UNIVERSIDADE FEDERAL DO CEARÁ
INSTITUTO UNIVERSIDADE VIRTUAL
CURSO DE GRADUAÇÃO EM SISTEMAS E MÍDIAS DIGITAIS

MARCOS DOUGLAS ARAÚJO LIMA

SEGURANÇA DA INFORMAÇÃO NA PANDEMIA DE COVID-19 NO BRASIL: A CIBEREDUCAÇÃO COMO MEDIDA PREVENTIVA CONTRA ATAQUES DE PHISHING

FORTALEZA
2022

MARCOS DOUGLAS ARAÚJO LIMA

SEGURANÇA DA INFORMAÇÃO NA PANDEMIA DE COVID-19 NO BRASIL: A CIBEREDUCAÇÃO COMO MEDIDA PREVENTIVA CONTRA ATAQUES DE PHISHING

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas e Mídias Digitais do Instituto Universidade Virtual da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Sistemas e Mídias Digitais.

Orientador: Prof. Dr. Leonardo Oliveira Moreira

FORTALEZA

2022

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

L699s Lima, Marcos Douglas Araújo.
Segurança da informação na pandemica de Covid-19 no Brasil : a cibereducação como medida preventiva contra ataques de phishing / Marcos Douglas Araújo Lima. – 2022.
46 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Instituto UFC Virtual, Curso de Sistemas e Mídias Digitais, Fortaleza, 2022.
Orientação: Prof. Dr. Leonardo Oliveira Moreira.

1. Cibereducação. 2. Cibersegurança. 3. Ciberataque. 4. Segurança da Informação e Prevenção. I. Título.
CDD 302.23

MARCOS DOUGLAS ARAÚJO LIMA

SEGURANÇA DA INFORMAÇÃO NA PANDEMIA DE COVID-19 NO BRASIL: A CIBEREDUCAÇÃO COMO MEDIDA PREVENTIVA CONTRA ATAQUES DE PHISHING

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas e Mídias Digitais do Instituto Universidade Virtual da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Sistemas e Mídias Digitais.

Aprovada em:

BANCA EXAMINADORA

Prof. Dr. Leonardo Oliveira Moreira (Orientador)
Universidade Federal do Ceará (UFC)

Profa. Dra. Raquel Santiago Freire
Universidade Federal do Ceará (UFC)

Prof. Dr. Robson Carlos Loureiro
Universidade Federal do Ceará (UFC)

À minha família e à minha estrelinha Wanessa Marília

AGRADECIMENTOS

A Deus por ter me dado saúde, força e perseverança para superar as dificuldades.

Agradeço ao meu orientador Prof. Dr. Leonardo Oliveira Moreira por aceitar conduzir o meu trabalho de pesquisa.

Ao Doutorando em Engenharia Elétrica, Ednardo Moreira Rodrigues, e seu assistente, Alan Batista de Oliveira, aluno de graduação em Engenharia Elétrica, pela adequação do *template* utilizado neste trabalho para que o mesmo ficasse de acordo com as normas da biblioteca da Universidade Federal do Ceará (UFC).

Aos bibliotecários da Universidade Federal do Ceará: Francisco Edvander Pires Santos, Juliana Soares Lima, Izabel Lima dos Santos, Kalline Yasmin Soares Feitosa e Eliene Maria Vieira de Moura, pela revisão e discussão da formatação utilizada neste *template*.

A todos os meus professores do curso de Sistemas e Mídias Digitais da Universidade Federal do Ceará pela excelência da qualidade técnica de cada um.

A minha família, pelo amor e apoio incondicional, que me impulsionou ao longo de toda a minha trajetória.

A minha querida companheira Ana Vitória Santos Silva, que foi uma grande parceira ao meu lado, não medindo esforços para que eu chegasse até esta etapa da minha vida. Sem você, tudo seria mais difícil.

Também agradeço a todos os meus colegas de curso, pela oportunidade do convívio e pela cooperação mútua durante estes anos.

A todos os mestres que contribuíram de alguma forma com a minha formação, seja acadêmica, profissional ou pessoal.

“A mente que se abre a uma nova ideia jamais voltará ao seu tamanho original.”

(Albert Einstein)

RESUMO

As Tecnologias da Informação e da Comunicação mudaram o nosso cotidiano, alterando os paradigmas do modo de funcionamento da sociedade. A informação se valoriza e passa a ser então, um dos principais produtos para a Sociedade do Conhecimento. Novos espaços de liberdade são gerados com a evolução da tecnologia. Porém a liberdade exacerbada acaba por transformar o ambiente gerador de conhecimento em um espaço de risco à segurança. Em um mundo digitalizado devido a pandemia do coronavírus, os ciberataques reacendem se aproveitando do momento de fragilidade, colocando em risco não somente a privacidade dos usuários como sua liberdade e segurança. Para tanto, o presente trabalho teve como objetivo principal analisar o papel da cibereducação como medida preventiva aos ciberataques de phishing e para isto, utilizamos a metodologia de investigação que se desenvolve ao longo três eixos ou etapas, tomando como base o método de investigação desenvolvido por Quivy e Campenhoudt (1998), utilizando-se da pesquisa exploratória, analisando exemplos que estimulassem a compreensão a fim de apresentar os conceitos básicos necessários para que se possa entender o problema e objetivo de pesquisa como da pesquisa não-experimental onde foram aplicadas observações no intuito de tirar conclusões a partir de um conteúdo teórico reunido. Permitindo assim, discutir os desafios que o ciberespaço nos coloca em meio a um cenário de pandemia, analisar o Brasil diante desta crise de segurança, propor formas de prevenção e mitigação de danos para os ataques de *phishing*, além de apresentar a cibereducação como uma solução de prevenção, levantando uma discussão sobre sua eficiência para a proteção do usuário. Usando os processos anteriores como base, foi possível chegar a conclusão de que a cibereducação pode vir a ser uma eficiente solução para a prevenção do usuário mediante o seu constante desenvolvimento e incentivo ao usuário ao consumo e transmissão de saberes permitindo aos usuários conhecerem o meio ao qual estão inseridos, seus riscos e como se prevenir.

Palavras-chave: Cibereducação. Cibersegurança. Ciberataque. *Phishing*. Segurança da Informação e Prevenção.

ABSTRACT

Information and Communication Technologies have changed our daily lives, changing the paradigms of the way society works. Information is valued and then becomes one of the main products for the Knowledge Society. New spaces of freedom are generated with the evolution of technology. However, the exacerbated freedom ends up transforming the knowledge-generating environment into a space of security risk. In a digitalized world due to the coronavirus pandemic, cyberattacks rekindle taking advantage of the moment of fragility, putting at risk not only the privacy of users but their freedom and security. Therefore, the present work had as main objective to analyze the role of cybereducation as a preventive measure against phishing cyberattacks and for this, we used the research methodology that develops along three axes or stages, based on the research method developed by Quivy and Campenhoudt (1998), using exploratory research, analyzing examples that stimulate understanding in order to present the basic concepts necessary to understand the problem and research objective as well as non-experimental research where observations were applied in the in order to draw conclusions from a theoretical content gathered. Thus, allowing us to discuss the challenges that cyberspace poses in the midst of a pandemic scenario, analyze Brazil in the face of this security crisis, propose ways to prevent and mitigate damages for phishing attacks, in addition to presenting cybereducation as a solution of prevention, raising a discussion about its efficiency for the protection of the user. Using the previous processes as a basis, it was possible to conclude that cybereducation can become an efficient solution for user prevention through its constant development and encouragement to the user to consume and transmit knowledge, allowing users to know the environment at which they are inserted, their risks and how to prevent them.

Keywords: Cybereducation. Cybersecurity. Cyberattack. Phishing. Information Security and Prevention.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CERT	Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CGI.br	*Comitê Gestor da Internet no Brasil*
CISA	*Cybersecurity and Infrastructure Security Agency*
CVE	*Common Vulnerabilities and Exposures Explained*
DDoS	*Distributed Denial of Service*
ENISA	*European Union Agency for Cybersecurity*
FBI	*Federal Bureau of Investigation*
NIC.br	*Núcleo de Informação e Coordenação do Ponto BR*
PIN	*Personal Identification Number*
SQL	*Structured Query Language*
TI	Tecnologias de Informação
TICs	Tecnologias da Informação e da Comunicação
URL	*Uniform Resource Locator*
XSS	*Cross-Site Scripting*

SUMÁRIO

1 INTRODUÇÃO

A popularidade das aplicações web aumentou, principalmente nestes tempos de pandemia, onde serviços de comércio, alimentação, educação e outros segmentos tiveram que se servir de ambientes web no intuito de manterem seus serviços em operação mesmo diante das restrições e do isolamento social (NASCIMENTO *et al.*, 2021). Com isso, muitos segmentos conseguiram fazer com que suas empresas, instituições e pequenos empreendimentos não fossem totalmente interrompidos, diminuindo desempregos e o fechamento dos empreendimentos (NASCIMENTO *et al.*, 2021). Ademais, Jahromi *et al.* (2020) preveem que o volume de aplicações web, seja para uso pessoal e comercial, continuará a aumentar.

