CENTRO UNIVERSITÁRIO UNA

RICARDO TEIXEIRA NUNES MARQUES
THAMYRIS RODRIGUES DE MATTOS
THAYLA IZABELLE COSTA MARTIM

PHISHING: Técnicas, Impactos e Estratégias de Prevenção à Luz do Ordenamento Jurídico Brasileiro

Belo Horizonte
2023

RICARDO TEIXEIRA NUNES MARQUES
THAMYRIS RODRIGUES DE MATTOS
THAYLA IZABELLE COSTA MARTIM

PHISHING: Técnicas, Impactos e Estratégias de Prevenção à Luz do Ordenamento Jurídico Brasileiro

Trabalho de Conclusão de Curso apresentado ao curso de Direito, do Centro Universitário UNA, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Orientador: Daniela Mateus de Vasconcelos

Belo Horizonte
2023

RESUMO

Este estudo aborda o fenômeno do *phishing*, seus impactos no Brasil e as estratégias de prevenção no contexto jurídico nacional. Os impactos do *phishing* são significativos, incluindo prejuízos financeiros substanciais, roubo de dados confidenciais, danos à reputação de empresas e instituições, bem como casos notórios de ataques cibernéticos. Além disso, o *phishing* também pode ser utilizado para a disseminação de conteúdo enganoso e ataques subsequentes. Em relação ao ordenamento jurídico brasileiro, ainda há muito o que progredir no campo do Direito Digital para dar guarida às vítimas desse tipo de golpe. Nesse contexto, os Poderes Legislativo e Judiciário desempenham um papel fundamental na regulamentação e fiscalização de atividades relacionadas à segurança cibernética, acompanhando os avanços tecnológicos na sociedade. A prevenção e o combate a esses ataques requerem uma abordagem multifacetada, que inclui educação, conscientização e regulamentação.

Palavras-chave: Ataques cibernéticos. Direito Digital. Ordenamento jurídico brasileiro. Phishing. Segurança cibernética.

ABSTRACT

This study addresses the characteristics of phishing, its impacts in Brazil and prevention strategies in the country's legal context. The impacts of phishing are significant. This includes substantial financial losses, data theft caused, damage to companies and institutions, as well as notary cases of cyber attacks. Additionally, phishing can also be used to spread misleading content and subsequent attacks. In relation to the Brazilian legal system, there is still a lot of progress in the field of Digital Law to provide guarantees to victims of this type of scam. In this context, the Legislative Branch and the Judiciary play a fundamental role in regulating and supervising activities related to cybersecurity, following technological advances in society. Preventing and fighting these attacks requires a multi-pronged approach that includes education, awareness and guidance.

Keywords: Cyberattacks. Digital Law. Brazilian legal system. Phishing. Cybersecurity.

LISTA DE ABREVIATURAS E SIGLAS

ASP.NET	Páginas ativas do servidor (do inglês Active serves pages)
CERT.br	Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil
PHP	Pré-processador de hipertexto (do inglês Hypertext preprocessor)
SQL	Linguagem de consulta estruturada (do inglês Structured query language)

SUMÁRIO

1 **INTRODUÇÃO**

Nos últimos anos, o avanço das tecnologias digitais transformou profundamente a maneira como indivíduos, empresas e instituições interagem e conduzem suas operações no mundo virtual. A evolução das tecnologias veio acompanhada de problemas de ordem delituosa que ainda não são tipificados no ordenamento jurídico pátrio, como fraudes cibernéticas de diversas naturezas, mais especificamente, o *phishing*.

O *phishing* é considerado como um tipo de golpe que figura no Brasil como um dos mais recorrentes, desde a virada do século, com a popularização no uso da Internet. Esse tipo de crime que antes só acontecia de modo presencial, começou a ocorrer nos meios digitais, com o uso de artifícios cada vez mais ardilosos. Por ser considerado um crime análogo ao estelionato, sendo acrescentado a sua tipificação ao Código Penal em 2021, vislumbra-se a necessidade de se entender mais sobre o tema, uma vez que afeta uma quantidade expressiva de pessoas, anualmente.

Este artigo tem como objetivo principal explorar o fenômeno do *phishing*, dentro da classificação de crime cibernético e do conceito de engenharia social, além de demonstrar sua relevância à sociedade e ao meio jurídico-acadêmico. Também tem por objetivo este trabalho, fomentar maior discussão sobre o tema, para que a sociedade como um todo se beneficie, ao conhecer mais sobre os riscos dessa ameaça e como proceder caso venha a se tornar uma vítima de *phishing*.

