JNT - FACIT BUSINESS AND TECHNOLOGY JOURNAL - ISSN: 2526-4281 - QUALIS B1
ANO 2025 – MÊS DE MAIO - FLUXO CONTÍNUO – Ed. 62. Vol. 2. Págs. -274-287
DOI: 10.5281/zenodo.15530333

O GOLPE ESTÁ AÍ. VULNERABILIDADE SOCIAL, ESTUDO DOS CRIMES VIRTUAIS E PREVENÇÃO DAS NOVAS MODALIDADES DE CRIMES CIBERNÉTICOS: GOLPES *PHISHING*

THE SCAM IS HERE. SOCIAL VULNERABILITY, STUDY OF VIRTUAL CRIMES AND PREVENTION OF NEW TYPES OF CYBERCRIMES: PHISHING SCAMS

Renata Costa MACEDO
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: reeh08012004@gmail.com
ORCID: http://orcid.org/0009-0009-2930-4837

Mainardo Filho Paes da SILVA
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: mainardoadv@hotmail.com
ORCID: http://orcid.org/0009-0009-0919-4781

RESUMO

O termo *phishing* remete-se a ampla utilização de meios on-lines para o cometimento de crimes cibernéticos. O avanço tecnológico trouxe diversos benefícios, no entanto, com o crescente número de usuários de internet, houve um significativo aumento nas atuações criminosas por meios virtuais, principalmente entre o período pandêmico enfrentado em meados de 2020. Este trabalho tem como objetivo analisar o fenômeno do *phishing*, suas principais características, impactos, mecanismos de prevenção e formas de denúncias. A pesquisa foi desenvolvida abordando os aspectos, diferenças das tipologias e práticas de *phishing* para que a população identifique de forma rápida e eficaz as metodologias fraudulentas utilizadas. Conclui-se que, embora a prática seja reconhecida por grande parte da população, a temática ainda sim é ignorada por uma pequena parcela da sociedade desencadeando o crescente número de vítimas de crimes. Portanto, torna-se evidente a necessidade de políticas públicas voltadas à educação digital da população no combate ao *phishing.*

Palavras-chave: *phishing*. Crimes cibernéticos. Denúncia. Impactos.

ABSTRACT

The term phishing refers to the widespread use of online means to commit cybercrimes. Technological advances have brought several benefits, however, with the growing number of internet users, there has been a significant increase in criminal activities through virtual means, especially during the pandemic period faced in mid-2020. This work aims to analyze the phenomenon of phishing, its main characteristics, impacts, prevention mechanisms and forms of reporting. The research was developed addressing the aspects, differences in phishing typologies and practices so that the population can quickly and effectively identify the fraudulent methodologies used. It is concluded that, although the practice is recognized by a large part of the population, the issue is still ignored by a small portion of society, triggering the growing number of crime victims. Therefore, the need for public policies aimed at digital education of the population in the fight against phishing becomes evident.

Keywords: Phishing. Cybercrimes. Reporting. Impacts.

INTRODUÇÃO

A crescente dependência de meios tecnológicos em nosso cotidiano vem transformando a maneira como indivíduos e organizações interagem. Com o surgimento de meios on-lines e eletrônicos, a população tem se utilizado cada vez mais de recursos acessíveis para a realização de transações e compartilhamento de dados.

No entanto, essa digitalização vem causando lacunas de possiblidades para novas formas de criminalizações, entre as quais se destaca o *phishing*. Os impactos dessas ações vão além das perdas financeiras, comprometendo também a privacidade, a integridade e a confiabilidade das redes e dos sistemas.

Portanto, em decorrência das situações expostas acima, a presente pesquisa visa colaborar no conhecimento do assunto, na informatização da população em relação a incidência de delitos utilizando o *phishing* no Brasil, bem como nos métodos utilizados pelos fraudadores, levando em consideração ainda as consequências e prevenções desta prática.

