MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

OS GOLPES NO SISTEMA FINANCEIRO NA ÓTICA DA ENGENHARIA SOCIAL

BEZZUTTI, Michael Calgaro
FERNANDES, Elisiane Alves

RESUMO

Esta pesquisa tem como objetivo a busca de conhecimento sobre os golpes aplicados através da engenharia social, alertando a população sobre seus riscos, técnicas e mecanismos comumente utilizados pelos golpistas para conseguirem se apropriar de informações pessoais de terceiros sem seu consentimento. Por meio da pesquisa bibliográfica buscou-se dados para analisar o tamanho do problema enfrentado pela população brasileira comparado a outros países e transferindo para as instituições financeiras a responsabilidade de distribuir para maior parte de clientes as informações e as prevenções necessárias para mitigar o risco de se sofrer um golpe. É visível a fragilidade da população frente o baixo conhecimento sobre o tema e como prevenir-se. Percebe-se que o principal alvo são os idosos, com isso, sugere-se que, as instituições financeiras e os familiares os auxiliem fornecendo dicas e prevenções, para os mesmos não caírem nessas armadilhas.
PALAVRAS-CHAVE: Engenharia social. Golpes. Golpes financeiros. Ameaças cibernéticas.

ABSTRACT

This research aims to seek knowledge about the scams applied through social engineering, alerting the population about their risks, techniques and mechanisms commonly used by scammers to be able to appropriate personal information of third parties without their consent. Through bibliographical research, we sought data to analyze the size of the problem faced by the Brazilian population compared to other countries and transferring to financial institutions the responsibility of distributing to most customers the information and preventions necessary to mitigate the risk of suffering a blow. The fragility of the population is visible in the face of low knowledge on the subject and how to prevent it. It is perceived that the main target is the elderly, with this it is suggested that financial institutions and family members help them by providing tips and preventions, so that they do not fall into these traps.
KEYWORDS: Social engineering. Blows. Financial scams. Cyber threats.

MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

1 INTRODUÇÃO

Este artigo foi elaborado com o intuito de orientar e enfatizar a sociedade, dos riscos inerentes do mal uso ou a falta de cuidado com dados e informações pessoais. Podendo ocorrer sérios problemas financeiros, visto, a quantidade de ataques utilizando-se da engenharia social no Brasil. Trazendo um panorama de âmbito latino americano elencando os países mais afetados, e dados referente aos ataques ou tentativas efetuadas contra a população brasileira.

A pesquisa traz em ordem cronológica os acontecimentos antes da criação do internet banking, referenciando os golpes anteriores à chegada das novas tecnologias. Começando pelo golpe do bilhete premiado, o que é, como ele ocorre. Com a chegada de novos mecanismos bancários, juntamente criaram-se as novas tentativas de golpes, as ameaças cibernéticas, como o Phishing e SMiShing, no qual, são tentativas de golpes efetuados pela internet, utilizando como meio, os aparelhos tele comunicativos, como, por exemplo, o smartphone e o computador.

Um fator crítico dentro do setor da segurança da informação é a engenharia social, sendo este o mecanismo utilizado para manipular indivíduos e conseguir acesso a dados restritos, onde, pessoas maldosas buscam atingir o ponto fraco da tecnologia quando relacionado a segurança, o ser humano.

Diante disto, o objetivo da pesquisa é chamar a atenção da sociedade brasileira frente estes acontecidos e alertar o quão importante é a prevenção, deixando claro as medidas a serem tomadas, para evitar de serem as próximas vítimas desses criminosos.

Neste sentido, busca-se neste trabalho esclarecer a seguinte problemática: Como as novas tecnologias podem contribuir diariamente os clientes bancários e quais são os cuidados pertinentes a serem realizados para que evitem possíveis golpes? Nesse contexto também será esclarecido a diferença entre golpe e fraude. Nessa parte se deve abordar a delimitação do assunto do objeto de pesquisa, a finalidade e objetivo do trabalho, a justificativa que vai descrever a contribuição e a relevância da pesquisa, enfatizando a importância do tema tanto no âmbito acadêmico

como profissional e uma menção dos métodos empregados, para que o leitor tenha uma visão geral da temática.

2 REFERENCIAL TEÓRICO

Esta parte do estudo é dedicada à contextualização, referenciando autores, tornando compreensível os assuntos abordados no decorrer da pesquisa. Destrinchando a temática abordada posteriormente, destacando de forma mais assertiva, cada tópico foi elaborado para esclarecer as referências bibliográficas.

2.1 Banco físico e virtual

As instituições financeiras são responsáveis por captar, gerenciar, custodiar e intermediar recursos financeiros da sociedade onde está inserida. Rentabilizando-o, seja por meio de concessão de crédito ou negociação de títulos e valores mobiliários. Comercializam soluções financeiras das mais simples até as complexas, e, também, é o instrumento utilizado para pagamento de salários e aposentadorias, conforme o Banco Central do Brasil (s.d).

Segundo Furtado e Mendonça (2020), os bancos virtuais foram os responsáveis por acelerar as transformações do setor, aumentando a concorrência e o número de transações, ganhando a preferência dos clientes por ofertar um portfólio de produtos idênticos, de forma vantajosa, o custo de operação é baixo e consegue-se atingir uma escala maior de pessoas, simultaneamente.

Neste cenário, disponibilizou-se outros canais para os clientes transacionarem de forma prática, segura e ágil. Utilizando mecanismos da transformação digital para aprimorar o gerenciamento das finanças, mostrando-se eficientes nas soluções e experiências ofertadas. Assim, o cliente passou a acessar sua conta de casa, do trabalho ou onde estiver. Dentro deste contexto, estão elencadas as duas formas mais utilizadas.

MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

2.1.1 Internet Banking

Com o avanço tecnológico, as instituições financeiras acharam um diferencial competitivo em ofertar um serviço virtual para os seus clientes, dentro deste contexto, ano a ano vem investindo na aprimoração desta tecnologia de ponta, assim, a tornando-a mais acessível para todos os tipos de público, com baixo custo e rapidez nos processos.