Quanto à estrutura geral do artigo, dividiu-se os tópicos em conceituação, técnicas utilizadas, impactos no Brasil, aspectos legais e estratégias de prevenção. A metodologia utilizada é a qualitativa de base documental e bibliográfica, com pesquisa em livros, artigos e websites, na qual observa-se a literatura já disponível sobre o assunto, descreve-se o tema e seus pontos importantes e se expõe as visões relevantes para ampliar o entendimento sobre o assunto.

Sendo assim, até que ponto a ampliação da proteção às vítimas de golpes cibernéticos através de leis é o suficiente para reduzir a ocorrência de *phishing* no Brasil?

2 **PHISHING: CONCEITO E TÉCNICAS**

2.1 DEFINIÇÃO DE PHISHING

O *phishing* representa uma ameaça cibernética difundida e altamente eficaz, fundamentada na engenhosidade e manipulação psicológica para ludibriar as vítimas e obter informações confidenciais. Esse método, amplamente utilizado por cibercriminosos, tem causado impactos significativos globalmente e é definido da seguinte forma

> Inicialmente os termos *phishing*, *phishing* scam ou mesmo só *scam* são utilizados indistintamente. Derivam do vocábulo bretão “to fish” ou “fishing”, que significa pescar. Podemos dizer que se trata de verdadeira engenharia social que tem como finalidade obter informações relevantes, na modalidade fraude virtual para a obtenção de dados valiosos dos particulares (CRESPO, 2011, p.25).

Complementarmente, Bomfati (2020) apresenta outra definição para o *phishing* :

> *Phishing* é uma maneira desonesta que cibercriminosos usam para enganar você a revelar [sic] informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem enviando e-mails falsos ou direcionando você a websites falsos (BOMFATI,2020, p.124).

Em virtude disso, é essencial a compreensão aprofundada do conceito e das técnicas subjacentes ao *phishing*, como o uso da engenharia social: "Entende-se como engenharia social todo método de mascarar a realidade para explorar ou enganar a confiança de uma pessoa detentora de dados importantes a que se quer ter acesso" (CRESPO, 2011, p.25). Relacionando estes conceitos, Ribeiro (2020) classifica o *phishing* como um ataque cuja base é a engenharia social, no qual o *hacker* engana o usuário com o objetivo de obter dados que julga necessários para praticar sua ação.

Em outra passagem, Crespo (2011) cita algumas técnicas de *phishing* que são comumente usadas atualmente

> O *phishing* funciona da seguinte forma: uma pessoa mal-intencionada envia uma mensagem eletrônica (pode ser um e-mail, um recado em uma página de relacionamentos etc.) a outrem e, utilizando-se de pretextos falsos, tenta enganar a pessoa receptora da mensagem e induzi-la a fornecer informações como número do cartão de crédito, senhas, dados de contas bancárias, ou, ainda, instiga a baixar e

> executar arquivos que permitam a futura subtração ou roubo de informações ou o acesso não autorizado ao sistema da vítima. (CRESPO, 2011, p.25).

A autora Ribeiro (2020), classifica o *phishing* na categoria de ataques do tipo *exploit*[1]

> Existem duas formas pelas quais os indivíduos podem se utilizar para dar início à execução de *exploits.* Um deles é visitando um site que não oferece segurança, com um código não confiável. E o outro método é abrir um arquivo que a princípio parece ser seguro por com um código malicioso. Os métodos mais usados para propagar os *exploits* é por meio de correios eletrônicos de *phishing* [...]. (RIBEIRO, 2020, p.12).

Por outro lado, Ferreira (2021) classifica o *phishing* como um tipo de *ransomware*. Juntamente com spam, vulnerabilidades e páginas web corrompidas, o phishing figura nessa classificação, que segundo este autor se define como

> O *ransomware* é uma forma de ataque do tipo extorsão, causando limitação de acesso ao usuário. Possui crescimento acentuado e atinge vários países no mundo. Pode infectar diferentes tipos de dispositivos, como computadores, tablets, celulares, roteadores e até *switches*. (FERREIRA, 2021, p.48).

Por fim, o *phishing* é uma ameaça cibernética que se baseia na engenhosidade e na manipulação psicológica para obter informações confidenciais. É essencial que indivíduos e organizações compreendam as técnicas por trás desse tipo de ataque, bem como implementem medidas de segurança eficazes para se proteger contra ele.

2.2 PRINCIPAIS TÉCNICAS DE ATAQUE

Existem várias técnicas de *phishing* utilizadas por cibercriminosos. Uma das abordagens mais comuns é o "phishing por e-mail", no qual os criminosos enviam e-mails falsos que se assemelham a comunicações legítimas de bancos, empresas ou sites de mídia social. Outra técnica é o *Spear Phishing*, que segundo Silva (2023), busca alvos humanos ao enviar mensagens contendo um link malicioso de uma oferta imperdível, por exemplo. Este autor continua

[1]Programa feito com a finalidade de explorar a incapacidade de defesa de um programa de computador

"Depois de o código ser baixado e executado no dispositivo alvo, o atacante tem total acesso a ele pode agir" (SILVA, 2023, p.68).

