques de phishing enganosos podem ocorrer por vários canais, incluindo e-mail, mensagens de texto, telefonemas ou anúncios falsos em sites legítimos. Seu principal objetivo é forçar as vítimas a fornecer informações pessoais confidenciais, como senhas, números de cartão de crédito, dados bancários ou dados de identificação.

Para tornar os ataques mais convincentes, os golpistas podem usar técnicas de engenharia social, como criar um senso de urgência ou oferecer recompensas

falsas. Por exemplo, um e-mail de phishing fraudulento pode notificar as vítimas sobre atividades suspeitas em suas contas bancárias e solicitar que forneçam informações de login imediatamente para evitar atividades fraudulentas.

É importante conhecer os sinais de alerta para se proteger de ataques fraudulentos de phishing. Isso inclui verificar cuidadosamente a autenticidade dos remetentes de e-mail, verificar informações como erros gramaticais ou ortográficos, não clicar em links questionáveis, não validar solicitações e não fornecer informações pessoais ou confidenciais.

Também recomendamos que você use um software antivírus atualizado, mantenha seu sistema operacional e aplicativos atualizados e se informe sobre as práticas de segurança cibernética. Scripting entre sites acontece quando os hackers exploram vulnerabilidades nos scripts de um site para roubá-lo para seus próprios fins.

A clonagem de phishing é um tipo de ataque de phishing no qual os fraudadores criam cópias quase perfeitas de sites legítimos para induzir os usuários a revelar informações confidenciais. Nesse tipo de ataque, os criminosos copiam ou duplicam sites legítimos, incluindo seu design, logotipo e conteúdo para fazê-los parecer autênticos e confiáveis.

Phishing O processo de clonagem geralmente começa com o golpista enviando um e-mail de phishing para a vítima. Este e-mail pode se passar por empresas conhecidas, como bancos, redes sociais, serviços de correio e outras organizações conhecidas. Os e-mails podem conter mensagens falsas, como uma suspeita de violação de segurança ou uma solicitação para atualizar as informações da sua conta.

Ao clicar no link fornecido no e-mail, a vítima será redirecionada para um site clonado que se parece exatamente com o site legítimo. No entanto, o site clonado é controlado pelos bandidos e visa roubar informações privadas e confidenciais da vítima. Uma vez no site clonado, a vítima pode ser solicitada a inserir credenciais de login, informações bancárias, números de cartão de crédito e outras informações confidenciais.

Essas informações podem ser capturadas por fraudadores e usadas para fins fraudulentos, como roubo de identidade e acesso não autorizado à conta. Para se proteger de cópias fraudulentas, é importante ficar atento aos sinais de alerta. Isso inclui a triagem cuidadosa dos remetentes de e-mail, verificação de erros gramaticais e ortográficos, não clicar em links suspeitos e nunca compartilhar informações

confidenciais por meio de links em e-mails não solicitados ou e-mails. Além disso, recomendamos inserir manualmente endereços de sites legítimos na barra de endereço do navegador em vez de clicar em links e usar firewall e software.

A fraude de CEO, também conhecida como "CEO fraud" ou "Business Email Compromise" (BEC), é um tipo sofisticado de golpe que visa enganar e defraudar empresas. Nesse tipo de fraude, os golpistas se passam pelo CEO ou por outro alto executivo de uma organização para solicitar transferências de fundos ou informações confidenciais a funcionários da empresa.

A fraude de CEO geralmente envolve uma cuidadosa pesquisa e coleta de informações sobre a empresa-alvo, incluindo nomes de executivos, cadeia hierárquica, processos internos e relacionamentos comerciais. Os golpistas usam essas informações para criar e-mails falsos que parecem autênticos e convincentes.

Ao se passar pelo CEO, o golpista envia um e-mail para um funcionário da empresa responsável por operações financeiras ou transferências de fundos. O e-mail pode solicitar uma transferência de dinheiro urgente para uma conta específica, justificando a necessidade de confidencialidade ou alegando uma transação comercial importante.

Os golpistas também podem explorar outras técnicas de engenharia social, como o uso de e-mails com urgência ou situações de crise, para pressionar os funcionários a agirem rapidamente, sem questionar ou verificar a autenticidade do pedido.

A fraude de CEO pode resultar em perdas financeiras significativas para as empresas. As transferências de fundos podem ser direcionadas para contas controladas pelos golpistas, que podem rapidamente retirar os fundos e desaparecer.

Para se proteger contra a fraude de CEO, é fundamental implementar medidas de segurança robustas. Isso inclui a implementação de políticas de verificação rigorosas para solicitações de transferências de fundos, a criação de procedimentos de autorização.

A manipulação de links é uma técnica empregada por cibe criminosos para enganar os usuários e direcioná-los a sites maliciosos ou fraudulentos. Essa prática envolve a alteração do destino real de um link, fazendo com que pareça apontar para um site legítimo, quando na verdade redireciona para um site malicioso.

Os golpistas podem realizar a manipulação de links de diferentes maneiras. Uma técnica comum é a modificação do URL exibido, tornando-o semelhante ao de

um site confiável, mas com pequenas diferenças imperceptíveis para o usuário desavisado. Por exemplo, um link para o site "www.exemplo.com" pode ser alterado para "www.exenplo.com" ou "www.exemplo-secure.com".

Outra forma de manipulação de links é a ocultação do URL real por meio do uso de hiperlinks ou redirecionamentos. O texto exibido no link pode parecer seguro e confiável, mas ao clicar nele, o usuário é levado para um site diferente do esperado.

A manipulação de links é frequentemente utilizada em ataques de phishing, onde os golpistas enviam e-mails falsos que parecem ser de instituições legítimas, como bancos, empresas ou serviços online. Esses e-mails solicitam que os usuários cliquem em um link para fornecer informações pessoais ou confidenciais, como senhas, números de cartão de crédito ou dados de login.

Para se proteger contra a manipulação de links, é importante adotar algumas práticas de segurança. Verificar cuidadosamente os URLs antes de clicar em um link, passando o cursor do mouse sobre ele para exibir o destino real, é uma medida importante. Além disso, é recomendado evitar clicar em links enviados por e-mails não solicitados ou suspeitos e preferir digitar manualmente os endereços dos sites legítimos na barra de endereços do navegador. Utilizar softwares de segurança, como antivírus e bloqueadores de phishing, também é recomendado para detectar e bloquear sites maliciosos.

O pharming é uma forma sofisticada de ataque cibernético que visa redirecionar o tráfego de um site legítimo para um site falso, sem o conhecimento do usuário. É uma técnica mais avançada do que o phishing, pois não requer que o usuário clique em um link malicioso para ser redirecionado.

Os golpistas usam o pharming para explorar vulnerabilidades nos sistemas de resolução de nomes de domínio (DNS), que são responsáveis por traduzir nomes de domínio em endereços IP. Por meio de técnicas como envenenamento de cache DNS ou ataques de redirecionamento de DNS, eles manipulam os registros DNS para que os usuários sejam redirecionados automaticamente para sites falsos quando digitam o endereço de um site legítimo em seus navegadores.