Para Estrada (2004):

> Dispensando-se os terminais bancários, nascendo o home banking ou office banking, que permite a realização de negócios por meio de sistemas oferecidos pela instituição bancária a computadores de seus clientes, (...), O internet banking representa uma nova modalidade de comércio eletrônico, pela qual o cliente, valendo-se da internet tem acesso a vários serviços bancários para a realização de negócios e contratos eletrônicos. (ESTRADA, 2005, p. 140).

Segundo Diniz (2006), podemos classificar os produtos e serviços ofertados por este canal elencando três principais categorias, primeira: Principal meio de divulgação dos produtos e serviços utilizando-o como um veículo de publicidade; Segunda: Redução na demanda física com a facilidade nas transações digitais; Terceira: Aprimoração do relacionamento com seu cliente pois tem acesso fácil e ilimitado, quando precisar.

Diante destes argumentos citados acima, pode-se entender qual o propósito deste canal. Atrelado a este tema vem de encontro a desburocratização, destaca-se as mais de 10 milhões de transações feitas no ano de 2021 segundo dados do banco central do brasil.

2.1.2 Mobile Banking

Devido ao aumento das possibilidades e recursos tecnológicos disponíveis nos dispositivos móveis, o celular se tornou uma nova opção de canal com grande potencial de relacionamento no setor bancário. Diante das diversas transformações do mundo tele comunicativo, e após a rápida disseminação e aderência ao internet

MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

banking, as instituições começaram a avaliar a possibilidade de autoatendimento por esta ferramenta.

Para Marchetti (2010):

> O mobile banking representa uma das mais recentes inovações no setor de serviços bancários, e pode ser visto como uma tentativa de prover uma necessidade, adicionando valor para os consumidores com o fornecimento de mais oportunidades para conduzir diferentes serviços bancários. (LAUKKANEN et al, 2007, p. 420 apud MARCHETTI et al, 2010, p. 2).

Já este serviço veio da necessidade de transacionar em qualquer local com acesso à internet, de forma simples e segura, permitindo os mesmos acessos do internet banking, adaptando-se nos smartphones aplicativos financeiros com soluções inovadoras e eficazes, onde não se utiliza acesso com internet a cabo, sem que perca a agilidade e segurança nas transações do dia a dia dos usuários. Atualmente, segundo o BANCO CENTRAL DO BRASIL, é responsável por mais de 75 milhões de transações no mercado financeiro nacional. Comparado a 2019, obteve um crescimento de aproximadamente 121%, onde teve 34 milhões de transações.

Por ser muito utilizado, começaram as tentativas de novos golpes utilizando estas novas tecnologias. O tema a seguir será abordado os métodos mais conhecidos no sistema financeiro brasileiro

2.2 Golpes

Diferentemente de uma fraude, trata-se de artifícios empregados por criminosos a fim de enganar uma pessoa e lhe acarretar prejuízos, onde, as vítimas fornecem todas as suas informações pessoais, como, por exemplo, dados bancários, foto do documento de identidade entre outros.

Segundo o Ministério Público Federal (2016, p. 12):

> A prática de golpes financeiros gera graves danos ao sistema financeiro nacional, à economia popular e ao patrimônio dos consumidores, podendo atingir proporções gigantescas facilitadas pela rápida e incontrolável divulgação realizada pela internet e pela promessa de ganhos irreais. (BRASIL, 2016, p. 12)

MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

A grande elevação dos registros, o Decreto-Lei n° 2.848, de 7 de dezembro de 1940 (Código Penal), sofreu uma alteração, tornando mais severas as penas para estas práticas ilícitas, entrando em vigor a LEI Nº 14.155, de 27 de maio de 2021 (BRASIL, 2021).

2.2.1 Golpes no Brasil

Abaixo, estão elencados 2 golpes mais corriqueiros com envolvimento financeiro, relacionados a promessa de ganhar dinheiro fácil, influenciados pela ganância e falta de conhecimento, acarretando milhares de vítimas. Nestes próximos tópicos, serão descritos quais são e como funcionam.

2.2.1.1 Golpe do bilhete premiado

Historicamente, é o golpe pioneiro e com maior número de vítimas, geralmente utilizam bilhetes de loterias para aplicar, o foco são pessoas idosas. Com poder de persuasão e bem-vestidos estes criminosos atacam pessoas aleatórias na rua e informam dispor de um bilhete premiado, no qual necessitam de testemunhas para fazer o resgate, assim, ofertando-a uma porcentagem do prêmio, a vítima precisa aportar um valor como caução, boa-fé, ela vai até o banco e saca o dinheiro. Os golpistas com o dinheiro em mãos, argumentam algumas desculpas e desaparecem com o valor.

Existem diversas maneiras de induzir a vítima, uma delas segundo Pernambuco (2021), precisam vender o bilhete para outra pessoa com urgência, tendo compromisso importante já marcado e não tendo tempo hábil para sacar o valor do prêmio.

2.2.1.2 Golpe do boleto falso

Outro golpe popular é o pagamento de boletos falsos. Atrelado a descontos vantajosos, os golpistas utilizam de sites e anúncios falsos, para divulgar produtos e serviços abaixo do preço de mercado, mas, com pagamento exclusivamente à vista.

Segundo a FEBRABAN (s.d):

> O boleto de cobrança é um instrumento de pagamento de um produto ou serviço prestado por um fornecedor. Através de um boleto de cobrança, o emissor daquele documento, intitulado “Beneficiário”, receberá em sua conta o valor referente a este produto ou serviço. FEBRABAN, [s.i.]

Já o boleto falso segundo o Procon - SP (c2019), possui as mesmas características, utilizam do mesmo sistema de compensação bancária. Visualmente não possui alteração na estrutura, os criminosos copiam o mesmo layout, idêntico, as cores, logotipo e onde tudo confere: nome completo do devedor, endereço, CPF, valor da compra, mas, a única e mais importante divergência é o credor, pessoa física ou jurídica, que receberá o valor. Assim, o valor entrará em outra conta e a vítima não receberá o produto ou serviço “comprado”.