O vírus SARS-CoV2 surgiru em Wuhan na China no final do ano de 2019 e se espalhou rapidamente para outras províncias chinesas e outros países (LI *et al.*, 2020; SANTOS *et al.*, 2020). Muitos países tomaram como medidas como o isolamento e o distanciamento social para mitigar a proliferação do vírus (SMALING *et al.*, 2022). Com isso, a população teve que fazer um maior uso dos serviços *online* em diversos seguimentos, tais como: *delivery* de alimentos, *telemarketing*, comércio eletrônico em geral (*e-commerce*), internet *banking* etc. Diante disso, muitos comércios e indústrias acabaram sendo afetados pela pandemia e chegaram até a paralisar suas atividades (SANTOS, 2022). Além dos problemas sociais e econômicos impactados pela pandemia, o uso massivo das Tecnologias da Informação e da Comunicação (TICs) culminaram em uma maior ocorrência dos ciberataques ou ataques cibernéticos (SALEOUS *et al.*, 2022).

Saleous *et al.* (2022) apresentam que dados do *Federal Bureau of Investigation* (FBI), durante a pandemia, os crimes cibernéticos aumentaram 400%. A Interpol também informou que os crimes cibernéticos aumentaram durante a pandemia de COVID-19 (SALEOUS *et al.*, 2022). Segundo (CUZZOCREA *et al.*, 2018) o ataque por *phishing* é um método destinado a imitar sites oficiais de qualquer organização, empresa, bancos, redes sociais, institutos etc. O objetivo do *phishing* é roubar credenciais privadas de usuários, como nome de usuário, senhas, número *Personal Identification Number* (PIN) ou quaisquer detalhes de cartão de crédito etc. O ataque de *phishing* é o mais comum e usado de várias maneiras para atacar o usuário-alvo (RIPA *et al.*, 2021). Geralmente, o meio mais comum de se propagar ataques de *phishing* é por *hiperlinks* embutidos em conteúdos de e-mail (CUZZOCREA *et al.*, 2018). Ao clicar nesses tipos de *hiperlinks*, a vítima é redirecionada para um site malicioso que permitirá o roubo de suas credenciais pessoais.

A segurança da informação não depende apenas da tecnologia, mas da forma como seus usuários empregam essa mesma tecnologia para gerir a informação. Nesse contexto, urge a necessidade de educar o usuário para uma melhor utilização das novas ferramentas. O conhecimento sobre o funcionamento e como a informação é processada permite reduzir os riscos e aumentar o nível de segurança da informação. Assim, surge a cibereducação como uma modalidade de ensino que consciencializa dos perigos da Internet e especifica o agrupamento de métodos para formação, práticas, comportamentos e tipos de conhecimento que se desenvolvem com o crescimento das TICs (LIMA, 2012).

Diante do quadro abordado, este estudo tem por objetivo analisar a atuação da cibereducação como medida preventiva contra ataques de *phishing*. Contudo, para atingir o objetivo proposto será necessário verificar o atual cenário de Segurança da Informação, como investigar o ciberataque de *phishing* e engenharia social no Brasil durante a pandemia de COVID-19, para então apresentarmos a cibereducação como medida de prevenção ao ciberataque.

1.1 Delimitação do Tema

A cibereducação pode ser uma aliada para prevenir que pessoas sejam vítimas de ciberataques, em particular, ataques de *phishing* diante do uso massivo das TICs durante a pandemia de COVID-19 no Brasil.

1.2 Definição do Problema

Gil (2002) apresenta algumas regras práticas para formulação de problemas científicos: deve ser elaborada como uma pergunta; deve ser o mais detalhado possível; e utilizar termos claros e sem ambiguidades. Neste sentido, pode-se definir o problema científico, que norteia este trabalho, com a seguinte pergunta: “Como a cibereducação pode conscientizar as pessoas sobre os ataques de *phishing* diante do uso massivo das TICs durante a pandemia de COVID-19 no Brasil?”.

1.3 Objetivos

O objetivo geral deste trabalho é analisar a atuação da cibereducação como medida preventiva contra ataques de *phishing* durante a pandemia de COVID-19 no Brasil. Segundo Marconi e Lakatos (2003) os objetivos específicos ou secundários almejam, de um lado, atingir o

objetivo geral e, de outro, aplicá-los a situações particulares. Assim, alcançar o objetivo geral, os seguintes objetivos específicos foram elencados:

a) explorar o cenário atual de segurança da informação;
b) investigar os ciberataques de *phishing* no Brasil durante a pandemia de COVID-19; e
c) discutir como a cibereducação pode ser uma medida de prevenção aos ataques de *phishing*.

1.4 Estrutura da Monografia

O restante deste documento está organizado da seguinte forma: O Capítulo 2 apresenta todo o arcabouço teórico e conceitual que permeiam este trabalho, envolvendo a cibereducação, ciberataques, pandemia de COVID-19 e um detalhamento sobre os ciberataques de *phishing*. Já o Capítulo 3 elenca, apresenta e discute os trabalhos correlatos ao trabalho proposto neste ensaio. O Capítulo 4 descreve os métodos de pesquisa utilizados neste ensaio e detalha as etapas que foram realizadas no decorrer da pesquisa. Uma análise discursiva sobre o impacto da cibereducação como medida preventiva contra ataques de *phishing*, durante a pandemia de COVID-19 no Brasil, é apresentada no Capítulo 5. Por fim, o Capítulo 6 destaca as conclusões do trabalho e elenca alguns trabalhos futuros que podem ser realizados a partir do estado atual desta pesquisa.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo reúne todo arcabouço teórico e conceitual necessários para um melhor entendimento e compreensão deste trabalho. Neste sentido, são apresentados conceitos básicos sobre o ciberespaço e segurança da informação, os perigos que rondam o ciberespaço como sua alta crescente na pandemia de COVID-19 e a necessidade de assegurar a proteção dos dados dos usuários.

2.1 Ciberespaço

A difusão de um ciberespaço como um meio de comunicação instrumentalizado pela informática e pela internet, incorporou rapidamente novos usuários e dispositivos, bem como a digitalização de novos serviços e atividades. E os computadores, tornam-se mais e mais pervasivos, ubíquos e conectados com o novo espaço.

É possível encontrar muitas definições de ciberespaço. Para Lévy (2000) é um "(...) espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores". Ainda afirma que:

> Essa definição inclui o conjunto dos sistemas de comunicação eletrônicos (aí incluídos os conjuntos de redes hertzianas e telefônicas clássicas), na medida em que transmitem informações provenientes de fontes digitais ou destinadas à digitalização. Insisto na codificação digital, pois ela condiciona o caráter plástico, fluido, calculável com precisão e tratável em tempo real, hipertextual, interativo e, resumindo, virtual da informação que é, parece-me, a marca distintiva do ciberespaço.

Percebemos que, para Lévy (2000), o termo especifica algo além da infraestrutura material da comunicação digital, que remonta todo o universo de informações que ele abriga. O termo ciberespaço foi cunhado pelo norte-americano William Gibson em suas obras literárias, ganhando notoriedade em Neuromancer, publicado no ano de 1984. A partir disso se espalhou nos círculos profissionais e acadêmicos, recebendo diferentes definições (KELLNER, 2001).

O elemento ciber foi extraído da palavra cibernética para a formação de novas palavras. Cibernética provém do grego kybernetikê e significa a ciência de governar. Nesse sentido, o físico Norbert Wiener cunhou, nos anos 40, o termo cibernética como a ciência do controle, comunicação e cognição. A partir daí, o prefixo "ciber-" passou a referenciar diversos termos relacionados ao domínio da computação e das "máquinas inteligentes" (CASCAIS, 2001). Para Gibson (2003), o ciberespaço é:

> Uma alucinação consensual vivida diariamente por bilhões de operadores autorizados, em todas as nações, por crianças aprendendo altos conceitos matemáticos... Uma representação gráfica de dados abstraídos dos bancos de dados de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz abrangendo o não-espaço da mente; nebulosas e constelações infindáveis de dados. Como marés de luzes da cidade.

Koepsell (2004) vai contra o ponto de vista do ciberespaço além da infraestrutura de Lévy (2000), afirmando que o ciberespaço é físico, fundamentado em uma realidade material que se desenvolveu junto com os computadores:

> Um meio composto de chips de silício, fios de cobre, fitas e discos magnéticos, cabos de fibra óptica e de todos os outros componentes de computadores, meios de armazenamento e redes que armazenam, transmitem e manipulam bits. [...] O software existe no ciberespaço como o texto existe no papel ou como uma estátua existe em pedra (KOEPSELL, 2004).