Quando um usuário digita o endereço de um site legítimo em seu navegador, o sistema de resolução de nomes de domínio direciona o tráfego para o site falso controlado pelos golpistas. Esse site falso geralmente é projetado para se parecer exatamente com o site legítimo, incluindo logotipos, layout e conteúdo. O objetivo dos

golpistas é roubar informações confidenciais dos usuários, como nomes de usuário, senhas, informações de cartão de crédito ou detalhes de contas bancárias.

O pharming pode ser particularmente perigoso, pois os usuários são redirecionados automaticamente para sites falsos sem seu conhecimento, tornando mais difícil identificar o ataque. Além disso, os golpistas podem atingir um grande número de usuários ao mesmo tempo, em vez de depender de envio de e-mails de phishing individualmente.

Para se proteger contra o pharming, é importante adotar medidas de segurança. Manter o sistema operacional e os aplicativos atualizados com as últimas correções de segurança, usar um software antivírus confiável, evitar clicar em links suspeitos e digitar manualmente os endereços de sites legítimos na barra de endereços do navegador são práticas recomendadas.

Também é recomendado verificar se o site acessado usa uma conexão segura (HTTPS) e monitorar regularmente as atividades financeiras e contas online em busca de atividades suspeitas. A partir das estratégias e dos tipos de golpe deste crime cibernético, vamos citar alguns exemplos de phishing por e-mail. Exemplos de e-mails de phishing

Conforme mencionado anteriormente, o e-mail é o método mais comum usado pelos hackers para cometer phishing. Existem três exemplos muito comuns de golpes relacionados a isso. Avisos bancários, relatórios governamentais e problemas de pagamento, alerta de banco.

Uma técnica comum usada pelos golpistas é convencer as vítimas em potencial a verificar seus dados bancários. De fato, muitas instituições financeiras emitem alertas regulares para detectar atividades suspeitas e saques a descoberto. Criminosos se comportam da mesma maneira. O que o governo diz?

Os usuários que seguem e confiam nas autoridades, como funcionários do governo, têm maior probabilidade de aceitar esses e-mails de phishing. Por exemplo, o aviso pode indicar que os usuários serão penalizados caso não forneçam os dados pessoais solicitados. Em vez disso, benefícios como reembolso de impostos podem ser fornecidos após os usuários confirmarem suas informações financeiras. Problema de pagamento/pagamento

Finalmente, outro tipo comum de ataque por e-mail é a incapacidade de pagar por um determinado produto ou serviço. O destinatário é notificado de que há um problema no pagamento da conta e é solicitado a fornecer informações financeiras na

página inicial. Para onde vão os dados roubados? "Cães, roubo, exposição. Isso mostra que os dados roubados são vendidos principalmente na dark web.

Existem informações mais baratas, como número da carteira de identidade, e outros mais caros, como prontuários médicos e contas de bancos digitais. Para evitar esses ataques, é possível adotar algumas práticas em sua empresa e, claro, educar os demais profissionais. Como evitar cair em um phishing?

A desconfiança é a primeira linha de defesa contra ataques de phishing. Existem sinais que os usuários podem analisar para garantir uma computação mais segura. A atitude da administração em relação aos golpes começa com a introdução de sistemas de proteção.

Ter um sistema de defesa um bom plano de segurança da informação fornece uma variedade de recursos para prevenir ou pelo menos complicar ataques cibernéticos. Usar um software de segurança anti malware, um bom software antivírus comercial e um firewall eficaz é essencial para evitar ser vítima de golpes. Isso não é tudo. Um sistema tecnológico que proteja a internet é essencial.

Por exemplo, ferramentas de segurança cibernética são capazes de detectar links e anexos maliciosos. Preste atenção no link outra forma de evitar golpes é ter cuidado com os links de entrada. Não abra links de remetentes desconhecidos para verificar se o link é válido, coloque o ponteiro do mouse sobre o link na mensagem (não clique). Em caso de dúvida, insira manualmente o site no seu navegador para verificar se é confiável.

Observe a ortografia de e-mails, mensagens, etc**.** Conforme mencionado anteriormente, os criminosos podem usar sites falsos para lançar ataques. Esta página pode ter o mesmo endereço do site original portanto, cuidado com erros de digitação e texto mal escrito com erros de digitação ou gramática. Agências confiáveis raramente cometem tais erros.

Não dê informações pessoais os criminosos querem suas informações, portanto, nunca forneça suas informações pessoais. É raro uma empresa conceituada solicitar esse tipo de dado por e-mail ou telefone. Se você não tiver certeza, inicie uma comunicação adicional por meio de nossos canais oficiais. Se você acha que seu site é oficial, verifique se o URL dele começa com "HTTPS".

Atenção às imagens os cibe criminosos falsificam sites oficiais e usam as cores, logotipos e slogans da marca da empresa. Sua finalidade é fornecer mais funcionalidade ao e-mail. Mas cuidado com esta foto. Para completar sua defesa

contra phishing, saiba como a proteção da Algar Telecom pode contribuir para o seu plano de segurança.

O objetivo do golpe é obter informações pessoais ou comerciais confidenciais. Antes de aprendermos como solucionar ataques de phishing, precisamos reconhecer que o mecanismo de ação é o mesmo. Os golpistas tentam induzir as vítimas a baixar anexos ou clicar em links para enviar dados confidenciais. Quanto mais habilidoso for um phisher, mais danos ele pode causar ao seu negócio.

Como o phishing pode prejudicar seus negócios? Os danos financeiros não são o único impacto negativo desses ataques cibernéticos. No centro da fraude está a representação de uma pessoa ou entidade em quem a vítima confia. É comum hackers criarem perfis falsos nas redes sociais com o objetivo de estabelecer relacionamento com possíveis alvos.

Se essa tentativa for bem-sucedida, a vítima pode perder a confiança em sua empresa. Afinal, como ela vai confiar em uma organização que perdeu seus dados? Portanto, o ataque não é apenas para roubar dinheiro, informações pessoais e outros dados. Outro motivo para aprender mais sobre mineração de dados, mineração de dados, mineração de dados, tipos de ataques.

Fernando Brandini Barbagalo disse "Como a lei brasileira não tem um crime separado para fraude, é confuso ter uma definição diferente do crime (fraude eletrônica) do que em outros países (como a Itália)." Inclui a obtenção (permitida ou tentada) de ganhos ilegais.

Por outras palavras, uma das críticas ao artigo 171.º, no 2, alínea a) do Código Penal assenta no postulado de que o termo “fraude” não pode ser utilizado como categoria primária. A desvantagem do legislador é que o usam como nome e não têm um imperativo verbal para se referir aos desvios. A fraude eletrônica exige que a vítima tome uma atitude positiva ao fornecer informações.

