FACULDADE DE ILHÉUS

FACULDADE MADRE THAÍS

COLEGIADO DO CURSO DE DIREITO
COORDENAÇÃO DE TCC
ARTIGO CIENTÍFICO

A IMPORTÂNCIA DO COMBATE À DESINFORMAÇÃO E A ATUALIZAÇÃO DO CÓDIGO PENAL PARA CRIMES VIRTUAIS DE ENGENHARIA SOCIAL/PHISHING

Ilhéus, Bahia
Novembro - 2022

COLEGIADO DO CURSO DE DIREITO
COORDENAÇÃO DE TCC
ARTIGO CIENTÍFICO

GUILHERME AFONSO DE MELO NASCIMENTO

A IMPORTÂNCIA DO COMBATE À DESINFORMAÇÃO E A ATUALIZAÇÃO DO CÓDIGO PENAL PARA CRIMES VIRTUAIS DE ENGENHARIA SOCIAL/PHISHING

Artigo Científico entregue para acompanhamento como parte integrante das atividades de TCC II do Curso de Direito da Faculdade de Ilhéus/Faculdade Madre Thaís.

Área de concentração: Direito Penal/Direito Digital
Orientador. Prof. Me. JACKSON NOVAES SANTOS
Coorientador. Prof. Me. GABRIEL OCTACILIO BOHN EDLER

Ilhéus, Bahia
2022

A IMPORTÂNCIA DO COMBATE À DESINFORMAÇÃO E A ATUALIZAÇÃO DO CÓDIGO PENAL PARA CRIMES VIRTUAIS DE ENGENHARIA SOCIAL/PHISHING

GUILHERME AFONSO DE MELO NASCIMENTO

APROVADO EM: ___/____/____

BANCA EXAMINADORA

_____

PROFª. DR. JACKSON NOVAES SANTOS
FACULDADE DE ILHÉUS – CESUPI
(ORIENTADOR)

_____

PROFª. DR. GABRIEL OCTACILIO BOHN EDLER
FACULDADE DE ILHÉUS – CESUPI
(COORIENTADOR)

_____

PROFª. (NOME DO PROFESSOR AVALIADOR)
FACULDADE DE ILHÉUS – CESUPI
(EXAMINADOR I)

_____

PROFª. (NOME DO PROFESSOR AVALIADOR)
FACULDADE DE ILHÉUS – CESUPI
(EXAMINADOR II)

Sumário

1 INTRODUÇÃO **6**
2 CONCEITO DE CIBERCRIME **7**
3 CONTEXTO HISTÓRICO DO DESENVOLVIMENTO DA ENGENHARIA SOCIAL **8**
4 A DIMENSÃO DA ENGENHARIA SOCIAL **8**
5 O MODUS OPERANDI DO PHISHING **9**
6 A TIPIFICAÇÃO DO PHISHING **10**
7 CONSIDERAÇÕES FINAIS **11**
REFERÊNCIAS **11**

A IMPORTÂNCIA DO COMBATE À DESINFORMAÇÃO E A ATUALIZAÇÃO DO CÓDIGO PENAL PARA CRIMES VIRTUAIS DE ENGENHARIA SOCIAL/PHISHING

THE IMPORTANCE OF FIGHTING DISINFORMATION AND UPDATING THE CRIMINAL CODE FOR SOCIAL ENGINEERING/PHISHING VIRTUAL CRIMES

Guilherme Nascimento[1], Jackson Santos[2], Gabriel Edler[3]

[1]Discente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia. e-mail: guilhermeafonso@protonmail.com

[2]Docente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia. e-mail: novaisjn@hotmail.com

[3]Docente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia. e-mail: gabriel.edler@gmail.com

Esse presente artigo traz um compilado de dados e estatísticas científicas sobre o tema de cibercrimes de engenharia social/*phishing*, com o objetivo de mostrar o desenvolvimento de novas condutas delitivas com o advento das novas tecnologias. Explicitar a necessidade da tipificação própria para essas novas condutas do cibercrime, evidenciar a amplitude da engenharia social e elucidar sua principal conduta nas redes que é o *phishing*, desvelando o modus operandi desse golpe e sendo elucidativo para mostrar informações simples que a sociedade civil tendo acesso pode evitar cair em boa parte desses golpes tão influentes com o avanço das novas tecnologias. Neste contexto, apresenta-se como é penalizado essa conduta quando não é possível evitar, porque a prevenção, não ser conhecida pela vítima ou não eficiente o bastante. Como o Código Penal Brasileiro é de 1940, obviamente não tinha como prever essas novas condutas com o advento da tecnologia da informação, no presente artigo é desvelado sua defasagem e suas deficiências. A lei com o pseudônimo “Lei Carolina Dickman”, de 2012, que acrescenta os Arts. 154-A e 154-B, que tipifica a invasão de dispositivo informático e entre outros crimes como falsificação de documento particular, que mesmo com essa tentativa de criminalizar esses golpes que consegue tipificar de fato vários, mas ainda ficando vago para muitos deles como o *phishing* não fazendo uma subsunção da norma com o fato.