O autor Gómez (2012) cita a definição do Departamento de Defesa dos Estados Unidos da América, que considera o ciberespaço como:

> Um domínio global dentro do ambiente da informação que consiste em uma rede interdependente de infraestruturas de Tecnologias de Informação (TI), incluindo as redes de Internet, telecomunicações, sistemas de computador e processadores embutidos e controladores (GÓMEZ, 2012).

Podemos então entender o ciberespaço como aquilo que se refere tanto a *Internet*, envolvendo toda a infraestrutura de seu funcionamento, quanto ao espaço que ela gera. Porém o ciberespaço é, antes de tudo, um ambiente de informação. É composto de dados criados, armazenados e compartilhados. Um novo mundo, um novo espaço de significações, um novo meio de interação, comunicação e de vida em sociedade (SINGER; FRIEDMAN, 2014).

O ciberespaço, como este novo meio social de liberdade, atrai diariamente diversos curiosos para o meio, tanto de boa como de má índole, visto a anonimidade garantida pelo sistema. Para tanto, urge a necessidade de manutenção da privacidade e proteção de dados de seus usuários, surgindo então novas áreas de conhecimentos para suprir esse déficit, como exemplo a segurança da informação.

2.2 Segurança da Informação

O termo "segurança" abrange diversas interpretações. O conceito deriva do latim securitas, e implica em prevenir ou eliminar qualquer tipo de risco na vida. Segundo Cepik (2001), segurança é "uma condição relativa de proteção na qual se é capaz de neutralizar ameaças

discerníveis identificáveis contra a existência de alguém ou de alguma coisa". Implica na qualidade ou no estado de estar seguro, sendo algo estável e indubitável como também uma necessidade.

A definição já estabelecida anteriormente também se torna válida para o digital, visto que sua finalidade consiste em garantir à informação a proteção necessária. O termo Segurança da Informação designa o novo conhecimento que salvaguarda o conteúdo presente no ciberespaço de acessos indevidos, modificações não autorizadas ou mesmo sua não disponibilidade (PEIXOTO, 2006). A norma ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2013) estabelece que:

> A segurança da informação também é definida por meio de três pilares: a integridade, que se relaciona com a fidedignidade e totalidade da informação bem como sua validade; a disponibilidade, que se relaciona com a disponibilidade da informação quando exigida pelo processo de negócio hoje e no futuro; e a confidencialidade,que está relacionada com a proteção de informações confidenciais para evitar a divulgação indevida.

Figura 1 – Pilares da Segurança da Informação

Fonte: DEB SOLUTIONSTI (2015).

Acrescido dos três pilares anteriores há ainda uma responsabilidade final, o não repúdio e autenticidade, que tem como objetivo verificar a identidade e autenticidade a fim de

garantir a integridade de origem. Tais pilares garantem ao precioso ativo que é a informação, a prevenção ou a impossibilidade de serem modificados, pervertidos, copiados ou eliminados, assim, perpetuando o dado em sua forma original (PEIXOTO, 2006). Segundo a Associação Brasileira de Normas Técnicas (ABNT), a informação precisa ser protegida, pois:

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

A ABNT também define, por meio da norma ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2013), a segurança da informação, como a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco e maximizar o retorno sobre os investimentos, sendo garantida a partir da implementação de controles adequados, tanto virtualmente quanto fisicamente

A segurança é assegurada por lei, mas ainda há muitos empecilhos entre a proteção total do usuário e os males presentes no mundo virtual. Para alcançar tal estado indubitável que é a segurança, torna-se necessário um aprofundamento nos perigos que nos rodeiam, para então traçar contramedidas de segurança e prevenção, assim, permitindo não só entidades protegerem seus usuários como garantir que o próprio indivíduo possa se proteger dos ciberataques.

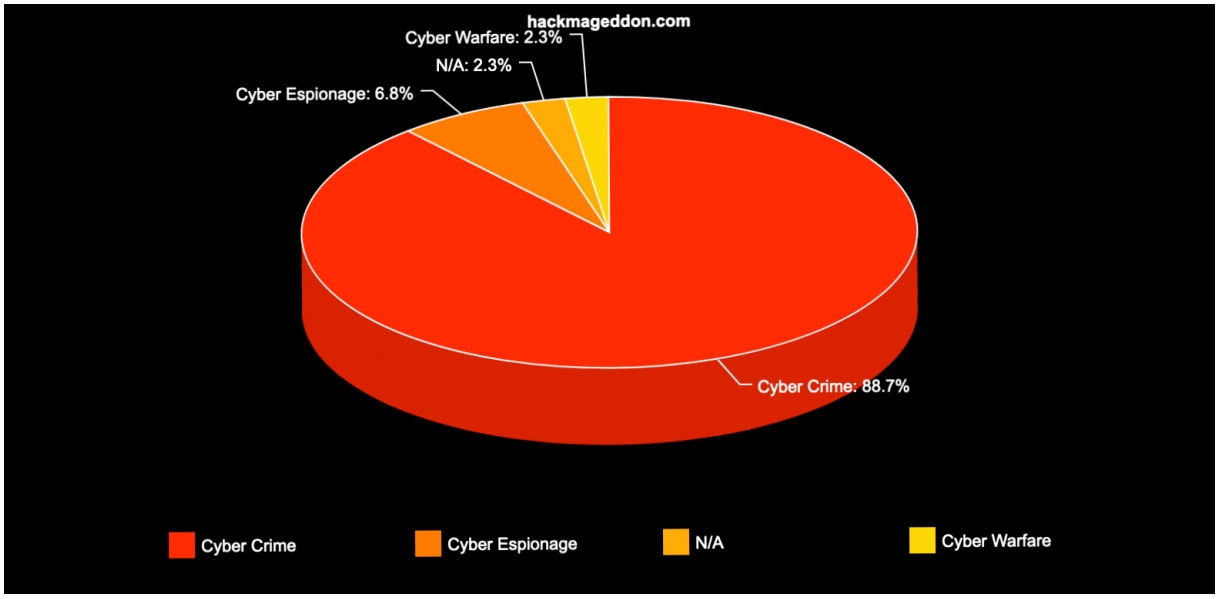
2.3 Ciberataque

O rápido acesso às informações e aumento da conectividade possibilitaram uma grande difusão de informações, incluindo o surgimento de usuários entusiastas pela cultura hacker de resolução de problemas ou obstáculos. Invasões de redes de computadores e captura ilegal de dados tornaram-se ações corriqueiras, mas que tiveram um grande avanço nos últimos cinco anos (MALWAREBYTES, 2021).

Um ciberataque é um conjunto de ações dirigidas contra sistemas de informação. Os alvos mais comuns são usuários que desconhecem o valor da informação ou que possuem privilégios especiais. Com o objetivo de prejudicar pessoas, instituições ou empresas, estes tipos de ações podem atentar tanto contra os equipamentos e sistemas que operam na rede como contra bases que armazenam informação (OLIVEIRA, 2019).

Segundo o Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores (CERT), as tentativas de invadir sistemas para adquirir, roubar, criptografar e bloquear o acesso tem objetivos que variam da simples diversão até a realização de ações criminosas (CERT.BR, 2012).

Figura 2 – Motivações de ataques cibernéticos 2021



Fonte: HACKMAGEDDON (2021).

Os títulos do adversários variam de acordo com a suas motivações: *hackers*, hacktivistas, ciberterroristas, cibercriminosos e ciberguerreiros são alguns deles. Para entender como proteger uma rede, é útil também saber o que motiva essas pessoas a atacar sistemas de computador.

Os *hackers* são muitas vezes motivados pela necessidade de notoriedade. Buscam envergonhar alguém ou mostrar ao mundo o quão inteligentes eles são. Normalmente, eles não causam danos graves. Os *hackers* muitas vezes tentam enganar as pessoas para que lhes forneçam diretamente dados de acesso (TRAILHEAD, 2019).

Os hacktivistas é um *hacker* ativista que têm como alvo uma organização específica porque são motivados por posições políticas, sociais ou morais. Um grupo hacktivista age como indivíduos em busca de um objetivo comum e pode se concentrar na negação de serviço, perda de reputação ou roubar dados confidenciais. Um dos maiores exemplos de hacktivistas é o grupo *hacker Anonymous* que realiza protestos e outras ações, muitas vezes com o objetivo de promover a liberdade na Internet e a liberdade de expressão (TRAILHEAD, 2019).