A estrutura semelhante de fraude e roubo indica claramente que o peculato está correto, como em "se o peculato for cometido" ou “obtenção de lucros ilícitos” aproveitando-se do conteúdo do crime para configurar o crime de furto. Outra questão é a semântica em torno do nome "e-scam". Os legisladores usaram o termo "eletrônica" em vez de "tecnologia da informação".

O termo eletrônica refere-se a dispositivos eletrônicos que exibem a estrutura eletrônica de elétrons ou átomos. Pela natureza deste crime, o uso de palavras informáticas ou digitais é claramente adequado e refere-se a informações transmitidas

e armazenadas em rede (a Internet). De acordo com as definições do dicionário, a palavra computador refere-se ao corpo de conhecimentos científicos e métodos que permitem que os computadores processem informações automaticamente.

Finalmente, o aumento contínuo do cibercrime não se deve à falta de classificação adequada, nem ao impacto simbólico e instrumental de padrões que não afetam mais os beneficiários. Com o crescimento exponencial do cibercrime em todo o mundo, além dos formuladores de políticas, a necessidade urgente de redes de prevenção ao cibercrime é enorme. O objetivo deste é facilitar a discussão jurídica e acadêmica sobre os conflitos processuais que possam surgir em relação à Lei de Sinistros 14.155/2021.

Pensar em acessar e usar a Internet hoje é também pensar em se proteger e manter as informações transmitidas na Web. Ataques a sites que vendem e fraudam internautas são cada vez mais frequentes e insidiosos. Coincidentemente, nos últimos 15 anos, os cibe criminosos deixaram de ser atividades de hackers amadores para se tornarem uma verdadeira indústria do crime organizado.

Roubo de identidade, senhas de cartão de crédito, roubo eletrônico e fraude de identidade são alguns dos golpes mais comuns usados por cibe criminosos e golpistas. Em nosso ambiente virtual conectado, existem muitas ameaças eletrônicas, entre elas a fraude online, umgolpe online generalizado que causa enormes prejuízos econômicos e sociais a bancos, empresas, governos e consumidores em geral[15].

Nesse tipo de fraude eletrônica, os criminosos frequentemente exploram as vulnerabilidades técnicas dos internautas e usam a engenhariasocial para induzir os usuários a revelar informações pessoais, pessoais ou secretas. Eles também oferecem muitas outras coisas[16]**.** Medidas que permitem que criminosos acessem informações confidenciais[17].

O maior desafio para os novos cibe criminosos é descobrir suas características. De fato, o cibercrime está mudando a estrutura da lei criminal, forçando estudiosos e agências de aplicação da lei a reexaminar ou reexaminar a lei com base em novos fatos sociais e de computador.

---

[15] MOORE, Tyler.; CLAYTON, Richard .; ANDERSON, Ross. The Economics of online crime. Journal of Economic Perspectives, v. 23, n. 3, p. 3-20, nov./dec. (2009)

[16] CGI.BR. Cartilha de Segurança para Internet. Comitê Gestor da Internet no Brasil, 2012. Disponível em: http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf . Acesso em: 28 ago. 2022.

[17] OLLMANN, Gunter. The phishing guide: understanding & preventing phishing attacks.2007, Disponível me: http://www-935.ibm.com/services/us/iss/pdf/phishing-guidewp.pdf. Acesso em: 29 ago 2022.

O maior desafio com os novos cibe criminosos é explicá-lo. Com efeito, o cibercrime desorganizou a estrutura do direito penal, forçando estudiosos e agências de aplicação da lei a reconsiderar ou revisar a lei com base em novos fatos sociais e de computador. No caso particular da fraude, descobrimos que nem a lei criminal,

nem a conhecida lei Carolina Dieckmann, nem a lei do consumidor aplicável eram capazes de proteger a ameaça por conta própria.

Da mesma forma, a menos que leis mais amplas e específicas sejam promulgadas, a fraude é geralmente considerada peculato ou roubo. Portanto, o objetivo deste estudo é focar especificamente nos aspectos técnicos e legais relacionados à fraude na Internet, para entender a relação entre o comportamento virtual e econômico da "fraude" e o pagamento Responder às seguintes perguntas. A fraude é adequada? É como um voo decente, vale a pena? A fraude não é considerada crime contra a economia nacional? Como digitar?

4.3 Crime, economia e tecnologia

A criminologia tem estudado as origens e causas do crime ao longo dos últimos dois séculos, valendo-se de conhecimentos da biologia, psicologia, sociologia e antropologia[18]. Assim, a abordagem econômica do crime surgiu pela primeira vez no final dos anos 1960 por meio de um corpo de trabalho que buscava analisar o comportamento criminoso com base na suposição econômica deque os lucros dos criminosos eram maximizados. Uma mudança de paradigma da antropologia e psicologia para a economia foi o artigo "Crime e Castigo: UmaAbordagem Econômica" do economista Gary Becker, no qual ele vê o crime como assassinato racional e como os criminosos se comportam. A relação entre os custos/desvantagens e os benefícios da atividade. Existem dois tipos de crimes cometidos por escritores americanos: crimes que visam ganhos econômicos, como sonegação de impostos e tráfico de pessoas, crimes de colarinho branco relacionados a atividades econômicas e industriais reais e crimes não comerciais, como assassinato, como o estupro[19]. Com base nos insights de Becker, outros estudos empíricos foram conduzidos sobre a teoria da escolha racional, que leva em consideração fatores mais estruturais, como mercado de trabalho, renda, dissuasão da polícia, demografia e outras variáveis[20].

Quando se trata de crimes cibernéticos, a linha entre a lei e os negócios é muito

[18] VIAPIANA, Luiz Tadeu. Economia do Crime: Uma Explicação para a Formação do Criminoso, Porto Alegre: 2006, AGE Editor

[19] SHIKIDA, Pery Francisco Assis. In: Economic Analysis of Law Review. Brasília, v 1 n 2 p. 424-jul-dez.2010. Disponível em: http://portalrevistas.ucb.br/index.php/EALR/ article/viewArticle/ 1%20EALR%20318. Acesso em: 29.ago 2014.

[20] CERQUEIRA, Daniel. LOBÃO, Waldir. Determinantes da criminalidade: uma resenha dos modelos teóricos e resultados empíricos. IPEA - exto para discussão nº 956. Rio de janeiro, jun. 2003. Disponível em: http://www.ipea.gov.br/portal/images/stories/PDFs/TDs/td_0956.pdf. Acesso em: 12 dez. 2013.

mais clara e inseparável. Porque existem golpes na Internet que visam principalmente ganhos financeiros ilegais. O impacto desses eventos é significativo e as consequências econômicas, sociais e sociais recentes são enormes. Segundo estudo

patrocinado pelo CERT.BR, ocorreram 7.959 ocorrências envolvendo instituições financeiras em 2010, número que subiu para 11.659 ataques em 2011[21]. Milhares de pessoas em todo o mundo sofreram perdas devido a esse tipo de ataque.