OBJETIVOS

Objetivo geral

Compreender e informar a população sobre o crescimento e identificação dos principais cibercrimes.

Objetivos Específicos

- Realizar uma pesquisa quantitativa da incidência dos crimes *phishing*
- Definir como identificar as modalidades de golpes e suas formas de denúncia.
- Informar a população sobre a importância da prevenção dos crimes *phishing.*

METODOLOGIA

A presente temática utilizou-se das abordagens metodológicas dos métodos bibliográfico, dedutivo, documental e qualitativo. Realizando revisão e análise de literaturas, legislação, estudos e artigos eletrônicos. Pretendendo, assim, compreender a realidade enfrentada pela população sobre a tese abordada.

Segundo Silva & Menezes (2000), na descrição do fenômeno de uma população notoriamente definida requer técnicas nas coletas relativas a informações, sendo estas mesmas estabelecidas através de questionários e observações.

Para Marconi e Lakatos (2010), a abordagem qualitativa diz respeito à pesquisa que versa sobre a análise, interpretação de aspectos, descrições em torno da complexidade do comportamento humano e investigações de atitudes atinentes.

Contudo, o presente artigo apresenta diversas informações confeccionadas através de profunda revisão de literatura e estudo de gráficos, buscando assim resolver problemáticas levantadas a partir das necessidades humanas expostas através de documentos, textos, artigos e livros.

REFERENCIAL TEÓRICO

De acordo com a revista da faculdade de direito de Lisboa (2013, p. 7) a denominação *phishing* é utilizada de forma ampla para referenciar a utilização de meios on-lines para a prática de atividades fraudulentas. O objetivo principal da utilização de *phishing* é a obtenção de dados e informações confidenciais protegidas

por meio da Lei 13.709/2018, mas conhecida como lei de proteção de Dados, para a aquisição de benefícios ilícitos através dos dados alcançados. Outrossim, vale destacar que há diversas formas de efetivação da atuação criminosa entre elas mensagens através de correios eletrônicos e de URLs ou Websites fraudulentos.

Após o período pandêmico vivenciado pela população com quarentenas e isolamentos, a utilização de internet e meios de trabalhos *home offices* alavancaram significativamente subindo a cada dia de forma descontrolada vindo a desencadear impactos em diversas áreas. Assim é o posicionamento dos autores Bossler e Holt (2009, p. 400) "[...] a penetração da tecnologia da computação proporcionou aos criminosos ferramentas eficientes para cometer crimes [...]".

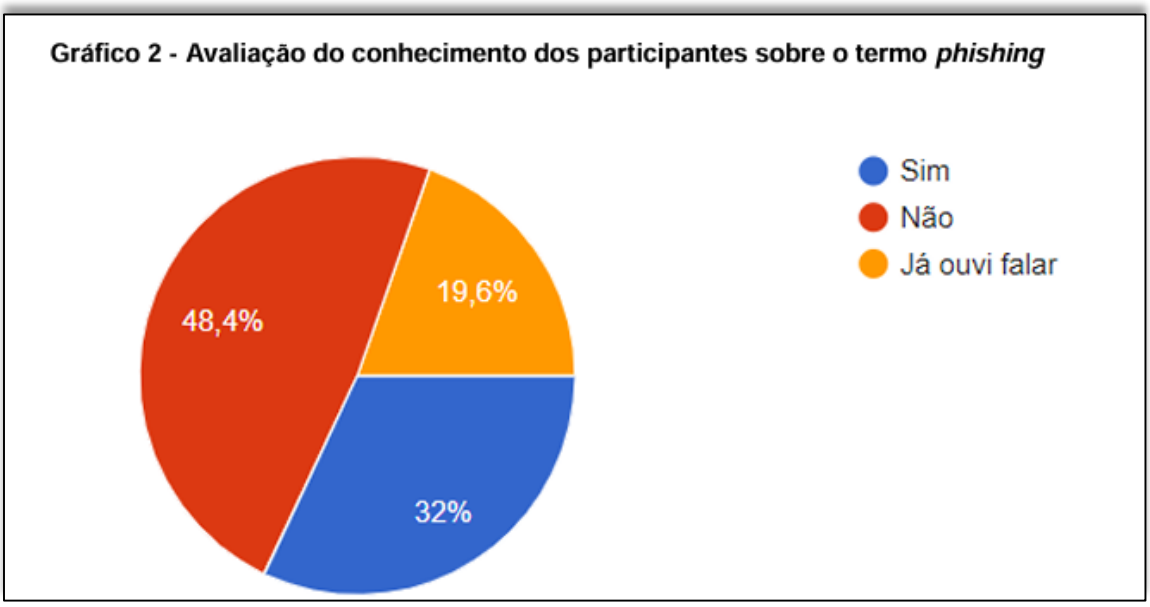
A PhishMe Inc, fornecedora líder das soluções de defesa de *phishing* humano, trouxe referências sobre a existência de uma grande quantidade de e-mails *phishing* que contêm um tipo de software malicioso chamado *ransomware* que será discutido no decorrer deste trabalho.