A autora Ribeiro (2020) cita alguns exemplos de *phishing*

> Exemplos de situações envolvendo *phishing* são: páginas falsas de comércio eletrônico ou internet banking; páginas falsas de redes sociais ou de companhias aéreas; mensagens contendo formulários golpistas; mensagens contendo links para códigos maliciosos; e solicitação de cadastramento (RIBEIRO, 2020, p.15;16).

Outro recurso que os cibercriminosos utilizam atualmente, segundo Crespo (2011)

> Os criminosos aproveitam-se do recurso de VoIP, uma tecnologia que permite a comunicação por voz pela internet (protocolo IP). Essa novidade torna possível fazer ligações telefônicas entre computadores ligados à rede ou entre computadores conectados entre si e telefones fixos e/ou celulares a custos baixos. Este nada mais é que um phishing baseado na telefonia VoIP (“voice over Internet Protocol”, ou voz sobre IP, isto é, aquela tecnologia em que a voz trafega pelo cabo da internet, não havendo cobrança de pulsos telefônicos). (CRESPO, 2011, p.25).

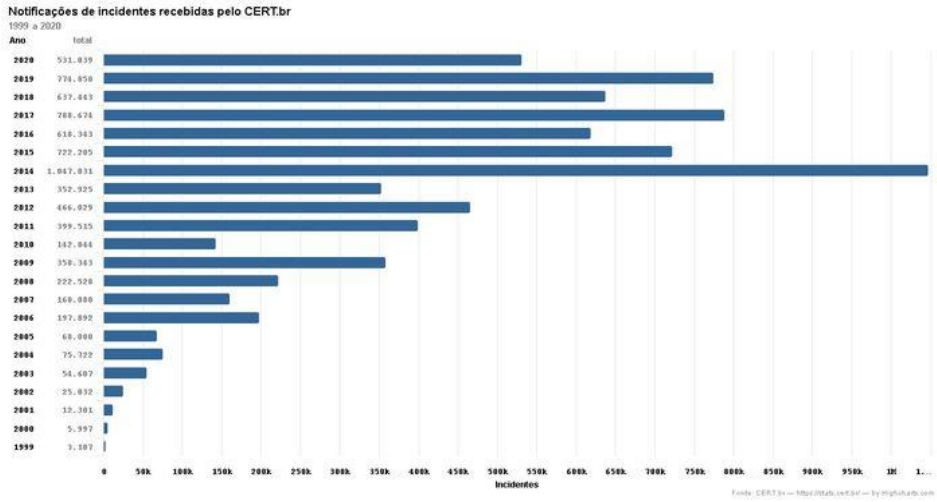
3 **IMPACTOS DO PHISHING NO BRASIL**

O *phishing*, uma das ameaças cibernéticas mais onipresentes, não poupa o Brasil de seus impactos prejudiciais. Essa prática fraudulenta envolve a falsificação de identidades e a manipulação de informações, a fim de enganar os usuários da internet e obter acesso a dados sensíveis. Os efeitos do *phishing* no Brasil são significativos, afetando tanto indivíduos quanto organizações, e agravando-se com o tempo.

Segundo Pinheiro (2021), apesar de ser conhecido desde os anos 90, ainda figura como a maior fonte de ataques e fraudes cibernéticas. No Brasil, o CERT.br[2] é o Grupo de Resposta a Incidentes de Segurança para a Internet, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil, segundo Silva (2023). No site CERT.br estão contidos gráficos com estatísticas de incidentes relatados sobre segurança na internet no Brasil, separado por ano, conforme a figura que segue:

[2]Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil

Gráfico 1 — Cibersegurança: uma visão panorâmica sobre a segurança da informação na internet

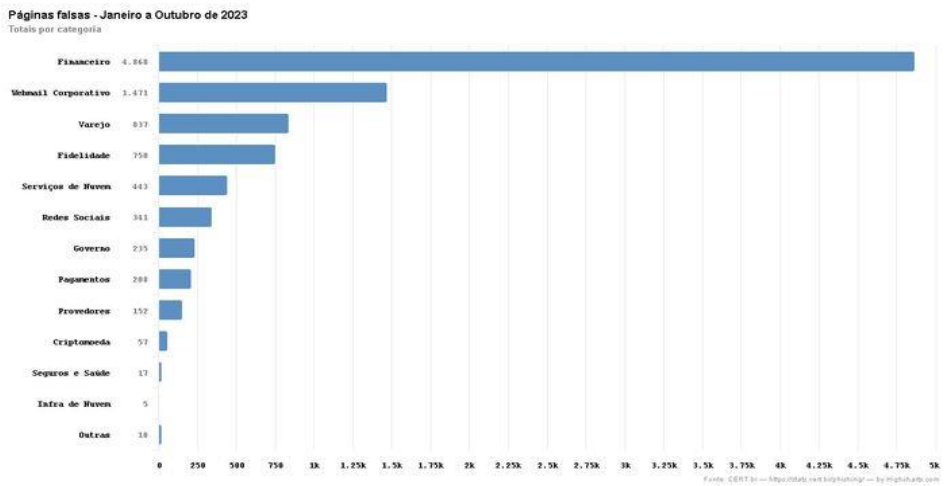


Fonte: Cert.br (2020)