4.4 Crime contra a economia popular: uma lei que parou no tempo

Modelado após o sistema italiano, a Lei de Proteção da Economia Nacional (HORN, 2013, p. 99)[22]. foi promulgada em 1951 para proteger os bens públicos contra fraude por meio de conduta desonesta ou enganar, monopólio, abuso e especulação podem prejudicar os interesses econômicos e a propriedade de indivíduos e pessoas (Ibid., p. 101). Este Código está registrado sob a Lei nº 2. 1.521/51 e um documento de 34 artigos que estabelece hipótese criminal sobre a ordem econômica humana, por exemplo, detenção de bens (I, art. 2º) crimes em favor de compradores e clientes (art. 2º, art. 2º) de produtos. se a prestação do serviço foi anunciada ou não (2. Artigo 4.º). Conforme observado acima, algumas disposições da Lei foram substituídas por estatutos posteriores que determinam conduta semelhante.

7.492/86 estabeleceu a norma para criminalizar as condutas contra o sistema financeiro nacional e acabou revogando diversos pontos e leis, principalmente no que se refere à criação de legislação para proteger os direitos do consumidor. Devido à extrema escassez de normas econômicas pós-crime, a consequência desse controle legislativo é que situações semelhantes ou semelhantes são esperadas, apesar de sua importância na proteção do Estado e da economia uma delas é o abandono e reutilização de normas.

De fato, não há lei. 8.137/90 e outrospadrões distribuídos não são poderosos o suficiente para remover todas as normas de uma só vez. 1.521/51 ordenamento jurídico brasileiro. Entre as poucas disposições importantes ainda em vigor, destacamos o Artigo IX 2°, que prevê atos ilícitos contra o Estado por meio de especulação e fraude em detrimento da economia internacional.

Segundo o artigo 2°:

[21] HOEPERS, Cristine. Fraudes via Internet –. Estatísticas e Tendências. 2011. Disponível em: http://www.cert.br/docs/palestras/certbr-forum-comercio-eletronico2011.pdf.
[22] HORN. Manuela Bittar. O duplo nível de legalidade e os crimes contra a economia popular no direito penal autoritário. Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Programa de Pós-Graduação em Direito, Florianópolis, 2013.

> ´´Art. 2º. São crimes desta natureza: IX - obter ou tentar obter ganhos ilícitos em detrimento do povo ou de número indeterminado de pessoas mediante especulações ou processos fraudulentos ("bola de neve", "cadeias", "pichardismo" e quaisquer outros equivalentes); (BRASIL, 1951)``[23].

O artigo referenciado a respeito da previsão acima menciona três tipos de fraude: “bola de neve”, “corrente” e “picardismo”, mas o principal entendimento doutrinário e legal vai além disso. Algumas espécies também devem ser incluídas[24]. para aplicação e proteção completas. O mesmo vale para o Artigo 2, Cláusula 9 da lei. 1.521/51 equivale aproximadamente ao peculato daSeção 2.

O artigo 171.º do Código Penal (“Actos destinados a obter lucros ilícitos para si ou para outrem, causar prejuízo a outrem, promover mal-entendidos ou prolongar mal-entendidos por meio de dolo, engano ou outras artimanhas. outros desleais.) tem natureza diversa. Questões relacionadas com os colaboradores da atividade. Com efeito, no caso de fraude, o contribuinte deve ser uma pessoa específica para descrever o comportamento.

Pode ser aplicada ao direito econômico ou interpretada no direito do consumidor[25]. Olhando para toda a história legislativa e considerando as novas e significativas alterações por ela introduzidas, questiona-se se é possível compreender se a lei acompanhou os tempos e se adaptou à sociedade atual. Lei nº1521/51, revogada devido a novos crimes cibernéticos, mas mais preocupada com aproteção legal contra processos fraudulentos de pessoas não identificadas. A principal razão é que a estrutura da Internet permite uma ampla gama de atividades criminosas indiscriminadas.

4.5 Phishing como criminalizar?

No caso do phishing, parece não haver uma lei específica e abrangente sobre

[23] Brasil. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 ago. 2022.
[24] FERNANDES, Antonio Scarance . Considerações sobre o vídeo pôquer como atividade criminal. Justitia (São Paulo), v. 52, p. 84-92, 1990. Disponível em: http://www.justitia.com.br/revistas/x722dx.pdf. Acesso em 15 jan 2023.
[25] GRECO FILHO, Vicente . Algumas observações sobre o direito penal e a internet. Revista de Direito Mackenzie, v. 1, p. 35-39, 2000.

a atividade criminosa, por isso há um ar de proibição que a vê como peculato, furto grave e, ainda por cima, de ordem econômica do povo.

Algumas pessoas inicialmente acreditaram que a fraude deveria ser classificada como crime de furto porque é praticada por meio de fraude nos termos

do Artigo 155, Seção §4º, II ou§4º-B, o texto legal do Código Penal. A referida lei trata de roubo fraudulento usando um dispositivo eletrônico ou informático.

Essa visão é baseada no fato de que o phishing coleta dados de usuários da Internet de forma fraudulenta, principalmente por meio do envio de mensagens por e-mail. No entanto, importa referir que este tipo de crime, ao contrário do phishing, caracteriza-se por uma boa inegabilidade, uma vez que envolve a transmissão intencional de dados por parte da vítima.

De acordo com Sarrubo:

> ´´Distinção do furto mediante fraude para o estelionato: no furto, a fraude ilude a vigilância do ofendido que, em razão disso, não percebe que a coisa está saindo da esfera de seu patrimônio. No estelionato, ao contrário, a fraude faz com que a vítima incida em erro e, em virtude desse erro, voluntariamente, despojou-se de seu bem, tendo consciência de que ele está saindo da esfera de seu patrimônio``[26].

Uma outra corrente considera o phishing como um crime de estelionato, na forma do artigo 171 do Código Penal, na medida em que trata da obtenção de vantagem ilícita, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.

Segundo Sequeria Patricia:

> ´´Há quem entenda que no caso do Phishing Scan, aplica-se o art. 171 do Código Penal (e não o art. 155 de furto mediante fraude), isto é, crime de estelionato, que é descrito como “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´´[27].

[26] SARRUBBO, Mário L. Direito Penal: Parte Especial. Barueri, SP: Editora Manole, 2012. Ebook. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788520444368/. Acesso em: 28 nov. 2022.

[27] PINHEIRO, Patricia P. Segurança Digital - Proteção de Dados nas Empresas. 1ª edição. São Paulo, SP: Grupo GEN, 2020. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597026405/. Acesso em: 28 ago. 2022.

Com efeito, a observação das modalidades de peculato por fraude eletrônica elegíveis previstas no Código Penal pela lei n. º14.155/22 prevista no §2º-A do artigo 171 “Diploma Legal” aumenta ainda mais a probabilidade de o peculato ser enquadrado como crime.

Este tipo de fraude inclui fraudes realizadas com base em informações fornecidas pela vítima ou por um terceiro enganado por meio de mídias sociais, listas telefônicas ou mensagens eletrônicas ou outros meios de fraude.

Assim, o estelionato é entendido por muitos autores como o tipo penal ideal para o phishing, considerando a semelhança de suas características.