2.3 Ameaças cibernéticas

São riscos operacionais que todas as instituições enfrentam, infelizmente não é possível zerá-la, mas sim, pode ser mitigada. Segundo Monteiro (2010, p.51) “Ataques cibernéticos podem ser implementados das mais diferentes formas e a sua capacidade de lucro irá depender frequentemente do alvo dos ataques”.

Segundo a IBM (s.d), empresa referência em tecnologia da informação no Brasil, estes ataques não estão voltados apenas para danos financeiros, diretamente, mas sim, em vulnerabilizar a relação das empresas com seus clientes.

A seguir se conhecerá duas ameaças frequentemente utilizadas nos últimos anos em clientes de instituições financeiras.

2.3.1 Phishing

O pioneiro em ameaças cibernéticas é o PHISHING, que, traduzido do inglês tem o significado de “pescar”. Segundo Neto e Parente (2010, p. 1132), a vítima, muitas vezes por meio de um e-mail fraudulento é atraída, pescada, para uma página falsa onde entrega ao fraudador as informações necessárias para a prática das transações bancárias fraudulentas. O Comitê Gestor da Internet no Brasil (2012) reforça, os golpistas buscam chamar a atenção da vítima utilizando técnicas de engenharia social, juntamente, com o uso da tecnologia visando obter êxito no ataque.

MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

Para a Febraban (s.d):

> Um ataque de Phishing se inicia por meio de recebimento de e-mails que carregam vírus ou links que direcionam o usuário a sites falsos e que, normalmente, possuem remetentes desconhecidos ou falsos. As mensagens contidas nesses e-mails exploram as emoções do destinatário (medo, curiosidade, oportunidades únicas, entre outras), fazendo com que o mesmo clique nos links ou arquivos anexados. (FEBRABAN, s.i).

Prática utilizadas em outros segmentos, Queiroz e Rosa (2019) evidenciam um percentual significativo de usuários que relatam ataques desta modalidade, onde, criminosos criam sites e páginas idênticas, passando-se por verdadeiras, no qual atraem vítimas de diversos segmentos. ofertando facilidades como por exemplo, um produto com o valor inferior à comercialização a mercado

2.3.2 SMiShing

Essa estratégia criminosa age através de mecanismos mal-intencionados, onde enviam um link por SMS ou mensagem de texto para o usuário. De modo geral, o conteúdo conterá um link ou número de telefone. Assim como o Phishing, a mensagem de SMiShing geralmente pede ação imediata. Segundo Santos (2018), O golpe consiste em uma oferta ou informações duvidosas, solicitando que clique no link e se insira dados pessoais ou para retornar ligando ou enviando mensagens, como, por exemplo, transações indevidas no cartão de crédito ou transferência via PIX.

Mensagens estas, enviadas em horários e dias estratégicos, utilizando técnicas persuasivas da engenharia social. Com o SMS, o truque é mais difícil de ser detectado comparado ao Phishing via e-mail, pois as mensagens são curtas e contêm poucas informações além do próprio link. Abaixo um SMS recebido pelo autor.

MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

Figura 1: Golpe SMS

Fonte: Autoria própria

Importante lembrar, que, qualquer mensagem desse tipo é preciso agir com cautela. Nunca responda a um SMS/mensagem de texto desconhecido ou sequer, clicar em um link.

2.4 A engenharia social

Uma prática conhecida está influenciando centenas de pessoas a revelar informações confidenciais para desconhecidos mediante a importunação, sendo a principal dificuldade da segurança da informação, ultrapassando barreiras tecnológicas onde o principal alvo é o ser humano. Segundo Teixeira (2011), A engenharia social utiliza técnicas persuasivas para obter credibilidade, atacando nas vulnerabilidades da vítima através de manipulações.

Já Braga (2011), traz o conceito detalhado de o que é engenharia social.

> **Engenharia** - Estudo da habilidade de criar, inventar e manipular algo a partir da técnica. **Social** - Tudo aquilo que é relativo à forças externas ao indivíduo, provenientes do meio que este vive, que determinam grande parte do seu comportamento. (BRAGA, 2011, s.p).

A engenharia social não está atrelada diretamente com o virtual, pode-se utilizar outros meios, como, informação por telefone, pessoalmente, entre inúmeras outras formas. Segundo Brignoli e Popper (s.d), O intuito é compilar a maior quantidade de informação, pedindo fracionadamente para diferentes pessoas, até

MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

conseguir montar uma estratégia consistente que realmente surtirá efeito. Fazem uma análise completa do ambiente, estudando as possíveis vítimas, examinando seu comportamento e após possuir tudo mapeado, o engenheiro social parte para o ataque, utilizando de argumentos como a simpatia, proatividade e a premissa principal, é o poder de persuasão.

Por tanto, segundo a UFRGS (2019), tem relação direta com a falta de conhecimento ou a incapacidade dos indivíduos, as pessoas que não se atualizam com o avanço da tecnologia, se tornam alvos fáceis devido a carência de conhecimento. Independentemente, pode-se ter o melhor computador com o melhor sistema de segurança, mas, nada adiantará se não tiver a expertise de identificar as ameaças, pois a tecnologia não atua nas falhas do ser humano.

3 PROCEDIMENTOS METODOLÓGICOS

O presente artigo foi elaborado através do método de pesquisa bibliográfica, segundo Garcia (2016), utiliza-se de fundamentos e embasamento teóricos de obras já publicadas, como, por exemplo, livros, artigos científicos, sites, teses, dissertações, leis entre outros. Que segundo Alves, Oliveira e Souza (2021, p. 65) “tem a finalidade de aprimoramento e atualização do conhecimento”.

Diante da quantidade de informações distorcidas, o autor considerou a utilização do método qualitativo pois conseguirá evidenciar pontos de vistas diferentes sobre o assunto em debate, visando melhor entendimento. “A abordagem qualitativa de um problema, além de ser uma opção do investigador, justifica-se, sobretudo, por ser uma forma adequada para entender a natureza de um fenômeno social” (RICHARDSON, 1999, p. 79). Está pesquisa visa o detalhamento de assuntos complexos, com olhar crítico. Levando em consideração todos os aspectos para dar qualidade e credibilidade no texto, visto que, não analisa dados e sim fatos ou fenômenos.