Palavras-chave: Direito penal, Direito Digital, Phishing, Engenharia Social, Cibercrime

This article presents a compilation of data and scientific statistics on the topic of social engineering/phishing cybercrimes, with the objective of showing the development of new criminal behavior with the advent of new technologies. Explain the need for the proper classification for these new cybercrime behaviors, highlight the breadth of social engineering and elucidate its main conduct on the networks that is phishing, revealing

the modus operandi of this scam and being elucidative to show simple information that civil society has access to. can avoid falling into most of these influential scams with the advancement of new technologies. In this context, it is presented how this conduct is penalized when it is not possible to avoid it, because prevention is not known to the victim or not efficient enough. As the Brazilian Penal Code dates from 1940, obviously there was no way to foresee these new behaviors with the advent of information technology, in this article its discrepancy and deficiencies are revealed. The pseudonymous “Carolina Dickman Law” of 2012, which adds Arts. 154-A and 154-B, which typifies the invasion of a computer device and among other crimes such as forgery of a private document, which even with this attempt to criminalize these scams that manages to typify in fact several, but still being vague for many of them such as the phishing not making a subsumption of the norm with the fact.

Keywords: Criminal Law, Digital Law, Phishing, Social Engineering, Cybercrime

1 INTRODUÇÃO

O advento da Internet foi um dos principais propulsores para o desenvolvimento da globalização e o acesso à rede internacional de computadores que revolucionou as interações sociais. Por conta disso, como o Direito é um dos meios de pacificação social, ele precisa se adequar aos diversos novos conflitos criados pela tecnologia.

O direito, assim como nossa língua, é vivo e deve ser atualizado conforme muda as interações sociais. Novas condutas foram desenvolvidas nesse processo de difusão da rede internacional de computadores. Assim como muitos anos atrás se teve a revolução dos bancos e formas de pagamento via cheque, veio também novas condutas delitivas como a de cheque falso praticado por meio de engenharia social de pessoas se passando por outra para “legitimar” aquele cheque abusando da confiança e da boa-fé de outrem. Com a difusão dessa prática, obteve-se diversos prejuízos à ordem social, tendo que as leis se atualizassem a essa até então nova conduta delitiva devidamente tipificada no código penal brasileiro.

A grande fragilidade enfrentada é que a tecnologia da informática difunde esses comportamentos em massa, exponencialmente, e isso resulta em prejuízos alarmantes com ataques recorrentes e devendo assim o código penal ser atualizado para abarcar essas novas condutas de maneira específica para haver proporcionalidade e razoabilidade no seu julgamento já que o Processo Penal é um instrumento de limitação do poder de punir do estado (TUPINAMBÁ, 2017).

O estado sem compreender essas novas condutas pode cometer impunidade ou excessos, devendo ter legislação específica para essas condutas de engenharia social e em especial o *Phishing* a mais popular delas no meio digital.

O *Phishing* é um dos conflitos mais latentes na tecnologia da informação com crescimento exponencial, sendo presentemente um drama real com fortes repercussões e penalizações na sociedade e na economia (TEXEIRA, 2013). Atualmente, quem lidera o número de vítimas de *Phishing* no mundo é o Brasil, (SECURELIST, 2020). É um golpe de engenharia social que tem a prática no meio informático de obter por meio fraudulento dados sensíveis da vítima ao se passar por representante de pessoa jurídica fidedigna, ludibriando a confiança do usuário da rede. Em suma: é a conduta de pescar informações de usuário de tecnologias de rede (COIMBRA, 2020).

2 CONCEITO DE CIBERCRIME

O Cibercrime (ou Cybercrime) é um Crime Virtual, de acordo com (FERREIRA, 2005, p.261), é classificado como:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial.

É importante esclarecer que o Cibercrime não é um tipo de conduta e sim um meio com um universo de possibilidades delitivas no meio informático de obtenção de vantagem indevida em detrimento de outrem diretamente ou indiretamente. Essas vantagens podem ser desde a violação de produtos protegidos por direitos autorais a violação da privacidade particular para benefício de lucro direto ou indireto do infrator.