Segundo Gonçalves:

> ´´O tipo penal do estelionato exige a obtenção de vantagem em prejuízo “alheio”, sendo necessária, portanto, a identificação de pessoas ou pessoas determinadas que tenham sofrido lesão patrimonial. No estelionato, é necessária a identificação da vítima``[28].

O phishing normalmente envolve o envio de um e-mail genérico e não personalizado para atingir o maior número de pessoas possível. Na verdade, na maioria dos casos, o objetivo do phishing é coletar o máximo possível de informações pessoais sobre o usuário ou enganar certas pessoas. Portanto, a taxa de sucesso desse método é alta.

Portanto, é importante ressaltar que o alvo não é necessariamente uma pessoa específica, mas sim um grupo de potenciais vítimas. A fraude depende da cooperação da vítima. Como resultado, alcançar mais usuários aumenta as chances de os criminosos atingirem seus objetivos.

[28] GONÇALVES, Victor Eduardo R.; LENZA, Pedro. Esquematizado - Direito Penal - Parte Especial. São Paulo, SP: Editora Saraiva, 2022. E-book. ISBN 9786555597738. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555597738/. Acesso em: 29 nov. 2022.

Com isso em mente, podemos concluir que, na maioria dos casos, as vítimas de fraude não são pessoas específicas. Neste caso, no entanto, há exceções quando há alvos específicos nos quais os criminosos de informação estão particularmente interessados. Casos típicos de fraude cibernética nessa situação, ficando caracterizada a prática do spear phishing já citados anteriormente.

Claro, que o phishing pode causar danos incalculáveis à vítima. Portanto, a pena deve ser compatível com a gravidade do crime. Por outro lado, pode criar um sentimento de impunidade em favor dos criminosos.

Portanto, embora o phishing possa ser interpretado e punido pela lei penal vigente, é esperado que o phishing continue neste país porque não há regulamentação específica e atual, portanto, não há punição em conformidade.

Como qualquer outro crime cometido na Internet, é difícil para os legisladores acompanhar os avanços da tecnologia que os criminosos usam e desenvolver regulamentações que realmente abordam o comportamento criminoso na rede, deixando brechas que impossibilitam isso. A responsabilização de tais práticas que daqueles que a executam.

Pode-se dizer que o phishing é uma prática típica que existia antes da disseminação da Internet, mas para encontrar uma legislação que reflita as características da fraude, é necessário avaliar e considerar a singularidade da fraude. Conforme explicado acima, a ausência de regras específicas significa que certos detalhes relacionados a violações individuais podem ser excluídos do escopo da ação permitida, resultando em ação incomum.

Segundo Teixeira sobre o Código Penal:

> ´´Há uma enorme expectativa e ansiedade para uma adequada normatização que trata da informática, especialmente no campo criminal, pois diante da ausência de legislação específica têm-se aplicado o Código Penal (que recentemente foi alterado para abrigar alguns poucos crimes relacionados à informática) e leis especiais. Isso porque alguns fatos delitivos enquadram-se perfeitamente nestas normas. Porém, outros delitos eventualmente podem não se enquadrar nos tipos penais estabelecidos até então, surgindo a denominada atipicidade do ato, com a consequente impunidade do agente criminoso``[29].

[29] (TEIXEIRA, Tarcisio. Direito Digital e Processo Eletrônico. 5ª edição. São Paulo, SP: Editora Saraiva, 2020. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555591484/. Acesso em: 28 ago. 2022.

No entanto, é importante ressaltar que aplicar a lei para enfrentar adequadamente o problema do cibercrime não é uma tarefa fácil. Porque os cibercriminosos são constantemente atualizados e aprimorados e, portanto, a lei pode ficar desatualizada. Além de desenvolver padrões sobre como lidar adequadamente com o cibercrime, isso também é suficiente para outros aspectos importantes do combate ao cibercrime, como investigações policiais, métodos para identificar criminosos na rede e promover projetos e programas. Fazer. Um dos objetivos é conscientizar os internautas[30].

Problemas júridicos Pinheiro:

> ´´O maior problema jurídico dos crimes virtuais ainda é o fato de que os criminosos estão sempre um passo à frente. Há necessidade de investir mais no preparo da polícia para que tenham mais ferramentas para realizar perícia forense, bem como também em campanhas educativas da população, para que o cidadão saiba se defender melhor dos novos tipos de golpes e ameaças digitais``[31].

Portanto, é importante que a lei não apenas puna os criminosos hipotéticos, mas também garanta que os danos às vítimas sejam minimizados e o crime seja evitado. Ao mesmo tempo, os ambientes virtuais são menos seguros para os usuários, que devem buscar alternativas para combater esse crime.

Conforme mencionado anteriormente, o phishing é um crime de computador que envolve a obtenção ilegal de informações confidenciais de usuários da Internet. A frase vem da palavra inglês fishing, que significa pescar em português. Os cibercriminosos operam de várias maneiras, mas uma delas é o uso ilegal de suposições e processos enganosos para induzir os usuários da Internet a fornecer dados a grupos ou indivíduos mal-intencionados. Os meios mais comuns utilizados neste tipo de golpe são as comunicações oficiais óbvias, principalmente por e-mail, e os golpes de phishing que vazam informações sigilosas ou confidenciais aos usuários pela Internet sem que a vítima perceba o perigo, são vítimas de fraude eletrônica por

---

[30] SECURITY REPORT. Brasil é como um pássaro na mina para o cibercrime. Disponível em: https://www.securityreport.com.br/destaques/brasil-e-como-um-passaro-na-mina-para-o- cibercrime/. Acesso em: 30 ago. 2022.

[31] PINHEIRO, Patrícia P. Direito Digital. 7ª edição. São Paulo, SP: Editora Saraiva, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 30 ago. 2022.

curiosidade, caridade ou problemas financeiros. Outro ataque

menos conhecido que ainda ocorre são os ataques a sistemas de SMS, conhecidos como smishing ou realizados por telefone, que ocorrem após o batismo[32].

Os ataques não se limitam aos PCs dos usuários domésticos, pois foi relatada outra forma de phishing conhecida como "pharming", que envolve "contaminar" os servidores do Sistema de Nomes de Domínio (DNS) para associar as configurações ao endereço da web. Mesmo que o endereço correto seja inserido, ele pode ser modificado para redirecionar os internautas a sites falsos[33].

O mesmo é verdade na presença ou ausência de mensagens de spam e phishing, pois a natureza da arquitetura da Internet e a globalização permitem que os criminosos alcancem mais vítimas em potencial[34]. Sem um conhecimento claro do que está por trás do IP do proprietário ou usuário do e- mail, é difícil determinar quem é afetado.

Como tal, as técnicas de phishing não identificam a vítima com antecedência, e os crimes por e-mail normalmente enviam as seguintes mensagens indiscriminadamente, mesmo que o conteúdo seja privado. Mas quando esses truques foram descobertos, os golpistas usaram técnicas de programação e outros tipos de ameaças para enganar mais internautas e legitimar todo o processo.