Ciberterroristas causam perturbações ou danos contra um governo ou seu povo, por

meio de computadores, redes ou mesmo pelos dados armazenados neles para atingir objetivos ideológicos, resultando em danos destrutivos (físicos, mentais, ambientais etc.) tanto para as pessoas quanto para a infraestrutura crítica (MANAGE ENGINE, 2020).

Os cibercriminosos são motivados pelo dinheiro, tem como objetivo dados privados que permitam de alguma forma obter lucro. Tendem a ir atrás de empresas e não em indivíduos específicos, pois eles desejam obter a maior quantidade de dados possíveis, para poder utilizá-las, vendê-los ou alavancá-los de alguma maneira para ganhar dinheiro (JUSBRASIL, 2020).

Os ciberguerreiros são pessoas que se envolve em uma guerra cibernética motivados pelos interesses nacionais, pessoais ou por crença patriótica ou religiosa. A guerra cibernética pode ser praticada para defender os sistemas de computador e de informação ou para atacá-los (DEFINIRTEC, 2021) .

Os hackers éticos trabalham para proteger as empresas contra ataques digitais. Hackers éticos são treinados para descobrir fraquezas e reportar a uma organização para que ela possa se proteger contra invasores indesejados (TRAILHEAD, 2019).

Vale ressaltar a doutrina brasileira, por meio da Lei n. 12.737, de 30 de novembro de 2012, a qual dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências, específica, em seu Art. 154-A, os crimes cometidos por meios informacionais:

> Art. 154-A. Invadir dispositivos informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismos de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (BRASIL, 2012).

Estabelece também, pena de detenção de três meses a um ano e multa para quem produz, oferece, distribui, vende ou difunde dispositivos ou programas de computadores que tem por objetivo permitir a prática da conduta criminosa. Se a invasão resultar na obtenção de conteúdo, a pena de reclusão repercute em seis meses a dois anos e multa. Se tornando ainda mais grave se a prática atingir um órgão da administração pública municipal, estadual ou federal.

Conhecer as motivações de um invasor pode ajudar as organizações a se concentrarem no que proteger e em como proteger, mas conhecer os ataques também é de grande importância. Apesar dos ataques cibernéticos se adaptarem ao meio e às novas tecnologias e novos métodos surgirem a todo instante com os cibercriminosos que buscam contextualizar seus ataques em eventos e assuntos em alta de momento para direcionar melhor o ataque e obter maior êxito em

seus crimes. Os conceitos bases, referentes aos ataques cibernéticos, perpetuam mesmo com a evolução da tecnologia.

2.4 Tipos de Ciberataque

Nesta seção será apresentado os ciberataques que já se consolidaram na rede e que já vem ameaçando a segurança do indivíduo no ciberespaço por vários anos. Partiremos pelo mais conhecido que é o vírus de computador e passaremos por outros ataques como *Structured Query Language* (SQL) *injection*, *phishing*, ataques de negação de serviço e *Cross-Site Scripting* (XSS).

Vírus ou *malware* é uma classe de software malicioso que é bem parecido com o vírus biológico. Infecta o sistema operativo e programas, com o intuito de comprometer o desempenho ou os dados do dispositivo. Para este efeito, os vírus procuram manter-se indetectáveis, tornando o aparelho mais vulnerável, visto que um dispositivo comprometido por *malware* pode ser usado por criminosos cibernéticos para diversos fins. Entre eles, roubar dados confidenciais, usar o computador para realizar outros atos criminosos ou causar danos aos arquivos que contém informação (AVAST, 2017).

SQL *Injection* é um tipo de ataque usado para encontrar vulnerabilidades no banco de dados, permitindo a um atacante o roubo de informação (incluindo senhas e dados de cartões de crédito), ou ainda, incluir por exemplo, conteúdos não desejados num determinado sistema (AVAST, 2017).

Phishing é um ataque que consiste no envio de e-mails de spam ou outras formas de comunicação que são enviadas em massa com a intenção de induzir os destinatários a fazer algo que prejudique a segurança deles ou a segurança da organização em que trabalham. Os ataques de *phishing* geralmente são usados para revelar informações pessoais, como *passwords*, códigos de cartão de crédito, ou número de contas bancárias (KASPERSKY, 2019).

Os ataques de negação de serviço, ou *Distributed Denial of Service* (DDoS), visam derrubar sites ou redes inteiras sobrecarregando-as com tráfego proveniente de milhares de computadores infectados. Os sites de bancos, de notícias e até de governos são os principais alvos de ataques de DDoS (AVAST, 2017).

XSS permite a um atacante inserir códigos maliciosos em páginas e aplicativos que seriam confiáveis, e utilizá-los como suporte de dados ocultos, instalando *malwares* nos navegadores dos visitantes. Com XSS, os *hackers* visam disseminar *malwares* para o máximo de

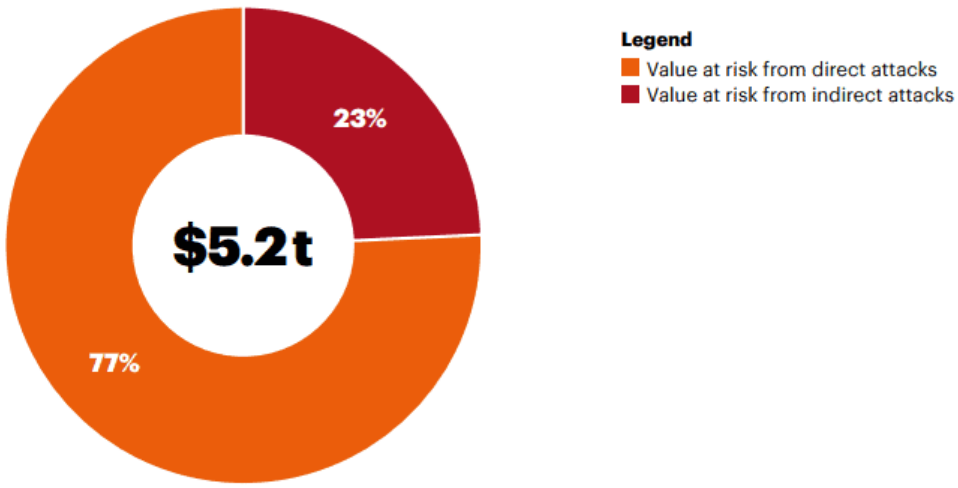
visitantes possíveis (AVAST, 2017).

Percebemos que o perigoso arsenal de ciberataques disponíveis aos cibercriminosos é demasiadamente extenso e que continua se desenvolvendo. A todo momento, os malfeitores buscam usuários inexperientes, pois estes se apresentam mais vulneráveis aos tipos de ataques, pois não possuem nenhuma educação de como se comportar em uma sociedade em rede.

A Verizon, empresa especializada em telecomunicações, observou que cerca de 93% de todos os *malwares* chegam aos nossos computadores por e-mail, e o *phishing* sendo o número um de ataque de engenharia social. O *Phishing* foi responsável por cerca de 80% de todos os incidentes relatados. Porém existem muitas outras fontes de vulnerabilidade para as quais as empresas de hoje não estão preparadas. Há cerca de 181.088 problemas exploráveis listados pelo Banco de dados comum de vulnerabilidades a *Common Vulnerabilities and Exposures Explained* (CVE) (VERIZON, 2019).

O relatório da Accenture, empresa multinacional de consultoria de gestão e tecnologia da informação, especulou que nos anos de 2019 a 2024, o total de perdas sofridas por crimes cibernéticos poderia chegar a cerca de US$ 5.2 trilhões. Notavelmente, a Accenture também descobriu que o *malware* foi o tipo de ataque que mais custou para ser superado. O preço de lidar com *malware* aumentou 11%, enquanto o custo de ataques internos mal-intencionados de dentro da empresa aumentou 15% (ACCENTURE SECURITY, 2019).

Figura 3 – Valor global para os risco de ataques cibernéticos diretos e indiretos



Fonte: ACCENTURE SECURITY (2019).

Diante dos dados apresentados, percebemos que o cenário de ciberataques já apresentava um crescimento constante e a pandemia do COVID-19 tornou-se o estimulo para impulsionar

as práticas ilícitas dos atacantes permitindo assim, o alto crescimento na quantidades de ciberataques, não só no Brasil como também em todo o Mundo, visto que proporcionou tanto uma alta crescente de novos usuários como novos alvos para esses predadores digitais.