PRINCIPAIS MODALIDADES

O *phishing* abrange o cotidiano dos usufrutuários de internet e rede, frequentando-se através de diferentes formas, dificultando a identificação da atividade criminosa pelo receptor do conteúdo desonesto.

O estudo dos autores Queiroz & Rosa em 2019, demonstra o nível de conhecimento dos usuários de redes e internet, confirmando que cerca de 93,5% dos participantes tinham conhecimento das possibilidades de furtos através de e-mails e websites falsos. Contudo, 48,4% dos participantes não tinham conhecimento do termo *phishing,* já 12,4% não tinham conhecimento tácito sobre o assunto e 10,5% já refletiram sobre o assunto, porém não viram relevância, conforme demonstra-se nos gráficos a seguir.

Figura 1

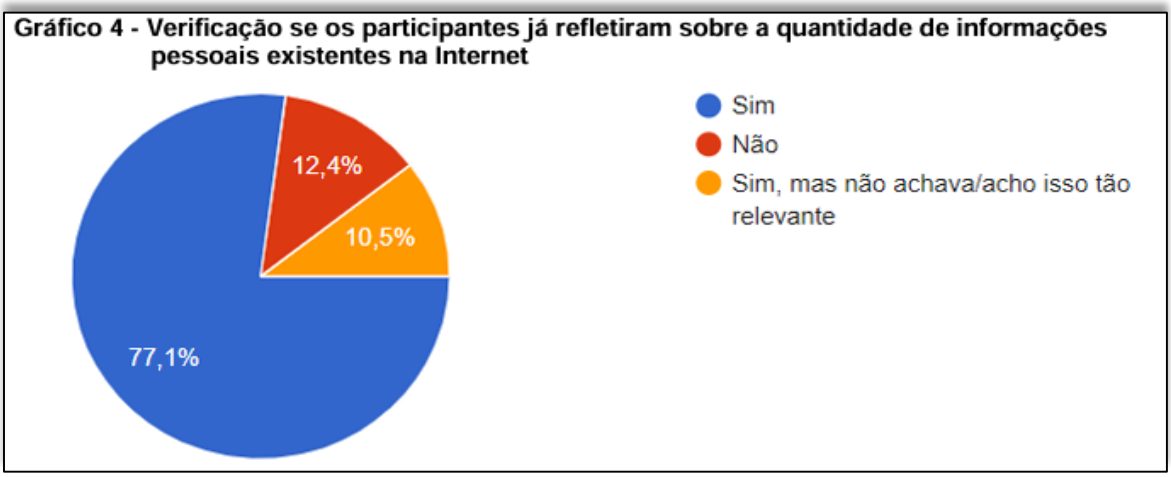


Fonte: Queiroz & Rosa 219, p. 55

Figura 2

Fonte: Queiroz & Rosa 219, p. 56

Figura 3



Fonte: Queiroz & Rosa 219, p. 56

Portanto, verifica-se que apesar das diversas formas de prevenção de *phishings*, a população não possui conhecimento das modalidades utilizadas por estes criminosos. Assim, aborda-se abaixo algumas modalidades utilizadas para melhor elucidação da comunidade.