Através das informações contidas no gráfico pode-se observar que o número de incidentes reportados no Brasil a partir de 2006 teve um aumento substancial, atingindo o seu pico em 2014 e após este ano manteve uma média de casos próximo a 600.000 (seiscentos mil) casos anuais.

No que diz respeito apenas aos casos reportados de *phishing* ocorridos no Brasil, envolvendo organizações nacionais e também de outros países, o site Cert.br disponibiliza um gráfico do período entre janeiro e outubro de 2023:

Gráfico 2 — Total de *phishing* por categoria



Fonte: Cert.br (2023)

Conforme o gráfico acima, os setores que possuem maior número de casos reportados são: financeiro, webmail corporativo e varejo. O setor

financeiro se destaca dentre esses três setores, com pelo menos três vezes o número de casos reportados pelo segundo colocado, totalizando 4868 (quatro mil oitocentos e sessenta e oito) casos somente no ano de 2023.

De forma comparativa, Silva (2023) expõe dados de organizações internacionais relativo ao número estimado de casos de *phishing* ocorridos globalmente. O Grupo de Trabalho Anti-Phishing (APWG) registrou 1,2 milhão de ataques desse tipo em 2016. O FBI estimou o número de 4000 (quatro mil) ataques diários em 2016, ultrapassando a cifra anual registrada pelo APWG. A *Privacy Rights Clearing House* estima que houve aproximadamente 2,8 bilhões de registros perdidos como resultado da violação de dados no mesmo ano, devido à ação de hackers.

Para combater eficazmente o *phishing* no Brasil, é essencial uma abordagem multifacetada. A educação cibernética, a conscientização pública e a capacitação de profissionais em segurança da informação são medidas críticas. Além disso, a cooperação entre o governo, setor privado e a sociedade civil é fundamental para estabelecer políticas e regulamentações sólidas.

3.1 PREJUÍZOS RESULTANTES DE CRIMES CIBERNÉTICOS

Os tipos de prejuízos decorrentes de crimes cibernéticos, podem ser divididos em financeiro, danos a reputação e roubo de dados pessoais. Segundo a Pesquisa Global de Fraudes e Crimes Econômicos[3] publicada em artigo na PwC[4] que ouviu mais de 7200 entrevistados em 123 países, no biênio 2016-2018, "[...] 7% dos brasileiros relataram prejuízos acima de US$ 50 milhões. Já para 66% no Brasil [...] essas perdas foram de até US$ 1 milhão nos últimos dois anos." Na sequência do artigo, a pesquisa informa que "Considerando os custos secundários, como investigações e intervenções, 31% das empresas brasileiras [...] afirmam ter gasto até duas vezes mais do que perderam com o crime." Dentre esses crimes, a pesquisa apurou que "De 2016 para 2018, 22% dos participantes brasileiros [...] foram afetados por ataques cibernéticos via *malware*[5] ou *phishing*."

[3]Do inglês, Global Economic Crime and Fraud Survey
[4]PricewaterhouseCoopers Brasil Ltda
[5]Do inglês, malicious software (software malicioso)

No tocante a prejuízos bancários pode-se observar que

> Os prejuízos decorrentes dos crimes cibernéticos são de grandes proporções. Segundo a Federação Brasileira de Bancos (Febraban), apesar do investimento na prevenção e no combate a essa modalidade de delito, somente no ano de 2010 eles provocaram prejuízos de novecentos milhões de reais para as instituições bancárias (BRAUN apud WENDT; JORGE, 2021, p.14).

Da mesma forma, ocorrem os crimes com foco em obter dados pessoais[6]como forma de conseguir vantagens financeiras ou para uso de identidade alheia, que podem causar danos à reputação, como corrobora o indicador da Serasa Experian, serviço de Cadastro Positivo no Brasil, referente ao ano de 2022.