2.5 Ciberataques na Pandemia de COVID-19

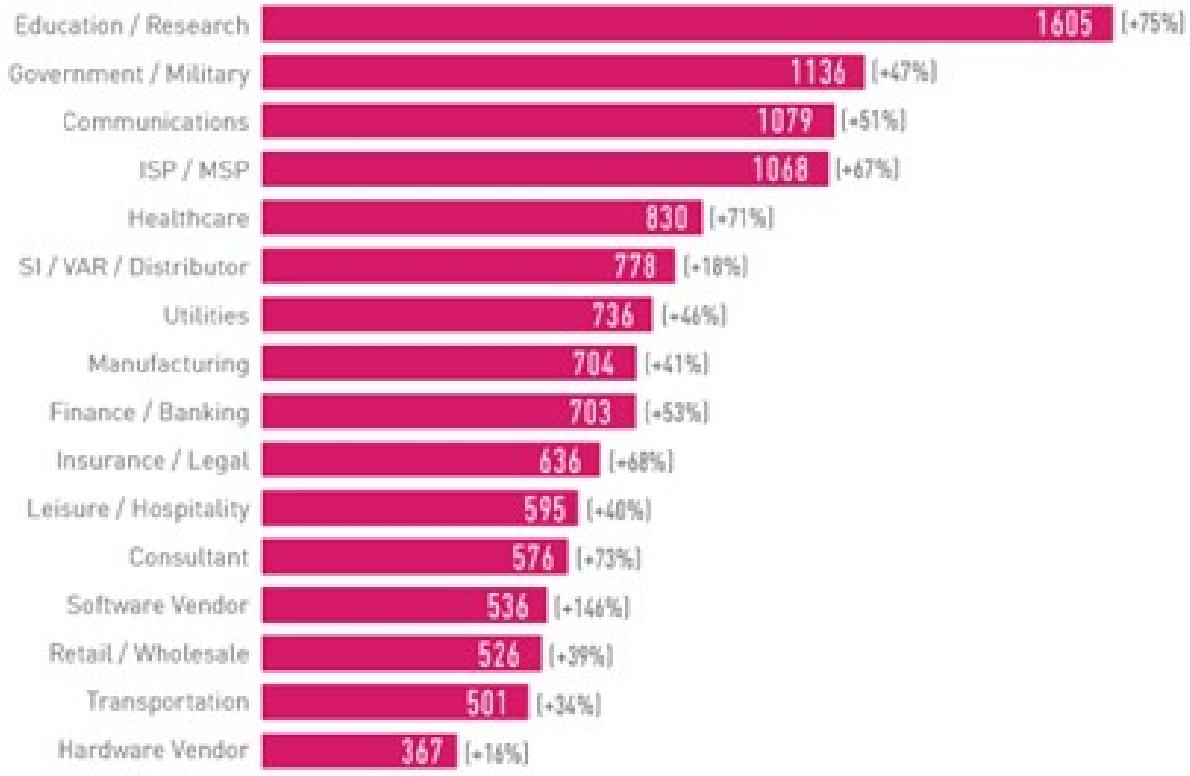
A pandemia de COVID-19 obrigou milhares de pessoas a mudarem seu comportamento para novos hábitos, sendo o catalisador para alavancar o uso da tecnologia para o que é hoje, o principal meio de comunicação de nossa sociedade. Com essa mudança, novos riscos e vulnerabilidades surgiram e segundo a Computerworld, a tendência é que tudo isso continuará a crescer durante os próximos meses ou até mesmo nos próximos anos (COMPUTERWORLD, 2021). A cibersegurança nunca teve tanta importância quanto nos últimos tempos, com a crescente de ataques e ameaças durante a pandemia e as brechas de segurança abertas pelo teletrabalho. Os atacantes veem a situação atual como uma oportunidade e, portanto, a conscientização da necessidade de investir cada vez mais em cibersegurança também aumentou, especialmente no mundo corporativo (MELO, 2020).

A pesquisa anual de cibersegurança da Check Point em 2020 apontou que organizações em todo mundo estavam no meio de uma onda massiva de ataques cibernéticos no primeiro trimestre. A pesquisa revelou que 58% dos profissionais de segurança de TI afirmaram que sua organização experimentou um aumento nos ataques cibernéticos desde o início do surto COVID-19. Descobriu-se ainda que proteger trabalhadores remotos será uma das principais prioridades e desafios nos próximos anos, já que cerca de metade das organizações acredita que o local de trabalho não retornará às normas pré-pandêmicas. Além disso, houve um aumento de aproximadamente 300% no número de registro de domínios com relação às vacinas do COVID-19, sendo 29% deles suspeitos de envolvimento com algum tipo de golpe (CHECK POINT SOFTWARE TECHNOLOGIES, 2020).

Outra empresa de pesquisa e consultoria em segurança da informação, a CyberEdge Group, entrevistou 1.200 profissionais e tomadores de decisão da área entre 2019 e 2020, todos empregados em empresas com mais de 500 funcionários em 17 países. A principal constatação do estudo é que os ataques parecem ser cada vez mais frequentes: 35% das empresas relataram ter sido vítimas de ataques efetivos, que não foram detidos pelas defesas da organização e atingiram seu alvo, pelo menos seis vezes ao longo de 12 meses.

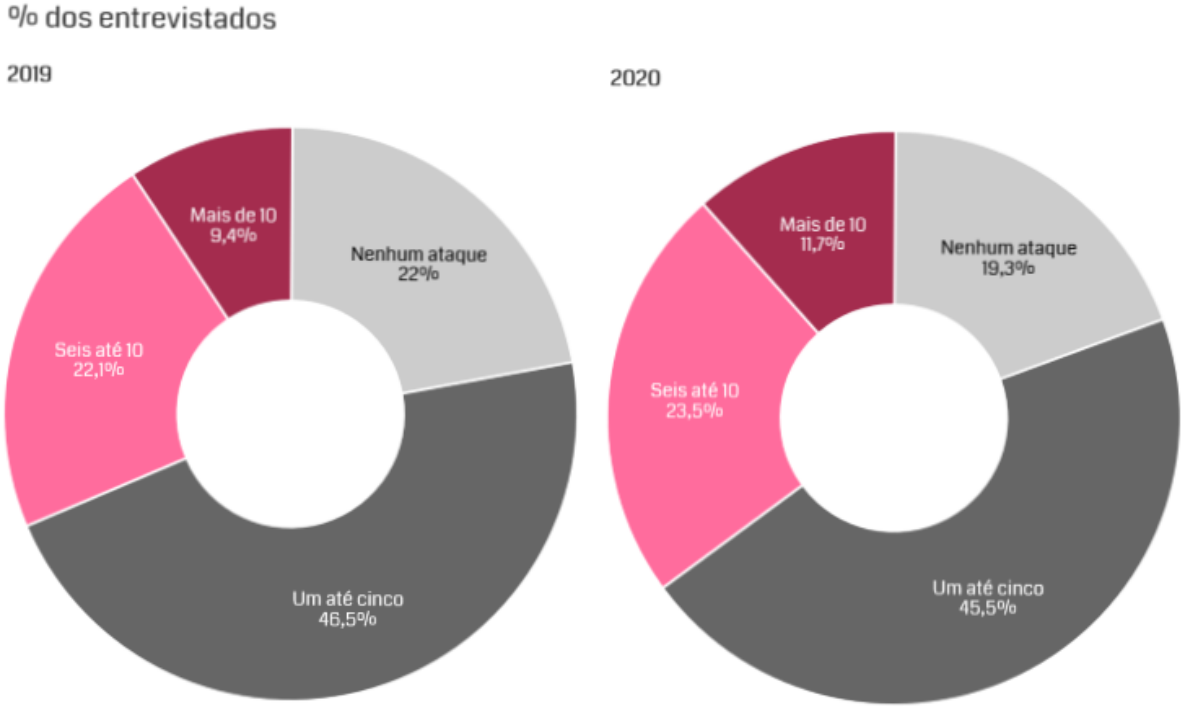
O volume de ciberataques cresceu 23% no Brasil de janeiro a agosto, em comparação

Figura 4 – Média de ataques semanais por organização, por setor, em 2021 em comparação com 2020



Fonte: CHECK POINT SOFTWARE TECHNOLOGIES (2022).

Figura 5 – Quantidade de ciberataques sofridos ao longo de 12 meses



Fonte: CYBEREDGE GROUP (2020).

com o mesmo período do ano anterior. Os dados são do Panorama de Ameaças 2021 da Kaspersky, estudo anual feito pela equipe de pesquisa e análise da empresa na América Latina.

Ao todo, a empresa de antivírus contabilizou 2.107 ataques por minuto dos principais 20 *malwares* na região. O Brasil é o maior alvo, com 1.395 tentativas de infecção por minuto, seguido por México (299 bloqueios/min), Peru (96 bloqueios/min), Equador (89 bloqueios/min) e Colômbia (87 bloqueios/min). Dmitry Bestuzhev, diretor da equipe de pesquisa e análise da Kaspersky na América Latina, afirma que:

> Quando analisamos os bloqueios realizados por nossas tecnologias, identificamos famílias de *malware* que nos permitem dizer que os internautas latino-americanos procuram as ameaças, pois são disseminadas por meio da pirataria de programas. (BESTUZHEV, 2021).