A pesquisa caracteriza-se como exploratória, segundo Gil (2008), é o método mais indicado para ser utilizado, quando o tema escolhido é pouco explorado, pois,

MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

possibilita a utilização de diversas formas para analisar o problema em questão, fazendo uso de artifícios mais flexíveis.

Referente a coleta e análise dos dados, será feita através de obras já publicadas como referência para solucionar ou mitigar o tema em debate. o autor utilizou um problema recorrente em seu cotidiano, que afeta milhares de pessoas, visto que o mesmo trabalha em uma instituição financeira, e, analisando os questionamentos dos clientes, resolveu fazer uma pesquisa sobre o problema identificado.

4 RESULTADOS E DISCUSSÕES

O setor financeiro no brasil está em constante processo de mudanças e aprimorações tecnológicas, com isso, muitas pessoas não conseguem acompanhar este processo de evolução, ficando submissas a outras para efetuar transações básicas no seu cotidiano tornando-se alvos mais fáceis. Diante destas percepções, pessoas maldosas se aproveitam da falta de conhecimento, oferecendo ajuda ou fazendo gentilezas, para aplicar os golpes.

Segundo levantamento feito pela FEBRABAN (2021), o Brasil vem enfrentando um aumento preocupante na quantidade de golpes. Conforme pesquisas recentes, os números mostram uma curva ascendente no país, apenas nos primeiros 6 meses de 2021 ocorreu um aumento de 165% comparado ao semestre anterior, número este, que se refere apenas à golpes com o uso da engenharia social.

De acordo com Tiinside (2022), os relatórios elaborados pelo laboratório de inteligência e ameaças da empresa, FortiGuard Labs, mapeiam a quantidade de ataques cibernéticos mundial, no ranking de países que sofreram ataques a nível latino-americano, o Brasil ficou em segundo lugar, perdendo apenas para o México. Em 2021 houve um aumento absurdo de 950% nas tentativas de ataques, comparado ao ano anterior. A alta nos números foi constante durante todo o ano e ocorreu em todos os países da região. A seguir o autor elaborou uma tabela ressaltando os dados e informações pesquisadas.

MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

Tabela 9: Ameaças versus habitantes

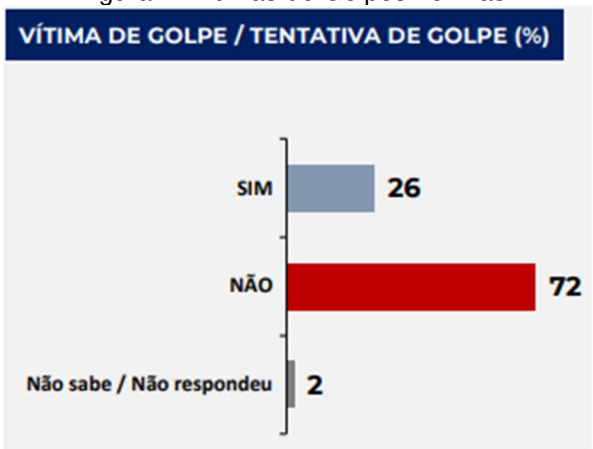
Países	Número de ataques (bilhões) (2021)	Número de habitantes (2020)
México	156,0	128.932.753
Brasil	88,5	212.559.409
Peru	11,5	32.971.846
Colômbia	11,2	50.882.884
Chile	9,4	19.116.209

Adaptado de Tiinside, 2021 e IBGE, 2022

Utilizando os dados da tabela anterior, comparando o número de habitantes versus a quantidade de ataques, utilizando como referência para os habitantes a última divulgação do IBGE (2020) e a quantidade de ataques o ano de 2021, chegamos à estimativa que cada brasileiro recebeu cerca de 416 ameaças cibernéticas apenas no ano de 2021, ou seja, em média, entre uma ou duas por dia.

Um estudo importante feito pela FEBRABAN (2022) traz à tona informações e dados das possíveis vítimas de golpes ou tentativas de golpes registrados no Brasil. Segundo esta pesquisa o maior envolvimento está concentrado em pessoas idosas, 60 anos ou mais, e com renda igual ou superior a 5 salários mínimos. Já o público com menos atingimento são os jovens de 18 a 24 anos. Abaixo, o autor trás os gráficos publicados no Radar Febraban, página que divulga informações relevantes voltadas às informações econômicas dos brasileiros.

Figura 1: Vítimas de Golpes no Brasil



Fonte: RADAR FEBRABAN (2022, p.25)

MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

Figura 2: Vítimas de Golpes no Brasil

(%)	TOTAL	IDADE				INSTRUÇÃO			RENDA FAMILIAR		
		18 A 24 ANOS	25 A 44 ANOS	45 A 59 ANOS	60 ANOS OU MAIS	FUNDA-MENTAL	ENSINO MÉDIO	SUPE-RIOR	ATÉ 2 SM	2-5 SM	+ DE 5 SM
SIM	26	17	26	28	29	23	27	29	23	26	30
NÃO	72	79	73	69	70	75	71	70	74	71	68
Não sabe / Não respondeu	2	4	2	3	1	3	2	1	2	2	2

Fonte: RADAR FEBRABAN (2022, p.25)

Estes dados estão relacionados à base amostral de 3.000 entrevistados, captados nas cinco regiões do Brasil, no período de fevereiro a março de 2022, possuindo uma assertividade de 95% na estimativa.

Diante disso percebe-se que os brasileiros estão expostos à constantes tentativas de divulgação dos seus dados pessoais e financeiros diariamente no país, pois o número de ameaças dos fraudadores a cada indivíduo é muito alto, portanto muitas vezes até as pessoas mais capacitadas e cuidadosas com cliques e cadastros em sites acabam com a correria diária fraquejando e sendo expostas aos ataques cibernéticos, dessa forma é importante que todas as pessoas estejam cada vez mais atentas a telas de celulares e computadores, a cada informação diferente que chegue através de correio eletrônico, sms, sites, nunca clique sem antes investigar na fonte oficial.