> Segundo indicador da Serasa Experian, de janeiro a setembro deste ano foram registradas 3.046.294 tentativas de fraudes de identidade contra o consumidor no Brasil, representando uma tentativa a cada 8 segundos. As tentativas de fraudes relacionadas com o segmento de Bancos e Cartões lidera com 1,7 milhão. Em segundo lugar, estão as Financeiras, com 528 mil tentativas, seguido pelo setor de serviços, com 457 mil. Varejo aparece em quarto lugar, com 254 mil pessoas que foram alvo e Telefonia em último lugar, com 79 mil (SERASA EXPERIAN, 2022).

Um exemplo corriqueiro de dano à reputação de uma empresa, envolve a criação de sites falsos, modificando apenas algum caractere no nome do domínio[7], o que faz com que usuários venham a entrar nesse site e realizar compras, acreditando ser a empresa autêntica. Nesse caso, prossegue Pinheiro (2020),

> [...] geralmente, são usados links patrocinados em buscadores ou anúncios em sites de grande audiência [...] também é importante frisar que, apesar de a empresa original não ser vítima dessas atividades, ela pode ter sua reputação manchada pela justa insatisfação dos consumidores (PINHEIRO, 2020, p.27).

Esse dano à reputação pode ter consequências nefastas para uma empresa como: destruição do valor da marca, impacto em negócios em andamento ou em fase de fechamento, destruição do valor e desgaste de imagem da empresa (PINHEIRO, 2020, p.79-80).

---

[6] Lei 13.709/18 - Art. 5º, I " dado pessoal: informação relacionada a pessoa natural identificada ou identificável;"

[7] Cada site possui um único nome de domínio e seu respectivo endereço.

4 **ASPECTOS LEGAIS DO PHISHING NO BRASIL**

Inicialmente, pode-se destacar como referência mundial nesse assunto a Convenção sobre o Crime Cibernético, de Budapeste, feita em 23 de novembro de 2001. Porém, o Brasil somente ratificou a Convenção no dia 30 de novembro de 2022 e com esse espaço de tempo desde a sua criação, a legislação nacional avançou de forma vagarosa rumo a uma maior coibição de crimes no meio digital. Já em abril de 2014, foi aprovada a Lei do Marco Civil da Internet (Lei 12.965/2014), que deu as diretrizes aos assuntos diversos relacionados à internet, bem como "estabeleceu princípios, garantias, direitos e deveres para o uso da rede no país" (BLUM, 2015).

A Lei nº 12.737/12, também conhecida como Lei Carolina Dieckmann, representou um marco significativo no cenário jurídico-penal brasileiro, especialmente no contexto do Direito Digital. Seu surgimento teve suas bases no PL nº 84/99 e foi impulsionado por um incidente emblemático envolvendo a atriz Carolina Dieckmann, que teve suas fotos íntimas vazadas na internet após um ataque cibernético. Ao analisar essa legislação à luz do Direito Digital, percebe-se sua relevância na proteção da privacidade, combate aos crimes cibernéticos e estabelecimento de parâmetros legais para situações emergentes na era digital.

A referida lei tipifica diversos delitos relacionados à invasão de dispositivos informáticos, interceptação não autorizada de comunicações e divulgação não consensual de materiais íntimos, que podem ser feitos com técnicas de *phishing*. Essa abordagem reflete a busca em coibir práticas prejudiciais e resguardar direitos fundamentais, ainda que tenha sido um pequeno passo, segundo o autor brasileiro Renato Opice Blum, especialista em Direito Digital e proteção de dados, quando entrevistado por Eduardo Reina, da revista eletrônica Conjur em 2022.

> A lei conhecida como Carolina Dieckmann acrescentou no código penal o artigo 154 A e 154 B e um parágrafo no artigo 266, aquele que interrompe o serviço de utilidade pública. Mas as penas eram muito baixas. Nós tivemos recentemente uma atualização legislativa, com aumento de pena. A nova lei, a 14.155, atualizou os artigos 154 A e a 154 B. Agora temos uma lei efetiva. Antes, ou as penas eram muito pequenas ou o crime prescrevia ou, quando se provava (o crime), o sujeito fazia um acordo e prestava serviços para a comunidade. (BLUM *apud* REINA, 2022).

No artigo supracitado, Blum alega que a Lei nº 14.155/2021, que alterou o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) foi uma progressão importante para coibir a impunidade de uma série de crimes digitais, como pode-se extrair de sua literalidade no Código Penal vigente:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
> § 4º Na hipótese do §3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.

Segundo esse especialista, a ratificação da Convenção de Budapeste representa mais um avanço na legislação pátria, pois cria uma colaboração mútua investigativa e obriga o país a melhorar suas leis:

> Opice Blum informa que o Brasil acabou de validar, com a assinatura da Convenção de Budapeste junto a 54 países, o protocolo 24/7 de colaboração e transferência do sistema jurídico dos países signatários. A Convenção de Budapeste é do Conselho da Europa e trata-se de um arcabouço que ajuda no combate aos crimes cibernéticos (REINA, 2022).