A pesquisa também indica que os ataques de *phishing* (mensagens fraudulentas) estão diminuindo. Mesmo assim, o Brasil detém a primeira colocação na região com 15,4% dos internautas registrando tentativas desse ataque.

A segurança da informação está em constante mudança, pois é diretamente associada à evolução tecnológica, visto que, em várias situações, a proteção também se associa com a tecnologia. Porém, mesmo em ambientes virtuais impenetráveis, os usuários se configuram como um elo vulnerável. Tendo em vista o comportamento humano, somos mais suscetíveis para a ocorrência de incidentes tanto na situações rotineiras, como pela falta de conhecimento sobre como agir ou mesmo pelo risco e grau de responsabilidade, tornando o fator humano e suas ações uma vulnerabilidade bastante explorada pelas ameaças de Sistemas de Informação (CARNEIRO; ALMEIDA, 2013).

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis (MITNICK; SIMON, 2003).

Ano após ano no país, a crescente preocupação com segurança da informação foi sendo notada e, em decorrência disso, surgiram novas leis como a Crimes Cibernéticos (Lei 12.737/12), o Marco Civil (Lei 12.965/14) e, mais recentemente, a Lei Geral de Proteção de Dados (Lei 13.709/18), que há pouco entrou em vigor.

É de elevada relevância consignar que o artigo 2º, inciso II, da Lei 12.965/14, o chamado Marco Civil da Internet, delimita a disciplina do uso da Internet no Brasil assentada igualmente nos fundamentos dos direitos humanos. Logo nos primeiros artigos da Carta Magna brasileira, precisamente o artigo 5º, encontra-se disposto os direitos e deveres individuais e coletivos. Para que sejam dissipadas quaisquer dúvidas sobre as implicações do direito à privacidade na Internet, a Lei 12.965/14, no artigo 3º, inciso II, estabelece que a disciplina do uso da internet no Brasil tem como princípio a proteção da privacidade (ARAÚJO, 2017). A educação tecnológica vem com o objetivo de preparar o usuário para uma vivência dentro da rede de tal forma que consiga assegurar a proteção de seus dados e direitos enquanto imerso.

Para tanto, ensinar os usuários a manipular de forma adequada os sistemas de informação é fundamental. Saber da existência dos perigos existentes na Internet, possibilita ao usuário se prevenir, buscando meios para se proteger no meio virtual, seja por softwares e sistemas livres ou pela ajuda de terceiros que comercializam essa proteção. Contudo o usuário, considerado o elo fraco em todas as etapas da vivência no ciberespaço, deve buscar a educação para então ter um alto controle sobre espaço, aumentando a eficácia de todos os outros mecanismos de segurança, assegurando sua proteção.

3 TRABALHOS RELACIONADOS

Este capítulo apresenta e discute alguns trabalhos relacionados à cibereducação como medida preventiva aos ataques de *phishing*, destacando a contribuição deste presente ensaio.

Existem vários trabalhos relacionados a medidas de *anti-phishing* por meio de *frameworks* e softwares a serem aplicados, como treinamentos e capacitações, mas ainda há um déficit quando se trata da prevenção por meio da educação do indivíduo fora do mundo corporativo.

De acordo com Carvalho e Marques (2017), a cibereducação é essencial para o sucesso na consciencialização e ação política no que diz respeito à cibersegurança. Em seu trabalho, apresenta a cibereducação como uma verdade absoluta no quesito de prevenção ao cibercrimes, sem a comprovação por meio dados que denotam sua eficiência, além disso, apresenta um compêndio das principais ofertas formativas na área da cibersegurança existente nas principais Universidades e Institutos Superiores de referência de Portugal. Concluindo com a afirmação de que a cibereducação é uma competência que deve ser lecionada na atividade formativa de cada cidadão, sendo de responsabilidade do Estado na capacitação do indivíduo.

Podila *et al.* (2020) apresentam como adolescentes são alvos mais vulneráveis aos ciberataques, evidenciando como esses jovens possuem baixo nível de conhecimento de segurança cibernética, surgindo a necessidade de desenvolver uma mentalidade de segurança cibernética para identificar ameaças, mitigá-las ou preveni-las. Para tanto, o trabalho apresenta uma abordagem formativa para treinar os alunos a identificar novas ameaças na prática, utilizando ciberataques conhecidos a fim de avaliar jovens no processo de identificação de ameaças à segurança cibernética. O trabalho acaba por se limitar ao público alvo e não se aprofunda no básico para o usuário saber para garantir a segurança na rede, submeter o indivíduo a esses ataques é uma boa metodologia de aprendizagem visto que em experiências futuras ele saberá como se comportar, porém acaba por se tornar mais um "aponta o erro e mostra a solução", se não levarmos em consideração o fator emocional do usuário nessas situações.

Abroshan *et al.* (2021) expõem que os efeitos das emoções humanas e comportamento durante a COVID-19 impactam diretamente nas taxas de vítimas do ataque de *phishing*. Ainda mostra em seus estudos que pessoas com níveis educacionais mais baixos tendem a ser mais suscetíveis ao *phishing*, porém pessoas que tiveram mais educação correm maior risco de serem vítimas de *phishing* durante o surto. Este estudo torna-se importante porque explica como as emoções e o comportamento dos indivíduos são influenciados pelo COVID-19, indo em

contrapartida ao nosso ponto principal, visto que, mesmo pessoas mais capacitadas ainda são propícias a serem vítimas dos ataque de *phishing* expondo que o acompanhamento psicológico também torna-se necessário para a etapa de prevenção.

Szarvák *et al.* (2021) evidênciam como interfaces móveis, que geralmente se apresentam de forma simplificada, reduzem a oportunidade de identificar ataques cibernéticos, já que ocultam informações importantes e, se o usuário não estiver suficientemente ciente ou estável emocionalmente, impossibilitam o reconhecimento de pontos chaves que indicam ameaça. Este trabalho apresenta um panorama dos ataques de *phishing* durante a pandemia principalmente em dispositivos móveis, mas com foco no design das interfaces. Apresenta soluções governamentais contra os ataques de *phishing*, mas que acabam se tornando somente uma forma de mitigar os dados do que prevenir, visto que essas campanhas apenas apontam o erro e mostram a solução, não levando em consideração o fator emocional que pode ser fundamental para a garantia da proteção do usuário.

Apesar de abordarem conteúdos relacionados à cibersegurança e ataque de *phishing* possuem temas distintos entre si, mas que acabam convergindo para o mesmo ideal, no qual apresentam a educação como uma das principais medidas de proteção do indivíduo. Os trabalhos acima citados possuem, individualmente, questionamentos a serem sanados, mas em conjunto, nos apresentam um panorama do que pode ser feito, como acabar por induzir novas reflexões, acerca da prevenção da proteção do indivíduo em meio cibernético

De acordo com os quatro trabalhos, vemos que induzir o indivíduo a conscienciali-zação sem levar em conta os aspectos sociais e psicológicos em sua educação, acabamos por apenas preparar uma solução momentânea para mitigar os danos. Em um cenário de crise como a pandemia do coronavírus, no qual há o esgotamento mental, a falta de informações válidas, uma rápida digitalização, sem preparo, de todos os meios e a perda de pessoa próxima, permitiram uma alta crescente nos ciberataques, já que o indivíduo deixa de lado seu lado crítico, geralmente por descuido e desatenção, em busca de meios que garantam o seu bem estar e a de seus conhecidos, mostrando que não é apenas uma consciencialização momentânea que resolveria isso, mas uma educação sólida, preparando o usuário para que possa prevenir e remediar tais ataques à sua segurança digital. A Tabela 1 sumariza a comparação entre os trabalhos correlatos e o presente trabalho.

Os trabalhos foram de grande importância pois não somente apresentaram novas óticas sobres os ciberataques e cenário da segurança da informação durante a pandemia, como

Tabela 1 – Comparativo entre os Trabalhos Relacionados e a Contribuição deste Trabalho

Trabalho	**Citação**	**Sobre**	**Comparativo**
Cibereducação como medida preventiva no combate ao Cibercrime	Carvalho e Marques (2017)	Apresentam a cibereducação como uma medida preventiva, mas falha em não apresentarem sua atuação e eficiência ao combate ao cibercrime.	Apresentamos a cibereducação, sua atuação e efetividade por meios teóricos e campanhas de conscientização.
Practice-Oriented Smartphone Security Exercises for Developing Cybersecurity Mindset in High School Students	Podila *et al.* (2020)	O trabalho apresenta uma abordagem mais formativa que se limita ao público alvo. Expõem superficialmente os ataques durante os testes de treinamento.	Tivemos uma abordagem mais ampla na qual aprofundamos um único tipo de ciberataque, assim apresentando soluções mais concisas para a prevenção.
COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic	Abroshan *et al.* (2021)	Apesar de apresentarem uma nova ótica acerca do ataques de *phishing*, principalmente durante a pandemia, não se aprofunda nos métodos de prevenção nem nos ataques existentes.	Aprofundamos teoricamente os ataques de *phishing*, apresentando soluções e medidas eficientes para diminuição do sucesso desses ataques.
Simplification on mobile devices reduces personal (cyber) safety	Szarvák *et al.* (2021)	Apresentam uma abordagem mais limitada aos dispositivos móveis, ao se aprofundarem nas limitações do design de interfaces dos *smartphones*. Apresentam superficialmente o conjunto de soluções implementadas pela União Europeia.	Abordamos os ataques em diversos tipos de dispositivos, apresentando soluções baseadas nas campanhas de conscienciaização europeias como também às existentes em nosso país.