Um dos meios menos técnicos que não precisa de tanto conhecimento de programação e às vezes é mais eficaz que métodos mais sofisticados tecnicamente como o de *brute force* (utilização de scripts de programação para a obtenção de senha e/ou informação através de automatização. Ex: um script para tentar todas as possibilidades de uma senha) que é a Engenharia Social uma técnica ironicamente mais antiga que a própria rede internacional de computadores que consiste em induzir pessoas de maneira sociável para obter vantagem indevida.

3 CONTEXTO HISTÓRICO DO DESENVOLVIMENTO DA ENGENHARIA SOCIAL

Em um exercício antropológico para entender a origem do estelionato, podemos começar pela etimologia da palavra que vem da Grécia antiga, a qual se

refere a *stellio* que significa uma espécie de lagarto da região que tinha por característica mais notável a mudança da cor de sua pele a fim de enganar/iludir suas presas. Desde então esta expressão ficou conhecida como sinônimo de enganar, dissimular.

Segundo o doutrinador Rogério Greco (2012) “Desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas”.

Foi no código criminal (1830) do império que o estelionato surgiu com este nomem juris, ele possuía em seus elementares a cláusula genérica de se valer de artifícios fraudulentos para se obter a vantagem patrimonial e além disso várias figuras as quais se distinguiam desta genérica.

Desde então foi sempre aparecendo na legislação brasileira e se aprimorando e atualmente o crime de estelionato está no código penal de 1940 no artigo 171 do código penal que tipifica essa conduta.

Os primeiros crimes cibernéticos aconteceram nos Estados Unidos, na década de 60, havendo sua intensificação em 1980, envolvendo crimes de pirataria, manipulação de dados bancários dentre outros, e com a chegada da internet nos demais países, esses atos ilícitos virtuais os acompanharam.

Já no que se refere ao contexto histórico jurídico no Brasil, pode-se dizer que a legislação se atualizou com morosidade, haja vista, que antes de aparecem as primeiras leis, a justiça ficava muitas vezes de mãos atadas, por não haver uma legislação especifica.

Por fim, a primeira norma que se refere a crimes digitais ocorreu apenas em 2012, a Lei n° 12.737, conhecida como “Lei Carolina Dieckmann”, tipificando-os como crimes informáticos, havendo também a alteração do Art. 171-A do Código Penal. (SILVA, 2020).

4 A DIMENSÃO DA ENGENHARIA SOCIAL

Como foi anteriormente elucidado, a Engenharia Social não é uma técnica nova, mas com o advento da internet ela ganhou forças para se reinventar e expandir de diversas e criativas formas para obtenção de vantagens indevidas. A Engenharia Social que acontece no meio físico é com a utilização de métodos de persuadir as

vítimas com eloquência e/ou se passando por uma pessoa importante para obter informações sensíveis ou privilegiadas ou até mesmo vantagem de maneira direta.

Já no meio virtual onde esse tipo de prática de crimes cibernéticos uma boa parte deles necessitam de amplo conhecimento prático de manuseio de softwares especializados e/ou uso de linguagem de programação para descobrir vulnerabilidades no código das prestadoras de serviços online como e-mails, bancos, redes sociais e etc. Com a Engenharia Social não é necessário tanto conhecimento técnico assim para boa parte dos seus métodos, precisando só de criatividade de como ludibriar a vítima ao ponto de ela passar "deliberadamente" os dados sensíveis para o golpista.

Dentro da Engenharia Social no meio da tecnologia da informação se tem diversos métodos como: *phishing - angler phishing, pharming, spear phis*hing, comprometimento de e-mail comercial (BEC) e *whaling*, para citar alguns.

Sendo o Phishing uma das técnicas mais importantes para o cibercrime. Originada da palavra *"fishing"* ("pescaria"), a expressão representa um método de ataque que consiste em jogar uma isca e torcer para que o alvo morda o anzol. Assim, é possível invadir uma conta sem grande transtorno.

De todos esses métodos citados o *Phishing* sendo disparado o mais popular entre os golpes. Segundo o relatório de uma das maiores empresas de segurança virtual do mundo, Kaspersky, mostra que o Brasil é o líder no número de vítimas de ataques de *phishing*: "Os países com maior número de tentativas de abertura de sites de *phishing* em 2018 lideraram o ranking novamente em 2020: Brasil, com 19,94%, em primeiro lugar" (SECURELIST, 2020, tradução nossa).[1]

5 O MODUS OPERANDI DO PHISHING

A expressão em latim Modus Operandi é muito utilizada na ciência da criminologia para evidenciar o modo pelo qual um indivíduo ou uma organização desenvolve suas atividades ou opera.