Uma das estratégias utilizadas é comprometida por códigos maliciosos como worms, bots, vírus e cavalos de Tróia[35]**.** e criminosos que utilizam os sistemas afetados para enviar mensagens ou acessar suas listas de contatos pessoais.

Independente da técnica utilizada, a verdade é que a intenção do atacante no phishing é sempre maliciosa[36]. Com acrescente ameaça de extorsão ilegal de dados, muitos países se protegem diretamente contra fraudes on-line adotando regulamentos rígidos contra esse tipo deataque.

De acordo com um relatório da Kaspersky Lab, o Brasil se tornou o principal

---

[32] DIEZ, Almudena Congil. Phishing. Problemática relativa a la calificación jurídica de laparticipación de los denominados “mulerosbancarios”. Estado actual de nuestra doctrina y jurisprudência. 2013, Disponivel em: http://www.elderecho.com/penal/PhisingProblematica-calificacion-participacion-jurisprudencia_11_533680004.html*f*. Acesso em: 24 jan 2023.

[33] CGI.BR. Cartilha de Segurança para Internet. Comitê Gestor da Internet no Brasil, 2012. Disponível em: http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 28 ago. 2022.

[34] EETEN, Michel J. G., BAUER, Johannes M Economics of Malware: Security Decisions, Incentives and Externalities, (2008).Report for the Organization of Co-operation and Development (OECD). Disponível em: http://www.oecd.org/internet/ieconomy/40722462.pdf. Acesso em: 18 dez. 2022.

[35] CERT.br. Índices reportados ao CERT.br. Juho a Setembro de 2013. Disponível em: http://www.cert.br/stats/incidentes/2006-jan-dec/tipos-ataque-acumulado.html. Acesso em 18 dez 2022.

[36] MOORE, Tyler.; CLAYTON, Richard .; ANDERSON, Ross. The Economics of online crime. Journal of Economic Perspectives, v. 23, n. 3, p. 3-20, nov./dec. (2009)

alvo de phishing do mundo em 2020. No ano passado, o país liderou as cinco regiões com os maiores índices de violações de dados, à frente de Portugal, França, Tunísia e Guiana Francesa. Nesse tipo de golpe, os golpistas usam anúncios falsos e links da Web maliciosos para roubar informações confidenciais das vítimas. Segundo a

pesquisa, quase 20% dos brasileiros tentam abrir um link de phishing pelo menos uma vez por ano[37].

A Kaspersky estima que o número de ataques aumentou durante o primeiro surto em fevereiro e março de 2020. Somente naquele mês, o número de tentativas de ataque aumentou mais de 120%. Os principais impulsionadores são o aumento do uso da Internet, maior capacidade de fazer compras e transações bancárias on-line e preocupações com as notícias do coronavírus que causam a doença do novo coronavírus (Covid-19).

Esta alegação é baseada em uma tentativa de acesso a páginas de phishing ou links falsos em e-mails, mas cujo acesso foi bloqueado pelo software antivírus da empresa. No geral, o software bloqueia mais de 434 milhões de visitas a sites de phishing em todo o mundo. Destes, cerca de 87 milhões são brasileiros. Confira nossa lista dos 10 principais países afetados por golpes online em 2020.

Países que mais acessaram phishing em 2020

País	Porcentagem de usuários atacados por país
Brasil	19,94%
Portugal	19,73%
França	17,90%
Tunísia	17,62%
Guiana Francesa	17,60%
Catar	17,35%
Camarões	17,32%
Venezuela	16,84%
Nepal	16,72%
Austrália	16,59%

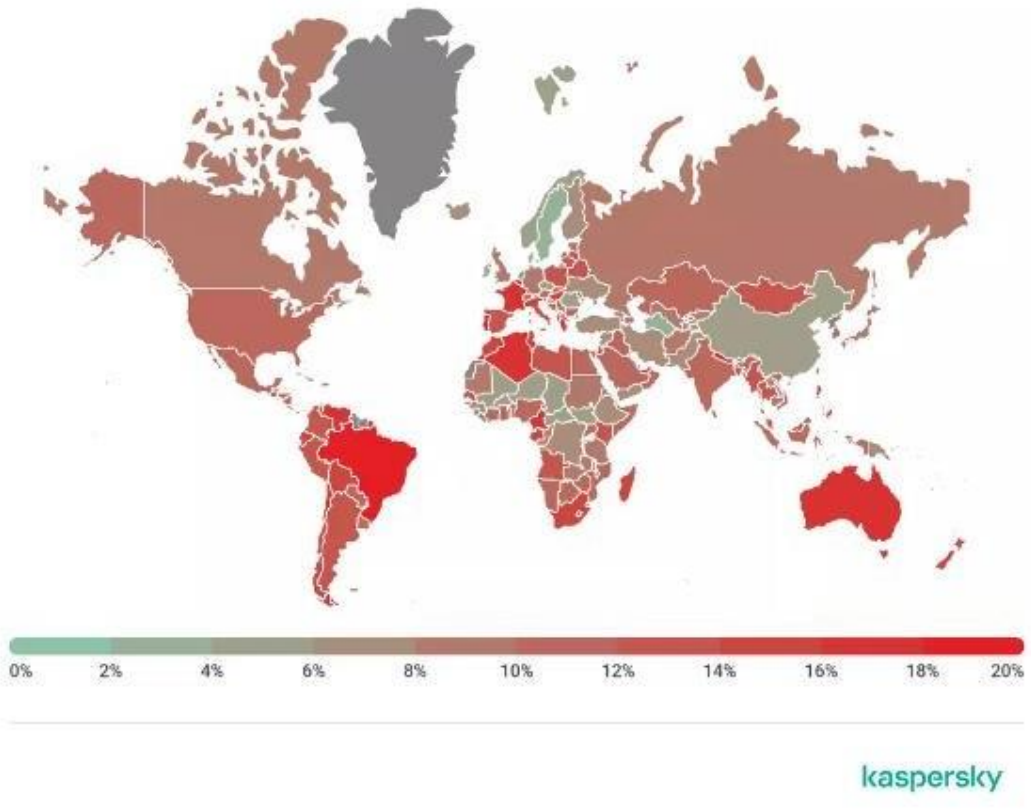
Fonte: Kaspersky

[37] TechTudo. Brasil é líder mundial em golpes de phishing: saiba se proteger. Disponível em: https://www.techtudo.com.br/noticias/2021/03/brasil-e-lider-mundial-em-golpes-de-phishing-saiba-se-proteger.ghtml. Acesso em: 29 ago. 2022.

O levantamento revela que o Brasil está acima da média global de phishing, que é de 13%. De acordo com Fábio Assolini, analista de segurança da Kaspersky, a diferença pode ser explicada pela dificuldade dos brasileiros em diferenciar golpes de mensagens verdadeiras na Internet[38].