Por outro lado, pessoas com baixo conhecimento tecnológico, crianças e idosos que os familiares devem se atentar muito mais, visto que são alvos mais fáceis dos fraudadores conseguirem reverter a ameaça em um efetivo golpe, pela facilidade de acesso à informação devido a curiosidade da criança ou falta de conhecimento tecnológico de um idoso, por exemplo.

O principal meio de defesa para conseguir reduzir a quantidade de casos, é com o conhecimento. Através dele se consegue o melhor entendimento para agir em situações delicadas. Segundo AUDY et al (2005, p.96):

> Conhecimento implica estar ciente e ter o entendimento de um conjunto de informações e como essas informações podem ser úteis para suportar determinado processo ou tarefa, envolvendo uma combinação de instintos, idéias, informações, regras e procedimentos que guiam ações e decisões. O conhecimento é uma informação valiosa da mente humana, que inclui reflexão, síntese e contexto. É difícil de estruturar, difícil de capturar em

> computadores, normalmente é tácito (não explícito) e sua transferência é complexa. (AUDY et al,2005, p.96)

É importante salientar que a sociedade pode e deve procurar a educação digital como meio de prevenção a novos golpes, pois a tecnologia muda constantemente e é de extrema relevância todos estarem sempre com o conhecimento do meio digital apurado para evitar exposição de seus dados pessoais e financeiros. Aliado a essa educação digital, os bancos e instituições financeiras podem contribuir com esta prevenção através de materiais, como, folders e panfletos na abertura de conta e vídeos interativos nas redes sociais, frisando e atualizando os golpes e prevenções, visto que o mesmo é a fonte segura na visão da sociedade.

Segundo Vasconcellos (2017), o avanço tecnológico possui grande participação na exploração do espaço cibernético, pois, criou-se uma dependência nas redes de computadores e na internet. Devido a facilidade, agilidade, armazenamento compacto de dados. Victoria (s.d), complementa, muitas vezes estes ataques não visam recursos econômicos, mas, um desafio pessoal, simplesmente por ego. Uma pessoa anônima efetua diversos ataques para testar os sistemas, afim, de conseguir adentrar ao mesmo. Conseguindo êxito, acarretará diversos problemas, como lentidão no sistema ou até mesmo a paralisação, gerando complicações nas negociações das entidades, sejam elas públicas ou privadas.

Diante das diversas tentativas, torna-se preocupante a recorrência de ataques direcionados ao país, analisando o percentual de aumento na quantidade de golpes e tentativa, o Brasil adotou medidas de segurança mais rígidas para tentar frear essa onda. Criada em 14 de agosto de 2018, A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, entrando em vigência, em 18 de setembro de 2021. No qual, o objetivo é proteger os dados, privacidade e a liberdade dos indivíduos. Tendo em vista a mitigação no vazamento de dados mediante a aplicação das duras penas previstas na lei.

Historicamente, as instituições direcionam a segurança da informação exclusivamente para a área de TI, como responsabilidade exclusiva da área. Um erro comum que ocasiona muitos problemas, pois esta, é muito boa em lidar com os aspectos tecnológicos. Graças aos aprimoramentos e ajustes dos mecanismos de

MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

segurança integrados com a base de dados, atuam com excelência, conseguindo detectar possíveis invasões e agir rapidamente na contenção. Atualmente, detemos de diversas informações confiáveis, como manuais, livros, métodos, no qual orientam as pessoas para o que elas devem ou não acessar, onde, usados corretamente, dificultando a vida dos invasores.

Por mais sofisticado que sejam os golpes, normalmente se aproveitam da falha ou desatenção humana. Segundo Pedroso (2019), o engenheiro social age manipulando instintos essenciais no ser humano, como emoções, sentimentos e ambições, para obter as informações almejadas. Fazendo que a vítima forneça as informações de forma natural, sem desconfiar, usando técnicas de comunicação, áudio visual, chamando a sua atenção e despertando uma necessidade involuntária, tudo isso atrelado a parceria e elogios com argumentos bem fundamentado, leva a interpretações errôneas e acaba fragilizando a diligência da segurança da informação.

Geralmente, os ataques possuem uma ordem cronológica pré-estabelecida que segundo Klettenberg (2016), acontece desta maneira:

> A primeira consiste em reunir os dados sobre as vítimas, perfis e vulnerabilidades relacionadas a elas e ao ambiente no qual estão inseridas. Na segunda etapa, o engenheiro social se aproxima da vítima para estreitar laços, aflorando um sentimento de confiança. Em seguida, os dados obtidos sobre a vítima e o canal de atuação passam a ser explorados e por fim, na quarta etapa, o ataque é executado e as informações sigilosas são obtidas. (KLETTENBERG, 2016. p.68).

O tempo é o aliado dos golpistas, pois, é através dele que consegue manipular os resultados efetivos das suas ameaças. O controle do conjunto de informações alinhado as técnicas persuasivas é uma ferramenta essencial, desta forma os golpistas alisam o perfil das vítimas antes de entrar em contato, para que a abordagem feita através deles sejam o mais próximo possível do estilo de vida e comunicação da vítima, para que esta se sinta confortável com o diálogo, neste momento o golpista já consegue criar uma “intimidade” com o indivíduo, tornando mais fácil o acesso a dados e informações sigilosas para posterior aplicar de fato o golpe.