Nesse sentido, deve-se esperar que mais avanços ocorram no tocante às legislações brasileiras que versam sobre crimes cibernéticos, muito embora, no mesmo artigo da Conjur, o conselheiro federal da OAB, Rafael Braude Canterji se posiciona da seguinte forma

> Não podemos incidir no erro de atribuir ao Direito Penal a responsabilidade de resolução ou prevenção de conflitos sociais e condutas desviadas dos comportamentos desejados. Ainda para aqueles que entendam que o propósito é este, sua prática resta dificultada pelos instrumentos tecnológicos da prática do crime. (CANTERJI apud REINA, 2022).

Especificamente, sobre o *phishing*, Crespo (2011) salienta que

> Tanto o *phishing* quanto o *vishing* são espécies claras de estelionato. Certamente a obtenção de senhas, numerais e códigos pessoais leva (ou intenta levar) à vantagem econômica por parte do agente ativo do

> crime que se utiliza da engenharia social e de artifícios tecnológicos ardilosos para induzir o usuário a erro. Uma vez com os dados obtidos, o agente pratica compras pela internet, faz saques, paga contas, cria documentos falsos, e assim por diante (CRESPO, 2011, p.25).

Esse autor pontua que o Substitutivo ao PL nº 84/99 (hoje é a Lei nº 12.737/2012), previa a criação do "estelionato eletrônico", acrescentando-se um §2º ao art. 171 do Código Penal "[...] prevendo que aquele que difundisse, por qualquer meio, código malicioso, com o intuito de facilitar ou permitir acesso indevido a sistema informático responderia nas mesmas penas do caput." (CRESPO, 2011, p.25). Segundo o autor:

> Essa modificação é pertinente porque tipifica o simples envio de e-mails (mensagens em geral, entre outros meios que possam veicular fraudes) que buscam atingir vítimas que forneçam seus dados pessoais a pessoas mal-intencionadas. Assim, caso haja o fornecimento de dados pessoais e a consequente obtenção de vantagem indevida, ter-se-ia configurado o estelionato (art. 171 do CP e Súmula 17 do STJ). (CRESPO, 2011, p.25).

Crespo (2011) conclui esse raciocínio da seguinte forma:

> Em suma, deve-se atentar para a criação de parágrafo dentro do art. 171 com redação que crie verdadeira conduta equiparada ao estelionato (“Nas mesmas penas incorre quem difunde comando, instrução ou programa, com o intuito de facilitar ou permitir a obtenção de vantagem ilícita”) de modo a tipificar a engenharia social (estelionato eletrônico) como crime formal. (CRESPO, 2011, p.25).

É importante salientar que à época da publicação do livro de Crespo, ainda não havia uma previsão concreta de quando ocorreria uma tipificação penal adequada para o *phishing*, ou em outras palavras o "estelionato eletrônico". Isso ocorreu apenas com a Lei nº 14.155/2021, que alterou efetivamente o artigo 171 do Código Penal, com a redação dada a seguir:

> Fraude eletrônica
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

Verifica-se, no âmbito do Direito Penal e Digital, que a Lei Carolina Dieckmann (Lei nº 12.737/2012), que veio como Substitutivo ao PL 84/99,

emerge como uma resposta legislativa fundamental para a proteção dos direitos individuais no ambiente virtual. De forma subsequente, a alteração dessa lei pelo dispositivo de nº 14.155/2021 e a ratificação do Brasil à Convenção de Budapeste foram avanços significativos no que tange a investigação e punição de crimes cibernéticos, dentre eles o *phishing*.

5 **ESTRATÉGIAS DE PREVENÇÃO**

Estratégias de prevenção contra o *phishing* no Brasil variam desde a educação cibernética e políticas de segurança sólidas até a colaboração interinstitucional e programas de treinamento em constante evolução. Estas abordagens se combinam para fortalecer a postura do Brasil na luta contra o *phishing* e ameaças cibernéticas similares.

O autor Crespo questiona até onde a inclusão digital é eficiente para que se possa esperar dos usuários um comportamento de "pouco risco" no ambiente virtual (CRESPO, 2011). Ele continua com uma sugestão: "Iniciativas como a busca pela certificação em uso adequado de computadores, como preveem as Licenças Internacionais para manejo de computador [...] podem ser um rumo a ser tomado [...]" (CRESPO, 2011, p.29).

Pode-se destacar o fator humano em ocorrências de crimes nas redes "Mitnick e Simon apontam o fator humano como o elemento mais importante na gestão da segurança da informação, já que o indivíduo é o elo mais fraco de um sistema de segurança." (MITNICK; SIMON apud PINHEIRO, 2020, p.97). Nesse mesmo sentido, as organizações não podem ignorar a parte social e comportamental em seus programas de segurança da informação, em detrimento do estabelecimento de políticas e a aplicação de controles técnicos (ALEXANDRIA apud PINHEIRO, 2020).