Phishing Tradicional

A presente variação objetiva-se no ato do fraudador criar uma mensagem enganosa, compatível com a legítima. O principal e mais novo exemplo de tal conduta, arrastou-se por meio das redes sociais e SMS. Podendo ser identificada por meio de mensagem, e-mail e ligação falsa, como: avisos de impostos, bloqueios de cartão de créditos, entre outros.

Spear Phishing

Os spears phishings trata-se de atos direcionados a um único grupo de pessoas, empresa ou instituição governamental. Estes possuem o foco maior na obtenção de conteúdos ou bancos de dados confidenciais.

De acordo com o entendimento dos autores Queiroz & Rosa (2019), o LinkedIn também deve ser foco de atenção, uma vez que outros usuários podem ver a empresa em que trabalha e seu cargo, facilitando a elaboração de um ataque de spear phishing.

Portanto, enfatiza-se que os perigos de ataques cibernéticos vêm aumentando a cada dia, devendo haver formas de transmissão de conhecimento das modalidades e formas de prevenção para evitar a majoração deste número, tendo em vista, que estamos vivenciando a era da tecnologia e utilizando de forma crescente e contínua a internet e suas facilitações, em meios como o trabalho, lazer e estudos.

Whaling

O Whaling refere-se ao ataque de *phishing* direcionado a indivíduos ou organizações de alto perfil, como CEOs, executivos de alto escalão ou funcionários-chave de uma empresa.

Este ataque utiliza-se de meios como comunicados fraudulentos que fazem parecer vir de uma pessoa muito influente na organização, pois psicologicamente os funcionários tendem a acreditar mais em informações de alguém que estes consideram importante (Salviano et. al, 2022).

Esse tipo de ataque requer uma pesquisa prévia sobre a vítima para tornar o e-mail ou a mensagem convincente e persuasiva.

Segundo, Bezerra & Silva (2024) para reduzir os riscos, é importante realizar treinamentos com os funcionários para reconhecer esses ataques, realizar verificação manual de transações bancárias e reforçar as medidas de segurança cibernética para membros importantes da organização".

Vishing

O vishing é um dos principais golpes e com um grande índice de sucesso, é o tipo de ato que se utiliza de mecanismos de voz para a obtenção de dados, o exemplo mais comum de tais práticas são as ligações de compras supostamente realizadas.

Segundo Avast (s/d. s/p), "Um cenário de vishing é alguém afirmando ser de uma organização ou empresa respeitável e conhecida por você, mas que, na verdade, é um golpista tentando roubar as suas informações, o seu dinheiro ou outros dados".

Trata-se de uma atuação bem corriqueira e comum, quem nunca recebeu uma ligação de compra on-line, que para ser confirmada necessita informar dados pessoais.

Smishing

Os Smishing são atos por meio de SMS, que miram no emocional da vítima, relatando sobre dívidas e abordando oportunidades com grandes vantagens.

Segundo Moura (2021), o smishing trata-se da prática de roubar informações pessoais ou financeiras por meio de alertas ou contatos enganosos. Em seu posicionamento, a autora traz referência à grande maioria dos casos, sendo estes os falsos alertas de bancos avisando sobre operações em contas bancárias da vítima, instigando-a vítima entrar em links que as redirecionam para falsas centrais.

Clone Phishing

O clone phishing diz respeito ao ato de interceptação de um e-mail legítimo já enviado em algum momento ao vitimado, atuando na criação de mensagens falsas praticamente idênticas aos originais, porém ao invés de anexos originais são utilizados vírus ou malwares.