O cibercriminoso opera o uso do *phishing* que é um neologismo da palavra americana *"fishing"* que significa pescar. Que encaixa muito bem com o conceito do crime que é de "pescar vítimas". Então o modus operandi desses criminosos normalmente é bombardear *SPAM* (que são mensagens não solicitadas) coordenadas

[1] The countries with the largest numbers of attempts at opening phishing websites in 2018 topped the rankings again in 2020: Brazil, with 19.94%, in first place (SECURELIST, 2020)

e em massa para o maior número de pessoas possíveis com o intuito de “pescar” uma vítima que foi enganada por uma mensagem onde dizia ganhar uma promoção ou que as golpistas estava se passando por uma empresa para obter vantagem indevida.

Assim como esses métodos genéricos de *phishing* que pessoas do mundo todo são bombardeadas quase todos os dias por essas tentativas de pesca de vítimas, se tem métodos mais elaborados de *phishing*.

Segundo Fabio Assolini, analista sênior de segurança da Kaspersky no Brasil, o brasileiro tem dificuldades de reconhecer uma mensagem falsa e a pesquisa mostra que 30% dos brasileiros que acessam a internet, nãos sabem reconhecer uma mensagem de correio eletrônico falsa. Dados disponíveis no relatório feito pela Kaspersky, SECURELIST, 2020.

Além do método de *SPAM* de e-mails com propagandas falsas com promoções ou confirmação de informações fraudadas.

Se tem métodos mais meticulosos de utilizar perfis falsos para ludibriar a vítima com o golpista se passando por outra pessoa para obter vantagem.

Nem sempre o golpista faz a operação afoito ao lucro direto e sim a obtenção de informações auxiliares para ser artificio para a aplicação de um golpe mais personalizado assim com mais probabilidade de êxito na sua próxima tentativa assim arrancando da vítima mais vantagem indevida.

6 A TIPIFICAÇÃO DO PHISHING

O *phishing* não foi propriamente tipificado no ordenamento jurídico brasileiro, atualmente não tendo um tipo penal que se encaixe perfeitamente com a conduta explicitada nesse artigo pelo Código Penal brasileiro.

Não obstante se tratar de uma ação autônoma, a prática é frequentemente associada a outros delitos que utilizam da ação de obter por meio fraudulento informações confidenciais, ludibriando a confiança das vítimas ao se passar por representante de pessoa jurídica fidedigna em ambiente informático, para subsidiar crimes diversos.

Assim, através do *phishing*, o criminoso obtém informações sigilosas de inúmeras pessoas, tais quais, qualificação civil, dados de cartão de crédito e dados bancários para se passar pela própria vítima da pesca informática, com o objetivo de assegurar a impunidade de outro crime que mais tarde será cometido.

Dados esses que hoje são assegurados com a Lei de Proteção de Dados, Lei nº 13.709/2018, lei que tem como objetivo assegurar o direito à privacidade dos dados pessoais e sensíveis da pessoa física.

Nessa lógica, a prática está dentro de uma cadeia organizada de crimes, sendo certo que as informações pescadas por muitas vezes são comercializadas numa espécie de mercado de informações entre criminosos. Funcionando de modo que o vendedor, que obteve de forma fraudulenta tais informações, disponibiliza para o comprador de adquiri-las ilicitamente, com intuito de usá-las para mascarar sua verdadeira identidade.

Malgrado o comércio de informações, o *phishing* geralmente é realizado por duas ou mais pessoas que integram um grupo organizado de criminosos cuja finalidade máxima não é a sua prática. Cada integrante possui sua função, desde aquele que programa os *spyware* (programa de espionagem), podendo ser diferente daquele que contata a pessoa jurídica a qual vai se passar para ludibriar clientes desta, até aquele que utiliza dos dados obtidos para fraudar o sistema de internet banking e obter vantagem econômica em detrimento da vítima e do banco.

Em consequência dessa “lacuna” no ordenamento brasileiro, muitas questões são levantadas em relação à tipificação de crimes cibernéticos: deve-se trazer novos tipos penais específicos? É possível enquadrá-los em tipos já existentes?

De fato, o Código Penal Brasileiro cuida satisfatoriamente de numerosos tipos e condutas criminosas. Todavia, em se tratando de uma legislação datada no ano de 1940 e com poucas atualizações, o fator histórico deve ser considerado ao responder essas indagações.

A discussão toma ainda mais profundidade com a ascensão da tecnologia como hoje é conhecida, atuando como um verdadeiro divisor de águas na sociedade e por conseguinte, nas ações criminosas, que cada vez mais a utilizam para subsidiar e facilitar delitos.