Conforme normativas internas bancárias, existe uma diferenciação dos termos entre Golpe e Fraude nas instituições financeiras, para que seja possível identificar a

MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

raiz do problema, realizando uma análise da situação que o indivíduo vivenciou para que posteriormente a instituição informe se é possível realizar o ressarcimento do valor perdido pelo seu cliente. Contudo depende se a vítima teve consentimento do envio de dados ou valores (golpe) ou se a vítima teve uma invasão de seus dados perdendo valores sem sua interdição no ocorrido (fraude). Como observa-se na tabela 2 a diferença entre Golpe e Fraude:

Tabela 2: Diferença de Golpe e Fraude

GOLPE	FRAUDE
O responsável por efetuar a transação ou fornecer os dados ao golpista é a própria vítima.	É quando ocorre a transação sem o consentimento ou conhecimento da vítima.
Responsabilidade da vítima.	Responsabilidade da instituição pelo fácil acesso aos dados.
Não ocorre ressarcimento do valor perdido.	Ocorre ressarcimento do valor transacionado ou é passível de ação judicial contra a empresa.
Utiliza-se a engenharia social para conseguir compilar as informações das vítimas.	Os fraudadores hackeiam o acesso aos bancos de dados das empresas. (endereço, cpf, nome completo).
Exemplo: Pagamento de boleto falso, fornecimento de informações pessoais.	Exemplo: Compras indevidas no cartão de crédito.

Fonte: Elaborado pelo autor (2022)

Tendo em vista a tabela apresentada, nota-se que o mais recorrente no Brasil são os golpes, pois o golpista possui mais facilidade em conseguir o dinheiro ou informações sem precisar de um conhecimento amplo tecnológico, visto que a própria vítima fornece os dados ao contrário de fraude que o fraudador consegue acessar dados da vítima através da engenharia social sem que haja o seu consentimento, como clonagem de cartão de crédito.

Em contrapartida, orienta-se que a população siga as dicas de proteção à informação e de seus dados que são fornecidos pelos órgãos do governo, instituições financeiras por meio de comunicação oficial, para que seja dificultado o acesso de terceiros aos dados sensíveis de cada indivíduo. Segundo Neto (2018), por fazerem uso de técnicas mais complexas fica difícil de mapear e intervir antes que o ato aconteça. A forma de abordagem não está relacionada diretamente com a instituição,

MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

não possui mecanismos tecnológicos para agir no combate. A única forma possível para evitar os ataques é através da prevenção, municiar os clientes de conteúdos e informações para mitigar a sua exposição. Atrelado a isto, pode-se elencar diversas formas de prevenção. Baseado em toda a pesquisa elaborou-se uma lista com dicas e cuidados comuns para prevenir-se dos golpes.

- Um exemplo de abordagem para possível golpe que está acontecendo nos dias atuais, são golpistas se identificando aos clientes como funcionários de instituições financeiras informando clientes sobre transações suspeitas realizadas com seus cartões. Assim, transferem o telefonema para uma falsa central de atendimento onde são solicitados dados da conta corrente, do cartão e senhas. Se receber esse tipo de contato desligue, não passe nenhuma informação.
- Ao receber uma ligação ou sms dizendo que há transações suspeitas em seu cartão, não passe informações e vá até uma agência ou entre em contato com seu gerente.
- Ao receber sms com links ou número de telefones, nunca retorne à ligação ou aperte no link, procure sempre o órgão oficial para sanar o possível problema.
- Ao comparecer na agência, nunca aceite ajuda de estranhos, procure sempre tratar estes assuntos com o profissional das instituições financeiras credenciadas.
- Cuidado com o descarte irregular de informações pessoais, como, extrato, fatura do cartão de crédito, comprovantes de depósitos ou transferência.
- Atentar-se ao armazenamento do cartão e senha, nunca os coloque juntos.
- Controle sua ambição e desconfie de ofertas generosas, dinheiro fácil não existe.
- E sempre que possível, oriente seus familiares, principalmente aos mais idosos, sobre os assuntos descritos acima.

MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

Dada a importância da prevenção se faz necessário passar o conhecimento adiante para outras pessoas, para que não sofram o traquejo, pois, o ataque ou as ameaças terão menor eficiência. Se conseguir atingir uma quantidade majoritária de pessoas com o conhecimento estruturado sobre o assunto, automaticamente, o índice de golpes efetivados irá reduzir, de forma que ajude a sociedade como um todo.

5 CONSIDERAÇÕES FINAIS

As mudanças realizadas nos últimos anos com o avanço tecnológico, trouxeram diversos benefícios para a sociedade, mas, difundiram-se novos golpes, com a inovação tecnológica e a proliferação da internet, pessoas maldosas perceberam a oportunidades de desenvolver técnicas possíveis para aplicar virtualmente, onde, antes era restritos somente ao contato físico.

As instituições financeiras deveriam dar uma atenção maior aos seus clientes, municiando-os de informações básicas e como agir em caso recebam algo suspeito em seus dispositivos eletrônicos, disponibilizando as informações de segurança a todos os usuários e não somente estar disponível para quem as procura. a criação de uma mini cartilha de segurança instruindo os procedimentos e alertando caso algo anormal aconteça, procurando sempre as fontes seguras e oficiais para melhor entendimento do ocorrido, sendo entregue junto com o kit de boas-vindas no ato da abertura da conta, e a forma simples e ideal para combates estes golpes.

O presente trabalho apresentou algumas das formas utilizadas para aplicar os golpes financeiros, trazendo características para elucidar a diferença da fraude, juntamente com as medidas de segurança a serem seguidas.

Devido a quantidade de ameaças efetivadas contra o brasil, tornou-se necessário a criação de leis mais rigorosas quanto às punições do uso de dados pessoais sem o consentimento do indivíduo, demandando a intervenção imediata do Direito sobre a regulação de tais práticas.

Visto que a única forma de reduzir a quantidade de casos efetivados, é utilizando o conhecimento. Pelo fato de os golpes não terem relação direta com a base de dados.

REFERÊNCIAS

ALVES, Laís Hilário; OLIVEIRA, Guilherme Saramago de; SOUZA, Angélica Silva de. A pesquisa bibliográfica: princípios e fundamentos. Cadernos da Fucamp, v.20, n.43, p.64-83/2021. Disponível em: < https://webcache.googleusercontent.com/search?q=cache:3FdAHX-eCwsJ:https://www.fucamp.edu.br/editora/index.php/cadernos/article/view/2336/1441+&cd=2&hl=pt-BR&ct=clnk&gl=br>. Acessado em 15/05/2022.