Fonte: elaborado pelo autor.

também forneceram questionamentos que puderam ser discutidos em nossos resultados. Permitindo assim, enriquecer nosso trabalho, já que levamos em consideração o que tinha sido abordado anteriormente por esses trabalhos traçando soluções concisas como forma de sanar não somente nossos objetivos, como também complementar o que foi proposto pelos outros autores. Assim, todos os trabalhos convergem para a ideia de que da educação como uma das melhores soluções para o tratamento, prevenção e eliminação dos riscos criados pelos ciberataques.

4 METODOLOGIA

Cabe a um objetivo de pesquisa vislumbrar uma ou mais hipóteses de trabalho e, segundo Wazlawick (2009), visa uma forma de demonstrar que a hipótese elaborada é verdadeira. Para tanto, o presente trabalho teve como objetivo principal analisar o papel da cibereducação como medida preventiva aos ciberataques de *phishing* e para isto, utilizamos a metodologia de investigação que se desenvolve ao longo três eixos ou etapas, tomando como base o método de investigação desenvolvido por Quivy e Campenhoudt (1998):

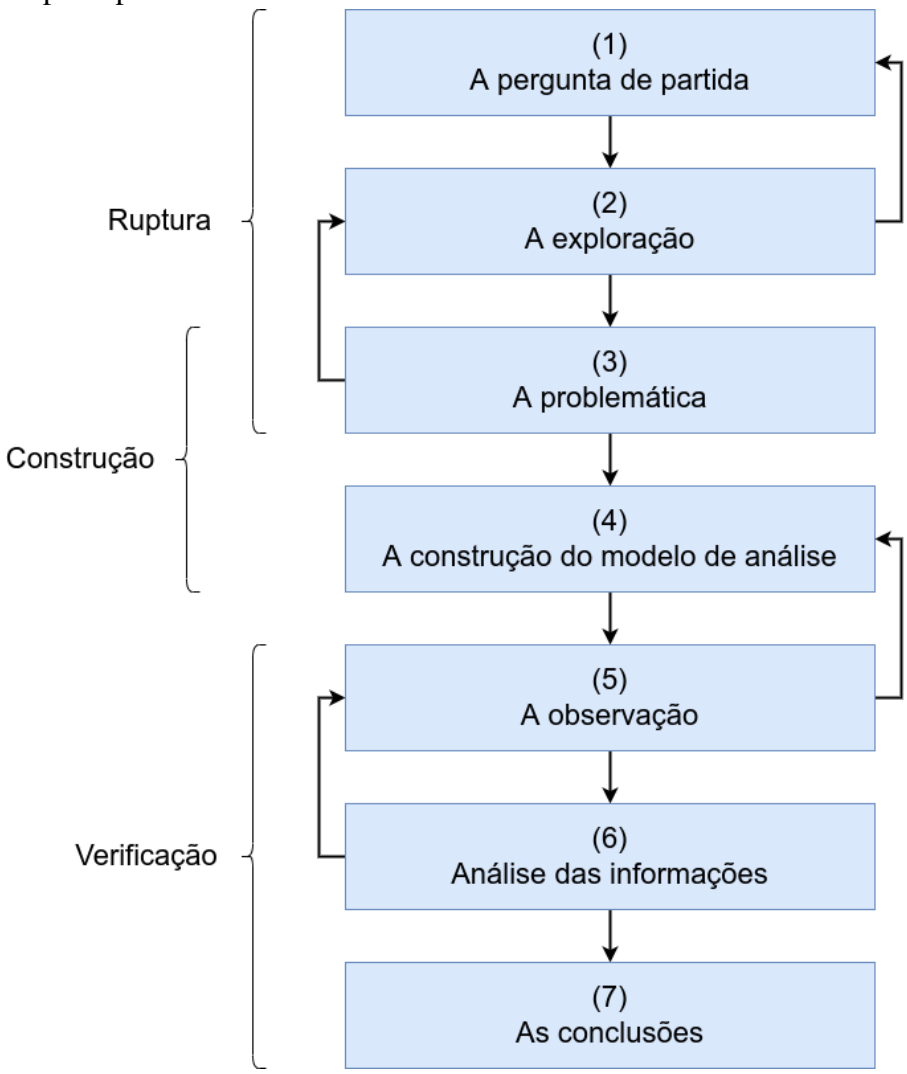
a) O projeto inicia pelo primeiro eixo denominado Ruptura, que consiste em romper com as ideias preconcebidas e com as falsas evidências e ilusão de compreender as coisas;
b) No segundo eixo, a Construção, desenvolvemos propostas explicativas do objeto em estudo com as operações necessárias a serem colocadas em prática e os resultados esperados ao final da pesquisa. As propostas explicativas foram o produto de um trabalho racional fundamentado numa lógica e num sistema conceitual validamente constituído;
c) Por fim a Constatação ou verificação, na qual a proposta de pesquisa é suscetível de ser verificada por informações da realidade concreta.

As etapas e os procedimentos metodológicos supracitados podem ser observados, de forma gráfica, na Figura 6. Em relação aos aspectos de caracterização e natureza, se fundamenta na pesquisa exploratória e não-experimental, visto a sua função principal de revelar determinados aspectos do material de estudo, permitindo assim, completar as pistas de trabalho sugeridas pelas leituras. Segundo Gil (2002) grande parte das pesquisas exploratórias envolvem:

a) Levantamento bibliográfico;
b) Entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado;
c) Análise de exemplos que estimulem a compreensão.

As partes de pesquisas exploratórias, apresentadas por Gil (2002), estão atreladas aos eixos discutidos por Quivy e Campenhoudt (1998). Neste trabalho, a natureza da pesquisa exploratória foi utilizada como forma de analisar os materiais reunidos, como também exemplos que estimulassem a compreensão a fim de apresentar os conceitos básicos necessários para que se possa entender o problema e objetivo de pesquisa, além de descrever, com maiores detalhes, os ataques e riscos à segurança da informação, o cenário de ciberataques durante o período da pandemia e formas de se precaver. A segunda etapa da metodologia se serviu da pesquisa exploratória para reunir todo arcabouço teórico e os conhecimentos necessários para o entendimento do presente estudo.

Figura 6 – Etapas e procedimentos



Fonte: Adaptado de Quivy e Campenhoudt (1998).

A pesquisa de natureza não-experimental consiste no estudo sem a intervenção sistemática do pesquisador, observando e tirando conclusões a partir de um arcabouço teórico levantado (WAZLAWICK, 2009). Neste trabalho, utilizou-se a pesquisa não-experimental para aplicar observações no intuito de tirar conclusões a partir de um conteúdo teórico reunido (WAZLAWICK, 2009). Portanto, a pesquisa não-experimental compreende as etapas da metodologia que refletem uma discussão sobre os aspectos técnicos dos ataques de phishing e seu cenário durante a pandemia do coronavírus, elencado durante a etapa exploratória, como também propostas de soluções que possam prevenir ou eliminar os riscos a esse tipo de ataques.

Assim, a terceira e última etapa da metodologia, investiga os fenômenos em toda a sua complexidade e em contexto natural, ou seja, analisamos a informação encontrada, a fim de chegar às conclusões, constatando assim, por meio de uma pesquisa não-experimental, os resultados obtidos e a discussão realizada (BOGDAN; BIKLEN, 1994).

5 RESULTADOS

Este capítulo discute como a cibereducação pode ser uma medida de prevenção aos ataques de *phishing* durante a pandemia de COVID-19 no Brasil, como resultado desta pesquisa.

Seguindo a metodologia de Quivy e Campenhoudt (1998), com a finalização dos dois primeiros eixos, formamos um arcabouço teórico por meio de levantamentos bibliográficos mediante a pesquisa de natureza exploratória que está presente em nosso Referencial Teórico e que não só nos possibilita apresentar os resultados obtidos, como também realizar uma discussão técnica do cenário dos ataques de *phishing* no Brasil. Diante da pandemia de COVID-19, apresentaremos os ataques mais comuns nesse período e seus riscos como soluções contra esse tipo de ataque além de levantar uma discussão sobre eficiência da cibereducação como uma solução preventiva contra os ataques de *phishing*.