Segundo os autores Souza, Bini & Lourenço, o clone da phishing trata-se do ato do hacker clonar um site original para atrair usuários a acessar o site falso e inserir informações cadastrais que serão transmitidas aos criminosos. Na sequência, sem perceber que foi vítima, o usuário é direcionado para a página original.

Ransomware

O ransomware trata-se de um tipo de malware para sequestro de dados, caracterizado pelo pedido de resgate por parte dos criminosos. Os dados da vítima são criptografados e usados como refém.

Segundo Lawrence Miller ransomware é um software malicioso (malware) usado em ataques cibernéticos para criptografar dados da vítima utilizando chaves de encriptação conhecidas unicamente pelo invasor, que tornam as informações inacessíveis até o pagamento de um resgate (normalmente por meio de uma criptomoeda, como a Bitcoin) a ser feito pela vítima.

Em seus estudos Liska e Gallo (2017), abordaram que há algumas variantes que atacam corporações que cobram dezenas de milhares de dólares, bem como existem

ransomwares que com o passar do tempo o preço sugerido é aumentado, para causar mais terror para as suas vítimas.

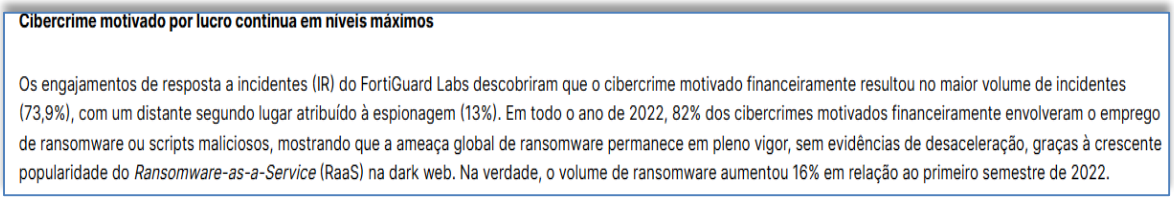
Gráficos de Incidência dos Cibercrimes no Brasil

A terminologia cibercrime relaciona-se a qualquer atividade ilegal onde há utilização de meios eletrônicos para aceder, alterar ou destruir informações confidenciais. Alguns desses crimes são: roubo de identidade, perseguição, intimidação ou terrorismo (Upadhyay & Yadav, 2018).

No Brasil a incidência dos cibercrimes se estende a uma grande escala, com a necessidade de utilização das redes pela população e o alto uso de internet, sendo infindo a vulnerabilidade da população.

Como estudos denotam que apesar da maioria da população ter ciência do que se tratam os crimes cibernéticos, grande parte não contém conhecimento do termo phishing e das modalidades utilizadas pelos criminosos. Além disso, uma pequena fração não dá a devida atenção por subentender que o tema não seja importante.

Contudo conforme demonstra a infra notícia podemos notar que a recorrência desta classe de crime está frequentemente direcionada a obtenção de lucro sendo está na modalidade direta ou indireta.



Cibercrime motivado por lucro continua em níveis máximos

Os engajamentos de resposta a incidentes (IR) do FortiGuard Labs descobriram que o cibercrime motivado financeiramente resultou no maior volume de incidentes (73,9%), com um distante segundo lugar atribuído à espionagem (13%). Em todo o ano de 2022, 82% dos cibercrimes motivados financeiramente envolveram o emprego de ransomware ou scripts maliciosos, mostrando que a ameaça global de ransomware permanece em pleno vigor, sem evidências de desaceleração, graças à crescente popularidade do *Ransomware-as-a-Service* (RaaS) na dark web. Na verdade, o volume de ransomware aumentou 16% em relação ao primeiro semestre de 2022.

Fonte: https://www.fortinet.com/br.

Já em 2022, com o ápice da pandemia e maior concentração de usuários este tipo de crime ganhou novamente lugares nas maquetes, tornando-se uma das grandes preocupações em meio à crise enfrentada no país.

Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%

País é o 2º na América Latina com mais ataques cibernéticos em 2022

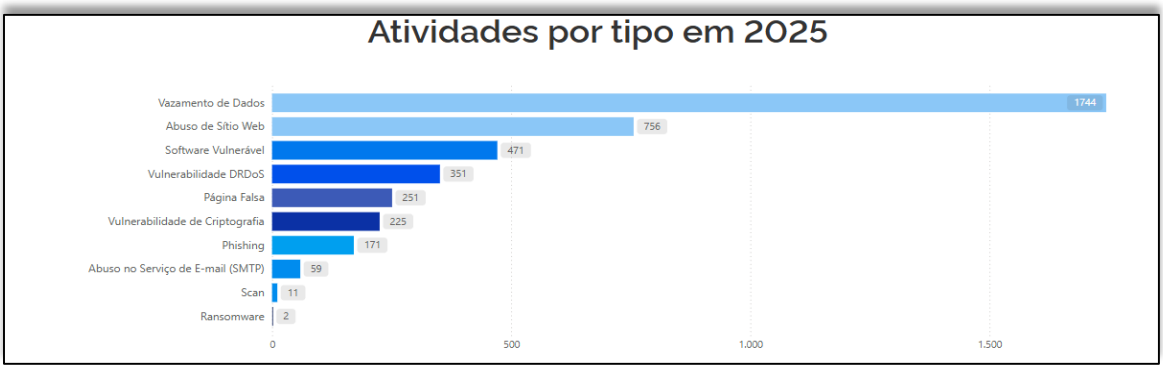
Ingrid Oliveira, da CNN

19/08/2022 às 17:42 | Atualizado 22/08/2022 às 11:24

Fonte: https://www.cnnbrasil.com.br.

Segundo o monitoramento realizado pelo governo relativo às atividades criminosas por meios virtuais entre os meses de janeiro a março do ano de 2025, observa-se que houve cerca de 1.744 vazamentos de dados, 756 abusos de sítio Web, 471 Softwares Vulneráveis, 251 Páginas falsas, 171 Phishing, entre outros.

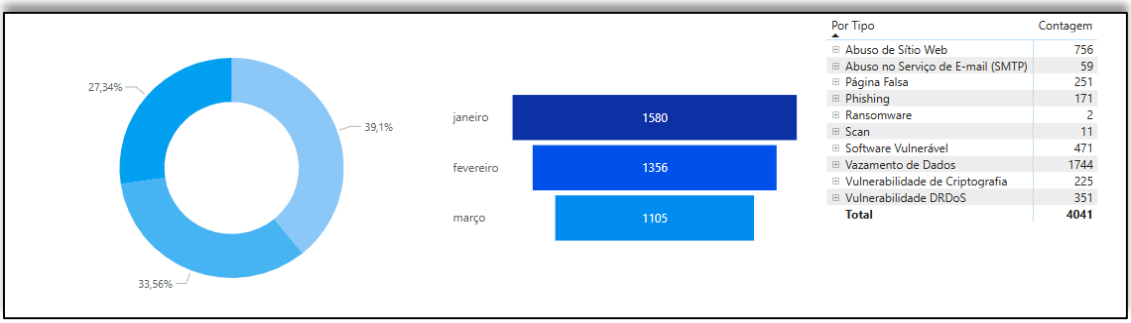
Figura 4



Fonte: https://www.gov.br

Podemos verificar, que no mês de janeiro houve uma maior incidência alcançando a um quantitativo de 1580, em fevereiro 1356, já em março o quantitativo despencou para 1105 reduzindo quase ⅓ da quantidade de janeiro.

Figura 5



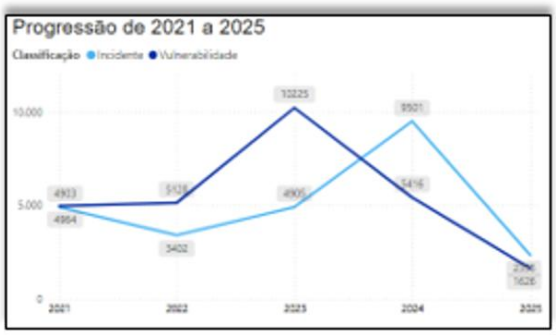
Fonte: https://www.gov.br.