Segundo Fábio Assolini:

> ´´Nossa recente pesquisa mostrou que cerca de 30% dos brasileiros não sabem reconhecer uma mensagem de correio eletrônico falsa. Isso nos torna vulneráveis e propensos a cair em "promoções imperdíveis" e outros golpes online´´[39].



Brasil é líder em tentativas de phishing no mundo em 2020 — Foto: Divulgação/Kaspersky

[38] TechTudo. Brasil é líder mundial em golpes de phishing: saiba se proteger. Disponível em: https://www.techtudo.com.br/noticias/2021/03/brasil-e-lider-mundial-em-golpes-de-phishing-saiba- se-proteger.ghtml. Acesso em: 29 ago. 2022.

[39] https://www.techtudo.com.br/noticias/2021/03/brasil-e-lider-mundial-em-golpes-de-phishing-saiba-se-proteger.ghtml

5 CONCLUSÃO

Nas últimas décadas, o desenvolvimento da tecnologia mudou significativamente o cotidiano das pessoas, principalmente as interações sociais. Em geral, a tecnologia tornou-se uma parte importante da vida da maioria das pessoas na sociedade como uma ferramenta para armazenar dados, apoiar procedimentos, monitorar a saúde, gerenciar finanças e criar condições de comunicação. Multifuncional.

Com isso, tarefas e atividades que muitas vezes demandam procedimentos administrativos e relações humanas são realizadas de forma digital, refletindo a importância dos meios tecnológicos.

Dada a importância do combate ao phishing, objeto deste estudo, e o potencial do phishing causar perdas econômicas significativas a pessoas físicas e jurídicas, a legislação brasileira tem possibilitado proteger a sociedade do uso da Internet e de outras tecnologias. Adaptar-se à velocidade de tal atividade criminosa para proteção da sociedade.

Pelas razões expostas, dadas as características particulares que o phishing apresenta, é possível identificar que a prática demanda uma tipificação penal própria, de modo que o crime possa ser efetivamente punido ou até impedido de acordo com as suas nuances.

Aprimoramento das leis existentes. Embora a falta de uma tipificação penal específica para o phishing possa ser um desafio, é possível trabalhar no aprimoramento das leis existentes relacionadas a crimes cibernéticos, como estelionato, furto, fraude eletrônica, entre outros. Isso pode ajudar a garantir que os perpetradores de phishing sejam processados e punidos.

Fortalecimento das instalações de investigação. É fundamental fortalecer as capacidades das instituições responsáveis pela investigação e repressão dos crimes cibernéticos. Isso envolve treinar e equipar as forças policiais e promover a colaboração internacional para rastrear e prender os responsáveis pelos ataques de phishing

Proteção e segurança online. Investir em tecnologias de segurança cibernética é crucial para combater o phishing. As instituições financeiras, empresas e provedores de serviços de internet devem implementar medidas de segurança, como

autenticação de dois fatores, criptografia de dados e sistemas de detecção de phishing.

Aí ainda acrescenta acordo internacional. Cooperação internacional o phishing é um problema global, e a cooperação internacional é essencial para enfrentá-lo. O Brasil deve trabalhar em parceria com outros países para compartilhar informações, trocar boas práticas e colaborar em reflexões transnacionais.

Embora a falta de tipificação penal específica para o phishing no Brasil possa representar um desafio, uma abordagem holística que envolve educação, cooperação entre setores, aprimoramento das leis existentes, fortalecimento das capacidades de investigação, proteção online e cooperação internacional pode contribuir para mitigar esse problema e proteja os usuários contra ataques de phishing.

Portanto cabe um acréscimo de uma línea que preveja, seja única e específica sobre o crime de phishing, incluindo no decreto Lei n° 2.848 de 07 de dezembro de 1940. Criar um novo artigo acrescentando a tal, suas especificações e sanções penais que versa sobre a tipificação da prática do phishing trazendo seus agravantes e atenuantes para melhor sanção e aplicação da Lei. Tendo como prevenir diversidades e entendimentos diferentes.

6 REFERÊNCIAS

BACIGALUPO, Henrique. Direito Penal - Parte Geral. São Paulo: Malheiros, 2005, p. 109.

BARRETO, Jeanine dos S.; ZANIN, Aline; MORAIS, Izabelly Soares D.; VETTORAZZO, Adriana de S. Fundamentos de segurança da informação. 1ª edição. Porto Alegre, RS: Grupo A, 2018. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595025875/. Acesso em: 30 ago. 2022.

BARROS, Antônio. Câmara dos deputados. Evolução dos crimes. Disponível em: https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-dos-crimes-ciberneticos#:~:text=Os%20primeiros%20crimes%20relacionados%20%C3%A0,delitos%20como%20sa. Acesso em: 28 ago. 2022.

BRASIL. Decreto-Lei nº 2.848, de 07 de dezembro de 1940. Código Penal. Rio de Janeiro – RJ, 07 de dezembro de 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decretolei/del2848compilado.htm. Acesso em: 29 ago. 2022.

BRASIL. Lei nº 1.521, de 26 de dezembro de 1951. Altera dispositivos da legislação vigente sobre crimes contra a economia popular. Rio de Janeiro – RJ, 26 de dezembro de 1951. Disponível em https://www.planalto.gov.br/ccivil_03/leis/l1521.htm. Acesso em: 29 ago. 2022.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Brasília, 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 29 ago. 2022.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 ago. 2022

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato.

Brasília, 27 de maio de 2021 Disponível em:

http://www.planalto.gov.br/ccivil_03/_Ato20192022/2021/Lei/L14155.htm#art1.
Acesso em:30 ago. 2022.
CERQUEIRA, Daniel. LOBÃO, Waldir. Determinantes da criminalidade: uma resenha dos modelos teóricos e resultados empíricos. IPEA - exto para discussão nº 956. Rio de janeiro, jun. 2003. Disponível em: http://www.ipea.gov.br/portal/images/stories/PDFs/TDs/td_0956.pdf. Acesso em: 30 ago. 2022
CERT.br. Índices reportados ao CERT.br. Julho a setembro de 2013. Disponível em: http://www.cert.br/stats/incidentes/2006-jan-dec/tipos-ataque-acumulado.html.
Acesso em 18 dez 2022.
CGI.BR. Cartilha de Segurança para Internet. Comitê Gestor da Internet no Brasil, 2012. Disponível em: http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 28 ago. 2022.
Conteúdo Jurídico. Aumento de crimes cibernéticos durante a pandemia do COVID-19 no Brasil. Disponível em:
DIEZ, Almudena Congil. Phishing. Problemática relativa a la calificación jurídica de laparticipación de los denominados “mulerosbancarios”. Estado actual de nuestra doctrina y jurisprudência. 2013, Disponivel em: http://www.elderecho.com/penal/PhisingProblematica-calificacion-participacion-jurisprudencia_11_533680004.html$f$. Acesso em: 24 dez. 2023.
EETEN, Michel J. G., BAUER, Johannes M Economics of Malware: Security Decisions, Incentives and Externalities, (2008). Report for the Organization of Co-operation and Development (OECD). Disponível em: http://www.oecd.org/internet/ieconomy/40722462.pdf. Acesso em: 18 dez. 2022.
FERNANDES, Antonio Scarance. Considerações sobre o vídeo pôquer como atividade criminal. Justitia (São Paulo), v. 52, p. 84-92, 1990. Disponível em: http://www.justitia.com.br/revistas/x722dx.pdf. Acesso em 15 jan 2023.
FRASA NET. Internet de fibra óptica e para eventos. Acesso em: 14 jan. 2023. Disponível em: https://frasanet.com.br/como-surgiu-a-internet/#:~:text=A%20internet%20surgiu%20em%201969,Unidos%20e%20a%20Uni%C3%A3o%20Sovi%C3%A9tica. Acesso em 30 ago.2022
GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. Revista de Direito Mackenzie, v. 1, p. 35-39, 2000.
HORN. Manuela Bittar. O duplo nível de legalidade e os crimes contra a economia

popular no direito penal autoritário. Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Programa de Pós-Graduação em Direito, Florianópolis, 2013.