7 CONSIDERAÇÕES FINAIS

É compreensível analisar que um código penal de 1940 não tinha a obrigação de tipificar novas condutas advindas com a evolução da tecnologia e da mudança das interações sociais com a internet. Desta forma não é compreensível, com dados alarmantes de golpes virtuais de engenharia social e de *phishing* avançarem de

maneira exponencial e o Brasil ganhando o n°1 de vítimas em todo o globo e não ter tipificação específica para um crime que está cada vez mais comum e até hoje não ter legislação específica tipificando essas condutas.

Campanhas de alerta sobre esses golpes precisam ser incentivadas, pois fazem a diferença conforme foi relatado pelos dados do Securelist, à proporção que for intensificada essas campanhas de alerta a tendencia é o número de vítimas diminuírem.

Atualmente a temática de crimes cibernéticos de engenharia social e *phishing* não se tem subsunção do fato com nenhuma norma brasileira, ficando suscetível ao uso de outros dispositivos da lei para tentar punir essas práticas algo que se abre uma discussão já que seria um tipo de analogia algo que se tem vedação no direito penal “in malam partem”.

Desta forma, a contribuição acerca do tema é alertar o seu conteúdo, a sua importância, bem como proporção e indagar a relevância que se tem a atualização do código para não só em punir de maneira adequada e proporcional a conduta, mas em abrir um debate nacional para um tema que quanto mais discutido e elucidado fica menos suscetível de ser bem sucedido a tentativa de engenharia social e *phishing*.

REFERÊNCIAS

KULIKOVA, TATYANA; SHCHERBAKOVA, TATYANA; SIDORINA, TATYANA. **Spam and phishing in 2020**: SPAM AND PHISHING REPORTS. [S. l.], 15 fev. 2021. Disponível em: https://securelist.com/spam-and-phishing-in-2020/100512/. Acesso em: 11 abr. 2022

Moura Dorneles, D., Barasuol Rohden, R., & Vinícios Telocken, A. (2021). **ATAQUES CIBERNÉTICOS USANDO ENGENHARIA SOCIAL**. REVISTA INTERDISCIPLINAR DE ENSINO, PESQUISA E EXTENSÃO, 9(1), 68-81. https://doi.org/10.33053/revint.v9i1.626

COIMBRA, Maria Cecilia Silva. **Phishing e o Código Penal brasileiro: como tipificar a conduta?** Uma análise do Acórdão em Apelação Criminal nº 5002347-69.2010.404.7000, do Tribunal Regional Federal da 4ª Região, com base na novatio legis in mellius. 2020. 58f. Trabalho de Conclusão de Curso (Graduação em Direito) -Instituto de Ciências da Sociedade de Macaé, Universidade Federal Fluminense, 2020.

Santiago Reis Salgado, A. L., Fontes Machado, C., & Borges Vieira de Carvalho, G. (2018). Crimes Cibernéticos em Sergipe: **uma análise da engenharia social e dos outros meios de ataques dos cibercriminosos, diante da fragilidade dos usuários**. Semana De Pesquisa E Extensão Da

Universidade Tiradentes - SEMPESq-SEMEX, (18). Recuperado de https://eventos.set.edu.br/sempesq/article/view/4113

TEIXEIRA, Paulo Alexandre Gonçalves. **O fenómeno do phishing enquadramento jurídico-penal**. Orientador: Monteiro, Fernando Conde. 2013. 155 p. Dissertação para obtenção do grau de Mestre em Direito, especialidade em Ciências Jurídico-Criminais. (Mestrado) - Universidade Autónoma de Lisboa, Lisboa, 2013. Disponível em: http://hdl.handle.net/11144/301. Acesso em: 11 abr. 2022.

BRASIL. Lei 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - **Código Penal**; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil 03/ ato2011-2014/2012/leil12737.htm. Acesso em 11 de maio de 2021.

GRECO, Rogério. **Curso de Direito Penal**. 17. ed. Rio de Janeiro: Impetus, 2015.

JESUS, Damásio de, e MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

MATSUYAMA, Keniche Guimarães; LIMA, JAA. **Crimes cibernéticos: atipicidade dos delitos**. 2017.

NUCCI, Guilherme de Souza. **Código penal comentado**. 14. ed. Rio de Janeiro: Forense, 2014.

RENATA MOURA TUPINAMBÁ. **Poder punitivo estatal: justificativas e limitações Conteudo Juridico**, Brasilia-DF: 04 dez 2017, 04:30. Disponivel em: https://conteudojuridico.com.br/consulta/Artigos/51099/poder-punitivo-estatal-justificativas-e-limitacoes. Acesso em: 18 out 2022.