O estudo ainda demonstra o aumento da incidência e vulnerabilidade nos anos de 2021 a 2025.

Figura 5

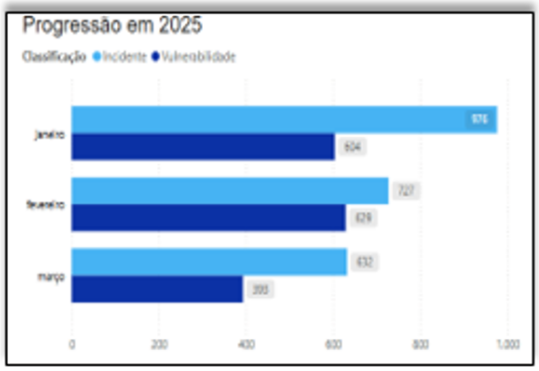
Fonte: https://www.gov.br

Figura 6



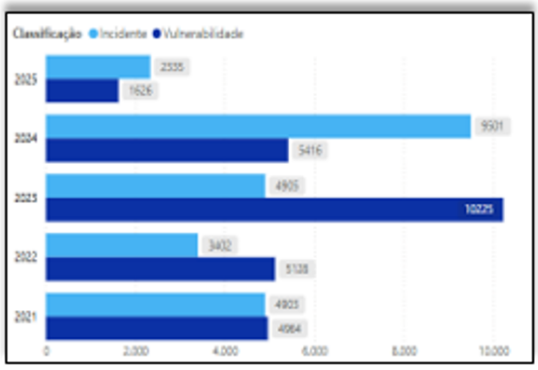
Fonte: https://www.gov.br

Figura 7



Fonte: https://www.gov.br

Figura 8



Fonte: https://www.gov.br

Lei 12.737 de 30 de novembro de 2012.

A lei 12.737/2012 foi proposta pelo Deputado Paulo Teixeira (PT-SP) em 2011, sendo sancionada somente em 30 de novembro de 2012 objetivando-se em prol da tipificação de crimes cibernéticos, como invasão de dispositivos informáticos, violação de dados e "derrubada" de sites, sendo a primeira lei brasileira a punir tais delitos.

Esta lei foi criada em resposta ao caso de violência contra a atriz Carolina Dieckmann, que teve seu computador invadido e fotos íntimas divulgadas na internet. Desde a criação da lei a busca pela conscientização e prevenção da população contra os crimes cibernéticos tem se arrastado demonstrando por meio de estudos um pequeno declive nos números.

Formas de denúncia dos cibercrimes

Os crimes cibernéticos podem ser denunciados por meio de boletins de ocorrência presenciais e virtuais podendo ser realizados nas delegacias civis ou

federais ou por meio de site conhecido como Sinesp Delegacia Virtual - DEVIR. Segue abaixo as instruções para realização de denúncia de forma virtual.

1) **Acessar o Portal:** Nessa etapa o cidadão deve acessar o Portal da Delegacia Virtual do Ministério da Justiça e Segurança Pública. **Canais de prestação**: Disponível em: Acesse o site;
2) **Selecionar o Estado onde o fato ocorreu:** Unidade da Federação onde o fato ocorreu;
3) **Selecionar a natureza correspondente ao fato que deseja comunicar;**
4) **Informar do que se trata o fato;**
5) **Se autenticar através de login na Conta gov.br;**
6) **Inserir o CPF e a senha de acesso da conta no sistema gov.br.**
   (Caso ainda não tenha cadastro no gov.br, acesse o link: https://www.gov.br/pt-br/servicos/criar-sua-conta-meu-gov.br";
7) **Preencher o formulário de comunicação:** O cidadão preencherá os campos mínimos obrigatórios referentes ao fato, para a finalização de sua comunicação.