AUDY, Jorge Luís Nicolas; ANDRADE, Gilberto Keller de; CIDRAL, Alexandre. Fundamentos de sistemas de informação. Porto Alegre, Bookman, 2005.

BANCO CENTRAL DO BRASIL – BCB. O que é banco (instituição financeira). Brasília, Distrito Federal, s.d. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/bancoscaixaseconomicas.>. Acessado em: 14/05/2022.

BANCO CENTRAL DO BRASIL – BCB. Estatísticas de Meios de Pagamentos. Brasília, Distrito Federal, s.d. Disponível em:<https://www.bcb.gov.br/estatisticas/spbadendos>. Acessado em: 14/05/2022.

BRAGA, Pedro Henrique da Costa. Técnicas de Engenharia Social. Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2011. Disponível em: < https://securityinformationnews.files.wordpress.com/2014/02/tecnicas_de_engenharia_social.pdf>. Acessado em: 15/05/2022.

BRASIL, LEI Nº 14.155, de 27 de maio de 2021. Brasília, 2021. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acessado em: 13/05/2022

BRASIL, LEI Nº 13.709, de 14 de agosto de 2018. Brasília, 2021. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acessado em: 30/05/2022

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão. O MPF de olho nas pirâmides financeiras: saiba como distinguir um investimento financeiro de um golpe. – Brasília: MPF/2ªCCR, 2016. Disponível em: < http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/cartilhas/guia-pratico-piramides-financeiras>. Acesso em 14/05/2022.

BRASIL sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021. São Paulo, 2022. Disponível em: <https://tiinside.com.br/08/02/2022/brasil-sofreu-mais-de-885-bilhoes-de-tentativas-de-ataques-ciberneticos-em-2021/>. Acessado em: 30/05/2022.

BRIGNOLI, Juliano Tonizetti; POPPER, Marcos Antônio. Engenharia social: Um Perigo Eminente. Instituto Catarinense de Pós-Graduação – ICPG Gestão Empresarial e Estratégias de Informática. Disponível em: <https://www.academia.edu/38720641/ENGENHARIA_SOCIAL_Um_Perigo_Eminente>. Acessado em: 15/05/2022.

COMITÊ GESTOR DE INTERNET NO BRASIL. Cartilha de Segurança para Internet, versão 4.0 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: < https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acessado em 10/05/2022.

DINIZ, Eduardo Henrique. 10 anos de internet banking: desvendando o processo de incorporação de tecnologia em um banco brasileiro através de uma abordagem sociotécnica. Fundação Getúlio Vargas, Escola de administração de empresas de São Paulo. São Paulo, 2006. Disponível em: <https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/13387/10%20Anos%20de%20Internet%20Banking.pdf>. Acessado em 05/05/2022.

ESTRADA, Manuel Martin Pino. A internet banking no Brasil, na América Latina e na Europa. Revista do Programa de Mestrado em Direito do UniCEUB, Brasília, v. 2, n. 1, p. 138-166, jan./jun. 2005. Disponível em: < https://webcache.googleusercontent.com/search?q=cache:fbHDCLw1nr0J:https://www.publicacoesacademicas.uniceub.br/prisma/article/download/185/161+&cd=12&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 07/05/2022.

FEBRABAN - Federação Brasileira de Bancos. Boletos de cobrança. Febraban News. São Paulo, sf. Disponível em: <https://portal.febraban.org.br/pagina/3077/82/pt-br/boletos-de-cobranca#:~:text=O%20boleto%20de%20cobran%C3%A7a%20%C3%A9,a%20este%20produto%20ou%20servi%C3%A7o.>. Acesso em: 14/05/2022.

FEBRABAN - Federação Brasileira de Bancos. Crescem golpes envolvendo manipulação de vítimas para roubo de informações pessoais. Febraban News. São Paulo, 2021. Disponível em: https://portal.febraban.org.br/noticia/3704/pt-br/. Acesso em: 29/05/2022.

FEBRABAN - Federação Brasileira de Bancos. Phishing. Febraban News. São Paulo, sd. Disponível em: < https://febraban.org.br/paginas/81/pt-br/>. Acesso em: 14/05/2022.

FERNANDES, Lucas Barbosa; REIS, Samuel Dornelas de Souza. Detecção, identificação e inferência de conglomerados espaciais de fraudes bancárias em uma

instituição financeira no centro-oeste do Brasil. 2011. 45 f. Monografia (Bacharelado em Estatística) - Universidade de Brasília, Brasília, 2011. Disponível em: < https://bdm.unb.br/handle/10483/3535>. Acesso em: 07/05/20220.

GARCIA, Elias. Pesquisa bibliográfica versus revisão bibliográfica – uma discussão necessária. Revista língua & letras, Volume 17, Número 35. e – ISSN 1981-4755, 2016. Disponível em: < https://webcache.googleusercontent.com/search?q=cache:dapbCsEJlc8J:https://e-revista.unioeste.br/index.php/linguaseletras/article/download/13193/10642/57515+&cd=19&hl=pt-BR&ct=clnk&gl=br>. Acessado em: 15/05/2022.

GIL, Antônio Carlos. Métodos e técnicas de pesquisa social. - 6. ed. - São Paulo: Atlas, 2008. Disponível em: < https://ayanrafael.files.wordpress.com/2011/08/gil-a-c-mc3a9todos-e-tc3a9cnicas-de-pesquisa-social.pdf>. Acesso em: 18/08/2022.

IBGE - Instituto Brasileiro de Geografia e Estatística. Países. Rio de Janeiro, 2022. Disponível em: <https://paises.ibge.gov.br/#/>. Acessado em 30/05/2022

IBM - Internacional Business Machines Corporation. Segurança cibernética do setor bancário. Nova York, EUA. Disponível em: <https://www.ibm.com/br-pt/industries/banking-financial-markets/cyber-security>. Acesso em: 01/05/2022.