De forma complementar, Wendt e Jorge (2021, p.14) comentam sobre a falta de percepção de risco dos usuários comuns na Internet "os usuários de Internet não conhecem a dimensão dos riscos que a utilização da rede mundial de computadores proporciona, nem as ameaças que enfrenta ao receber um e-mail, acessar um site ou instalar um programa em seu computador.".

No que tange às táticas de prevenção individuais, salienta Bomfati (2020)

> A prevenção ainda é a melhor alternativa para combater as diversas ameaças existentes. Algumas das atitudes assertivas para que se possa evitar a contaminação de computadores consistem em atentar-se para os treinamentos e as capacitações dos usuários de redes e manter os programas, sistemas operacionais e navegadores atualizados. Evitar abrir mensagens ou acessar *sites* suspeitos, ter o controle sobre quem acessa as máquinas e agir com redobrada atenção, fugindo da negligência, são ações que auxiliam na prevenção de ataques maliciosos. (BOMFATI, 2020, p.125-126).

Do ponto de vista empresarial, destaca Pinheiro (2020),

> Assim, para uma proteção adequada contra essas ameaças, é importante que sigamos as etapas de proteção contra malware, treinamentos e testes constantes contra phishing; é necessário que as informações da empresa sejam classificadas e, principalmente, compartimentadas, garantindo que apenas pessoas autorizadas e com legítimo interesse tenham acesso a certos dados da empresa. (PINHEIRO, 2020, p.26).

Esta última autora lista dicas práticas a serem adotadas principalmente no meio empresarial, como forma de prevenção a ataques como o *phishing*:

> Mantenha os sistemas sempre atualizados para tornar a proteção contra ataques e invasões mais eficiente; instrua os funcionários a criar senhas complexas, que combinem letras maiúsculas e minúsculas, números e símbolos em sua composição. Além disso, é importante criar senhas diferentes para diferentes tipos de acesso a serviços na internet e, também, que as senhas sejam renovadas a cada três ou seis meses, a depender da intensidade do uso da internet nos processos internos; adote procedimentos de análise interna para a verificação da segurança dos e-mails; embora não seja possível banir o contato por e-mail, ele pode ser realizado de maneira mais consciente, evitando invasões e ataques por meio de *phishing*; instale extensões de proteção a *malwares* – *adblock*, por exemplo – nos navegadores utilizados pelos funcionários (PINHEIRO, 2020, p.172).

No tocante à prevenção contra diversos tipos de *phishing*, Crespo (2011) fornece uma dica de prevenção:

> [...]um detalhe a que o usuário deve prestar atenção são os erros de gramática que essas mensagens geralmente apresentam, além de notarem a genuinidade do endereço do site, bem como o sinal de página segura (cadeado na parte inferior da tela) em seu navegador (CRESPO, 2011, p.25).

Verifica-se que "quanto maior a educação dos usuários dos computadores, menores as chances de os criminosos se locupletarem das situações de risco criadas pela atual sociedade global do risco informático e da informação" (CRESPO, 2011, p.29). Portanto, resta evidente a importância dos softwares de proteção contra *phishing* e outras estratégias implementadas nos

sistemas de informação, ainda que um elo inolvidável desta cadeia de prevenção seja o fator humano e comportamental, que pode colocar em risco a própria integridade ou de uma corporação, devido a uma baixa percepção de risco e atenção.

6 **CONCLUSÃO**

Este artigo teve como objetivo realizar uma análise dos impactos dos crimes cibernéticos no Brasil, especialmente os do tipo *phishing*. Foram abordados os tipos, técnicas, consequências, aspectos jurídicos e estratégias de prevenção para esse crime tão comumente praticado nessa era da informação. Esta exploração pela bibliografia de autoridades intelectuais no assunto, voltada ao aspecto jurídico e prático, objetivou reunir uma visão mais completa e multifacetada dos problemas enfrentados por empresas e particulares que lidam com essas fraudes.

Inicialmente, foi definido o fenômeno do *phishing*, com seu significado aludindo a uma "pescaria", na qual as vítimas são atraídas para uma armadilha que as "fisga". Assim, informações pessoais são reveladas ao hacker ou ele obtém dinheiro da vítima, através das diversas técnicas descritas ao longo do primeiro título.

Na sequência abordou-se a dimensão dos impactos que o *phishing* causou ao longo das duas últimas décadas, no Brasil. Através de gráficos elaborados pelo Cert.br, foi possível observar o grande volume de eventos dessa natureza, ainda que tenha sido considerado apenas os que foram reportados oficialmente. Dentre os setores que foram meio para ocorrência dessas fraudes, os que tiveram mais casos foram o financeiro, webmail corporativo e varejo. Em outra pesquisa, da PwC, foram trazidos dados de prejuízo financeiro dos entrevistados, bem como da frequência com que esses golpes foram sofridos por eles.