http://portalrevistas.ucb.br/index.php/EALR/ article/viewArticle/ 1%20EALR%20318. Acesso em: 29.ago 2029.

http://www.conteudojuridico.com.br/consulta/artigos/58466/aumento-de-crimes-cibernticos-durante-a-pandemia-do-covid-19-no-brasil. Acesso em: 31 ago. 2022.

DESLANDES, F. M.; ARANTES, A. F. Crimes virtuais: uma análise acerca da eficácia da legislação e os desafios de sua persecução penal. In: Revista Jurídica Cesumar - Mestrado, v. 17, n. 2, p. 173-194, 2017.

https://www.jusbrasil.com.br/artigos/crimes-virtuais-uma-analise-acerca-da-in-eficacia-da-legislacao-e-os-desafios-de-sua-persecucao-penal/1220973039. Acesso em: 30 ago. 2022.

JESUS, Damásio de; MILAGRES, José Antônio. Manual de Crimes Informáticos. 1ª Edição. ed. São Paulo: Saraiva, 2016. 231 p. ISBN 978850262724-6. Disponível em: https://docero.com.br/doc/ecv5ns.

Jusbrasil. Competência nos crimes cibernéticos. Disponível em: https://www.jusbrasil.com.br/artigos/competencia-nos-crimes-ciberneticos/514359859. Acesso em: 30 ago. 2022.

Jusbrasil. Crimes cibernéticos. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. Acesso em: 30 ago. 2022.

Jusbrasil. Crimes virtuais: uma análise acerca da (in)eficácia da legislação e os desafios de sua persecução penal. Disponível em:

Kaspersky. What is Cybercrime? Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 30 ago. 2022.

MOORE, Tyler.; CLAYTON, Richard.; ANDERSON, Ross. The Economics of online crime. Journal of Economic Perspectives, v. 23, n. 3, p. 3-20, nov./dec. (2009)

MPF - Ministério Público Federal. MPF e Conselho da Europa promovem encontro internacional das redes de Ministérios Públicos sobre cibercriminalidade e provas digitais. Disponível em: https://www.mpf.mp.br/pgr/noticias-pgr2/2023/mpf-e-conselho-da-europa-promovem-encontro-internacional-das-redes-de-ministerios-publicos-sobre-cibercriminalidade-e-provas-digitais. Acesso em: 30 ago. 2022.

Oficina da Net. O Marco Civil da Internet foi aprovado - entenda o que é e o que muda na sua vida. Disponível em: https://www.oficinadanet.com.br/post/12558-o- marco-civil-da-internet-foi-aprovado-entenda-o-que-e-e-o-que-muda-na-sua-vida. Acesso em: 30 ago. 2022.

OLLMANN, Gunter. The phishing guide: understanding & preventing phishing attacks.2007, Disponível me: http://www-935.ibm.com/services/us/iss/pdf/phishing-guidewp.pdf. Acesso em: 30 ago 2022

OLLMANN, Gunter. The phishing guide: understanding & preventing phishing attacks.2007, Disponível me: http://www-935.ibm.com/services/us/iss/pdf/phishing-guidewp.pdf. Acesso em: 28 ago 2022.

Paz Mendes Advocacia. Crimes Cibernéticos no Brasil. Disponível em: https://www.pazmendes.com.br/crimes-ciberneticos-no-brasil/#:~:text=Crime%20virtual%2C%20cibercrime%2C%20crime%20eletr%C3%B4nico, nomes%20atribu%C3%ADdos%20aos%20crimes%20cibern%C3%A9ticos. Acesso em: 30 ago. 2022.

PINHEIRO, Patrícia P. Direito Digital. 7ª edição. São Paulo, SP: Editora Saraiva, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 23 out. 2022.

PINHEIRO, Patricia P. Segurança Digital - Proteção de Dados nas Empresas. 1ª edição. São Paulo, SP: Grupo GEN, 2020. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597026405/. Acesso em: 30. 2022.

Planalto. Lei nº 12.965/2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14 jan. 2023.

ROQUE, Sergio Marcos. Crimes virtuais. 2022. Disponível em: https://jus.com.br/artigos/72619/crimes-virtuais. Acesso em: 30 ago. 2022.

Security Report. Brasil é como um pássaro na mina para o cibercrime. Disponível em: https://www.securityreport.com.br/destaques/brasil-e-como-um-passaro-na- mina-para-o-cibercrime/. Acesso em: 30 ago. 2022.

SHIKIDA, Pery Francisco Assis. In: Economic Analysis of Law Review. Brasília, v 1 n 2 p. 424-jul-dez.2010. Disponível em:

TechTudo. "Brasil é líder mundial em golpes de phishing; saiba se proteger." Disponível em: https://www.techtudo.com.br/noticias/2021/03/brasil-e-lider-mundial-

em-golpes-de-phishing-saiba-se-proteger.ghtml. Acesso em 29 ago 2022.
TechTudo. Brasil é líder mundial em golpes de phishing: saiba se proteger. Disponível em: https://www.techtudo.com.br/noticias/2021/03/brasil-e-lider-mundial- em-golpes-de-phishing-saiba-se-proteger.ghtml. Acesso em: 29 ago. 2022.
TEIXEIRA, Tarcisio. Direito Digital e Processo Eletrônico. 5ª edição. São Paulo, SP: Editora Saraiva, 2020. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555591484/. Acesso em: 28 ago. 2022.
TJDFT - Tribunal de Justiça do Distrito Federal e dos Territórios. Marco Civil da Internet. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas- e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet. Acesso em: 30 ago. 2022.
VIAPIANA, Luiz Tadeu. Economia do Crime: Uma Explicação para a Formação do Criminoso, Porto Alegre: 2006, AGE Editor
Wikipedia. Ciberespaço. Disponível em: https://pt.wikipedia.org/wiki/Ciberespa%C3%A7o. Acesso em: 28 ago. 2022.
Wikipedia. Internet. Disponível em: https://pt.wikipedia.org/wiki/Internet. Acesso em: 28 ago. 2022.