Klettenberg, Josiane. Segurança da informação: Um estudo sobre o uso da engenharia social para obter informações sigilosas de usuários de Instituições Bancárias / Josiane Klettenberg; orientador, Angel Freddy Godoy Viera - Florianópolis, SC, 2016. 181 p. Disponível em: < https://repositorio.ufsc.br/bitstream/handle/123456789/172575/343623.pdf?sequence=1&isAllowed=y> . Acesso em 04/06/2022.

MARCHETTI, Renato Zancan; PAVARINI, Sara Cordeiro Coelho; SILVA, Wesley Vieira da. Mobile banking: o impacto das características pessoais do consumidor e dos atributos percebidos da inovação na adoção deste serviço. IV encontro de marketing da ANPAD. Florianópolis – SC, 2010. Disponível em: <http://www.anpad.org.br/admin/pdf/ema356.pdf>. Acesso em: 04/05/2022.

MENDONÇA, Vítor Lobo Arruda de; FURTADO, Estevam de Oliveira. Dinâmica competitiva entre bancos tradicionais e bancos digitais no brasil: uma perspectiva do cliente. Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2020. Disponível em: < http://repositorio.poli.ufrj.br/monografias/monopoli10031105.pdf>. Acesso em: 14/05/2022.

MONTEIRO, Renato Leite. Crimes eletrônicos: uma análise econômica e constitucional. Universidade Federal do Ceará. Fortaleza – Ceará, 2010. Disponível em: < http://www.dominiopublico.gov.br/download/teste/arqs/cp142465.pdf>. Acesso em: 08/05/2022.

NETO, João Araújo Monteiro; PARENTE, Renan Veras. Fraudes tecnológicas bancárias. Trabalho publicado nos Anais do XIX Encontro Nacional do CONPEDI. Fortaleza – CE, 2010. Disponível em: <http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/fortaleza/3869.pdf >. Acessado em: 08/05/2022.

NETO, José Durval Carneiro Campello. Panorama Atual de Smishing no Brasil. Universidade Federal de Pernambuco. Recife, 2018. Disponível em: < https://www.cin.ufpe.br/~tg/2018-2/TG_SI/jdccn.pdf>. Acesso em: 06/06/2022.

PEDROSO, Reinaldo Vitor. Engenharia social: o vínculo mais frágil da segurança. Belo Horizonte, 2019. Disponível em: < https://repositorio.ufmg.br/bitstream/1843/38347/1/Engenharia-Social_O-%20vinculo-mais-fragil-da-seguranca_Reinaldo-Pedroso_GIFES.pdf>. Acesso em: 04/06/2022

PERNAMBUCO. Ministério Público. Assistência Militar e Polícia Civil. Cartilha prevenção a golpes virtuais e presenciais: atitudes para segurança pessoal e de dados. / Redação e texto Sérgio Souza dos Santos; Revisão técnica, André Luiz Freitas Ferreira; [recurso eletrônico]. – Recife: Procuradoria-Geral de Justiça, 2021. Disponível em: < https://www.mppe.mp.br/mppe/attachments/article/14933/Cartilha%20Prevenc%CC%A7a%CC%83o%20a%20Golpes%20Virtuais%20e%20Presenciais%20-%20MPPE.pdf>. Acessado em 11/05/2022.

QUEIROZ, Mariana Pessoa de; ROSA, Nícolas Domingues. Phishing e redes sociais: um estudo de caso. FATEC – Faculdade de Tecnologia de Americana. São Paulo, 2019. Disponível em: < http://ric.cps.sp.gov.br/bitstream/123456789/3780/1/20191S_QUEIROZMarianaPessoade_OD0669.pdf>. Acesso em: 08/05/2022.

RICHARDSON, R. J. Pesquisa social: métodos e técnicas. São Paulo: Editora Atlas, 1999. Disponível em: <https://climatechangemoz.com/wp-content/uploads/2020/04/Metodologia-de-Pesquisa-Social-Richardson.pdf>. Acessado em: 17/05/2022.

SANTOS, Sabrina Oliveira dos. Engenharia social e políticas de segurança da informação no ambiente corporativo. FATEC – Faculdade de Tecnologia de Americana. São Paulo, 2018. Disponível em: < http://ric-cps.eastus2.cloudapp.azure.com/bitstream/123456789/3426/1/20182S_SANTOSSabrinaOliveira_OD0589.pdf>. Acessado em 08/05/2022.

SÃO PAULO, Prefeitura Municipal de Diadema. Boletos falos: alerta do Procon Diadema. Procon Diadema. São Paulo, sd. Disponível em: < http://www.diadema.sp.gov.br/dmp/comunicacao/Comunicacao/Site2/Procon_Boletos%20Falsos.pdf>. Acesso em: 14/05/2022

MERCOSUR en Revista
EDUCACIÓN, TECNOLOGÍA Y SUTENTABILIDAD
ISSN 2957-8388

TEIXEIRA, Lígia. Engenharia social. São Paulo: Fatec, 2011. Disponível em: http://ric.cps.sp.gov.br/bitstream/123456789/1488/1/20111S_TEIXEIRALigia_TCCPD1096.pdf. Acesso em: 04/02/2022.

UFGRS - Universidade Federal do Rio Grande do Sul. Engenharia social (segurança da informação). Porto Alegre, 2019. Disponível em: < https://www.ufrgs.br/dequi/wp-content/uploads/2019/07/Engenharia-Social.pdf>. Acesso em 09/05/2022.

VASCONCELLOS, Alexandre Antônio Urioste. Ameaças cibernéticas à segurança nacional e os impactos nas expressões do poder nacional: um estudo de casos históricos. Rio de Janeiro: ESG, 2017. Disponível em: <ALEXANDRE ANTONIO URIOSTE VASCONCELLOS.pdf (esg.br)>. Acessado em: 30/05/2022.

VICTORIA, Artur. Ataques cibernéticos – síntese. Universidade Autónoma de Lisboa, s.d. Disponível em: < https://www.academia.edu/33983570/Ataques_Cibern%C3%A9ticos_S%C3%ADntese>. Acessado em 30/05/2022.