No tocante à parte jurídica, foi feita uma retrospectiva dos caminhos traçados pela legislação pátria, no sentido de coibir e punir estas práticas nefastas. Desde a elaboração do PL nº 84/99 até a criação da Lei nº 12.737/12 (Carolina Dieckmann), foram 13 anos de espera, que acrescentaram os artigos 154A e 154B ao Código Penal, porém com penas muito baixas, na visão de

Renato Opice Blum. Segundo ele, a alteração mais significativa veio a ocorrer somente com a Lei nº 14.155/21 que tornou as penas mais severas, proporcionais ao dano causado. Destacou-se também o Marco Civil da Internet, de 2014, que estabeleceu diretrizes importante no uso da Internet, a Lei Geral de Proteção de Dados (LGPD) para o tratamento de informação pessoais e por fim, a ratificação do Brasil à Convenção de Budapeste no ano de 2022.

No título sobre as estratégias de prevenção contra essas práticas criminosas, foram abordadas dicas práticas para os usuários da Internet, que exorbitam a questão de softwares de proteção e adequações dos sistemas de informação. Destacou-se a importância do treinamento de pessoas para um uso mais seguro das tecnologias que acessam a Internet, frisando a grande importância do fator social e comportamental apontado por Mitnick e Simon, como o "elo mais fraco da cadeia de segurança".

Portanto, verifica-se que houve um avanço substancial na legislação brasileira para amparar as vítimas de *phishing*. Em contrapartida, é possível observar que grande parte dessas ocorrências podem ser evitadas com treinamento, capacitação e atenção do usuário para utilizar a Internet. A prevenção tem papel fundamental para que mais usuários entendam as ameaças existentes e ajam com prudência, não confiando apenas no Estado para protegê-lo. Não obstante, se a parte preventiva falhar, a legislação penal pátria já possui formas de coibir e punir essa prática e a tendência é que surjam mais dispositivos legais à medida que a discussão pública sobre o tema se intensifica.

REFERÊNCIAS:

BLUM, Renato Opice. **As novas diretrizes do Direito Digital**. Consultor Jurídico. 2015. Disponível em: https://www.conjur.com.br/2015-out-05/renato-opice-blum-novas-diretrizes-direito-digital/. Acesso em: 21 nov. 2023.

BOMFATI, Cláudio Adriano; JUNIOR, Armando Kolbe. **Crimes cibernéticos**: Aspectos Jurídicos. 1 ed. 2020. 197 p. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 22 nov. 2023.

CERT.BR. Disponível em: https://stats.cert.br/phishing/#categorias-all. Acesso em: 18 nov. 2023.

CRESPO, MARCELO XAVIER DE FREITAS. **Crimes digitais**. Saraiva Educação S.A., v. 3, 2011. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788502136663/epubcfi/6/28[%3Bvnd.vst.idref%3Dc04]!/4/324/7:0[%2C%5E%2C%20q]. Acesso em: 13 nov. 2023.

FERREIRA, Haroldo. **Cibersegurança**. Editora Senac São Paulo, f. 98, 2021. 196 p. Disponível em: https://www.bibliotecadigitalsenac.com.br/?from=busca%3FcontentInfo%3D3256%26term%3Dcrimes%25252520cibern%252525C3%252525A9ticos#/legacy/epub/3256. Acesso em: 18 nov. 2023.

PINHEIRO, Patricia Peck *et al*. **Segurança Digital - Proteção de Dados nas Empresas**. 2020. Disponível em: https://integrada.minhabiblioteca.com.br/books/9788597026405. Acesso em: 17 nov. 2023.

REINA, Eduardo. **Lei Carolina Dieckmann completa 10 anos com necessidade de complementações**. Consultor Jurídico. Disponível em: https://www.conjur.com.br/2022-dez-27/lei-carolina-dieckmann-completa-10-anos-elogio-cautela/. Acesso em: 19 nov. 2023.

RIBEIRO, Priscilla Bortolotto. **Guerra Cibernética**: Cenário Mundial de Defesa e Segurança. 1 ed. São Paulo: Contentus, 2020. 93 p. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 15 nov. 2023.

SILVA, Michel Bernardo Fernandes da. **Cibersegurança**: Visão Panorâmica Sobre a Segurança da Informação na Internet. 1 ed. Freitas Bastos, v. 3, f. 82, 2023. 163 p. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 15 nov. 2023.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos 3a edição**: ameaças e procedimentos de investigação. Brasport, v. 3, f. 125, 2021. 249 p. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 22 nov. 2023.