A denúncia também pode ser realizada através do Disque 100. Se você foi vítima de algum tipo de golpe ou mesmo algum crime, o indicado é que entre em contato com a delegacia mais próxima por meios eletrônicos ou de forma presencial para que preste denúncia do acontecido ou pelo site acima informado, realizando passo a passo o boletim de ocorrência.

CONCLUSÃO

A presente pesquisa aborda a intensificação do quantitativo de ameaças de meios eletrônicos para o acometimento de delitos virtuais, destacando as principais ramificações de *phishing,* sendo estas: Clone *Phishing*, Spear *Phishing*, Whaling, Ransomware.

Diante do avanço tecnológico e o crescimento de usuários de redes e internet a população passou a ficar cada vez mais vulnerável a este tipo de fraude, sendo necessários meios de combates a tais atos.

Os dados demonstram a necessidade de meios para a conscientização da população sobre as formas de prevenção e os prejuízos causados em situações do

acometimento da ação fraudulenta, sendo estes financeiros, pessoais, psicológicos e sociais, portanto, este estudo busca elucidar os mecanismos de denúncias e prevenção.

Conclui-se, portanto, que o combate ao *phishing* exige não somente medidas repressivas, mas também medidas preventivas, como campanhas de conscientização, notícias, pesquisas ou quaisquer outros meios quais conscientizem a população sobre a importância da temática e com isso auxilie na redução de crimes virtuais no Brasil.

REFERÊNCIAS

AVAST, **O que é vishing e como posso me proteger contra ele?** Disponível em: <https://blog.avast.com/pt-br/stay-protected-vishing-scams>. Acesso em 19 de abril de 2025.

BRASIL, Lei. 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação de**, 2012.

BEZERRA, Paloma; SILVA, Rodrigo Cardoso. 2004. **Estudo de Técnicas de Phishing:** Métodos de Ataque e Estratégias de Defesa.

LISKA, A, GALLO, T. Ransomware: **Defendendo - se da extorsão digital.** 1. ed. São Paulo: Novatec, 2017. 223 p. ISBN 978 - 85 - 7522 - 551 - 6.

MILLER, LAWRENCE. **Ransomware defense form dummies a while brand**. Nova Jersey: John Wiley & Sons, Inc., 2017.

MOURA, Bianca. **O que é smishing?** Saiba tudo! 2021. Disponível em: <https://www.psafe.com/blog/o-que-e-smishing-saiba-tudo/>. Acesso em 19 de abril de 2025.

SALVIANO, Edgard Mesquita & SANTOS, João Pedro Ribeiro & Silva, Matheus Almeida. **Principais tipos de ataques Phishing e mecanismos de segurança**. UNICEPLAC. Jul, 2022.

UPADHYAY, V., & YADAV, D. (2018). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies: Current Technologies. **International Journal of Engineering Research And Management (IJERM),** 5. Retrieved from. Acesso: https://www.ijerm.com/download_data/IJERM0507021.pdf em 18 de abril de 2025.

SITES CONSULTADOS:

http://hdl.handle.net/10451/59340 acesso em 06 de abril de 2025.

https://g1.globo.com/ap/amapa/noticia/2024/12/20/quadrilha-cria-site-se-passa-por-empresa-de-energia-do-amapa-e-emite-boletos-falsos.ghtml acesso em 06 de abril de 2025.

https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/ acesso em 06 de abril de 2025.

https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent acesso em 08 de abril de 2025.

https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros acesso em 08 de abril de 2025.

https://www.proquest.com/openview/98e73333a91d01bced5e59ac0f07081a/1?cbl=2026366&diss=y&pq-origsite=gscholar acesso em 14 de abril de 2025.

https://ric.cps.sp.gov.br/handle/123456789/3780 acesso em 14 de abril de 2025.

https://doi.org/10.11606/issn.2316-9141.rh.2021.165401 em 18 de abril de 2025.