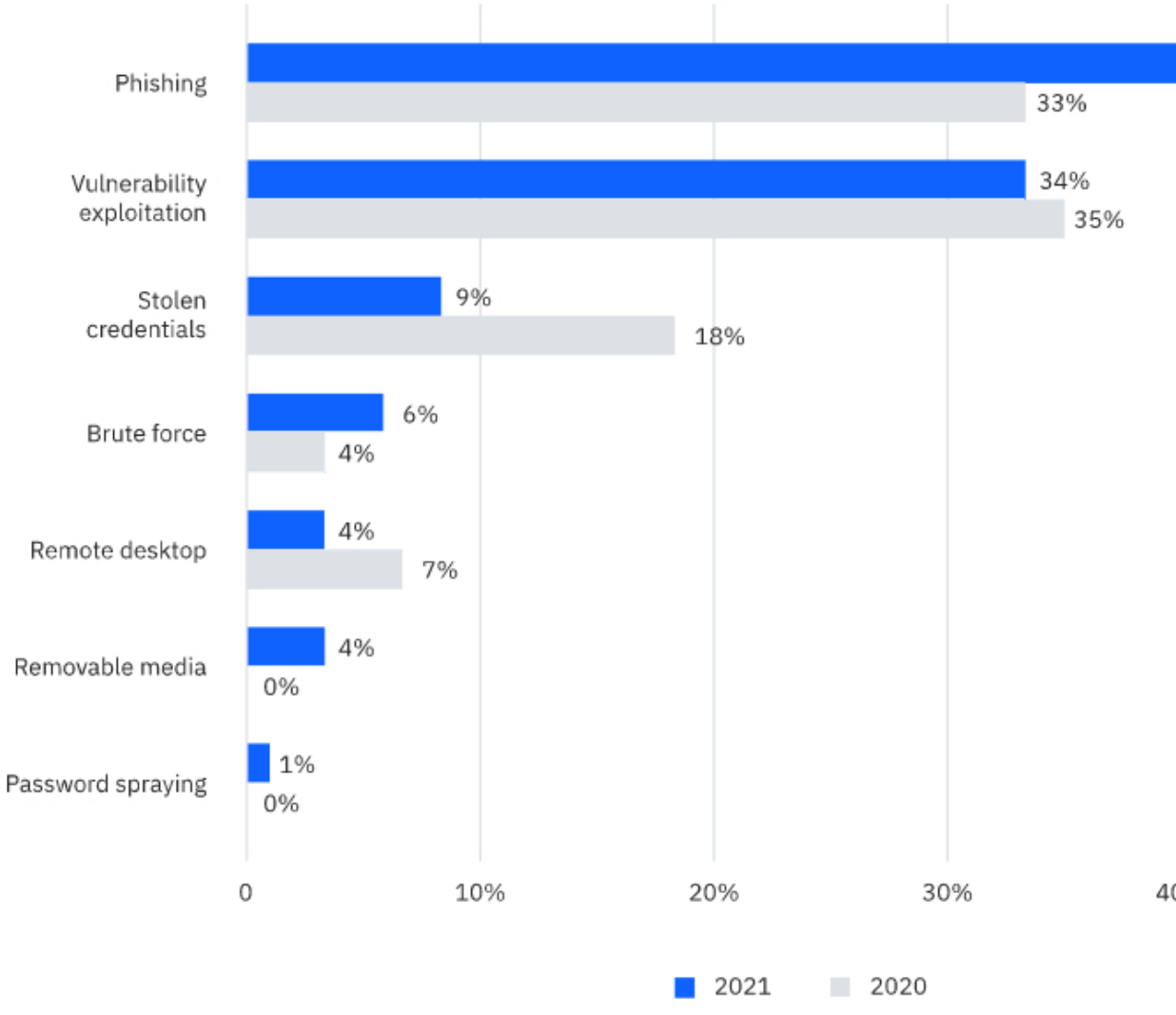
Os ataques de *phishing* acontecem por meio de e-mails, telefonemas ou mensagens de texto por alguém posando como outra pessoa ou instituição legítima visando atrair indivíduos para fornecer dados confidenciais. O destinatário é induzido a clicar em um *link* malicioso ou a preencher um formulário que pode levar à instalação de algum tipo de vírus, que permite o congelamento do sistema, como parte de um ataque de *ransomware* ou a revelação de informações confidenciais. A Figura 7 ilustra um exemplo de mensagem falsa usada em ataque de *phishing*.

Figura 7 – Exemplo de mensagem falsa usada em ataque de *phishing*

Fonte: TECHTUDO (2018).

Embora esse truque de engenharia social exista há mais de 25 anos, os ataques de *phishing* ainda estão em ascensão e continuam a ser um risco real. Esses ataques tiveram uma alta crescente durante a pandemia 2020, principalmente no Brasil. O auxílio financeiro fornecido pelo estado como a rápida digitalização, sem preparo, de nossa sociedade passa ser um grande chamariz para a prática maliciosa. De acordo com resultados de análises divulgados pela IBM X-Force Incident Response and Intelligence Services (IBM, 2020), pelo menos 693 sites maliciosos relacionados à COVID-19 e ao auxílio emergencial foram criados no Brasil. O relatório da IBM também mostra que o *phishing* está evoluindo; tornando os ataques mais difíceis de identificar e evitar, sendo apontado como o principal vetor de infecção como vemos na figura 8 que exibe um gráfico dos principais vetores de infecção entre os anos de 2020 e 2021.

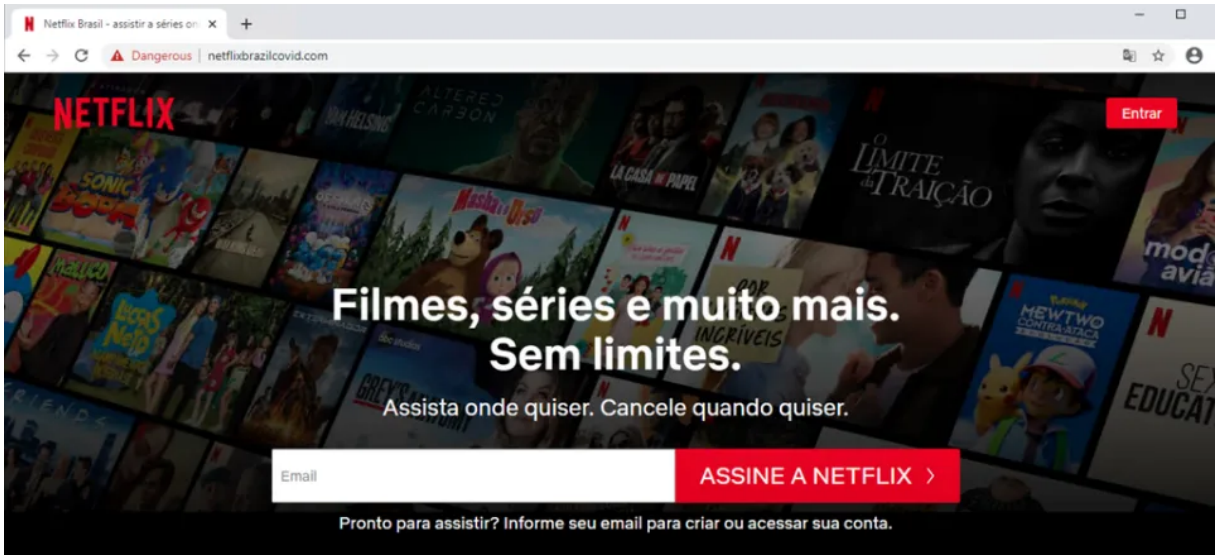
Figura 8 – Principais vetores de infecção, 2020 e 2021



Fonte: IBM (2022).

O *typosquatting* é uma técnica muito utilizada para o *phishing* na qual os atacantes registram uma versão mal escrita de uma nome de domínio de uma empresa legítima, como vemos na figura 9. Esses nomes de domínio são usados para clonar ou encenar páginas da web, executar golpes de e-mail, bem como distribuir *malware*, prejudicando significativamente a reputação da marca e a confiança do consumidor. Tornou-se comum no início da digitalização dos bancos, em que pessoas compravam domínios similares e criavam páginas espelhadas, fazendo com que o cliente digitasse seus dados pessoais, e também durante a pandemia com páginas referentes ao auxílio do governo ou de informações relacionadas a saúde e a pandemia.

Figura 9 – Exemplo de *typosquatting* que aconteceu durante a pandemia.

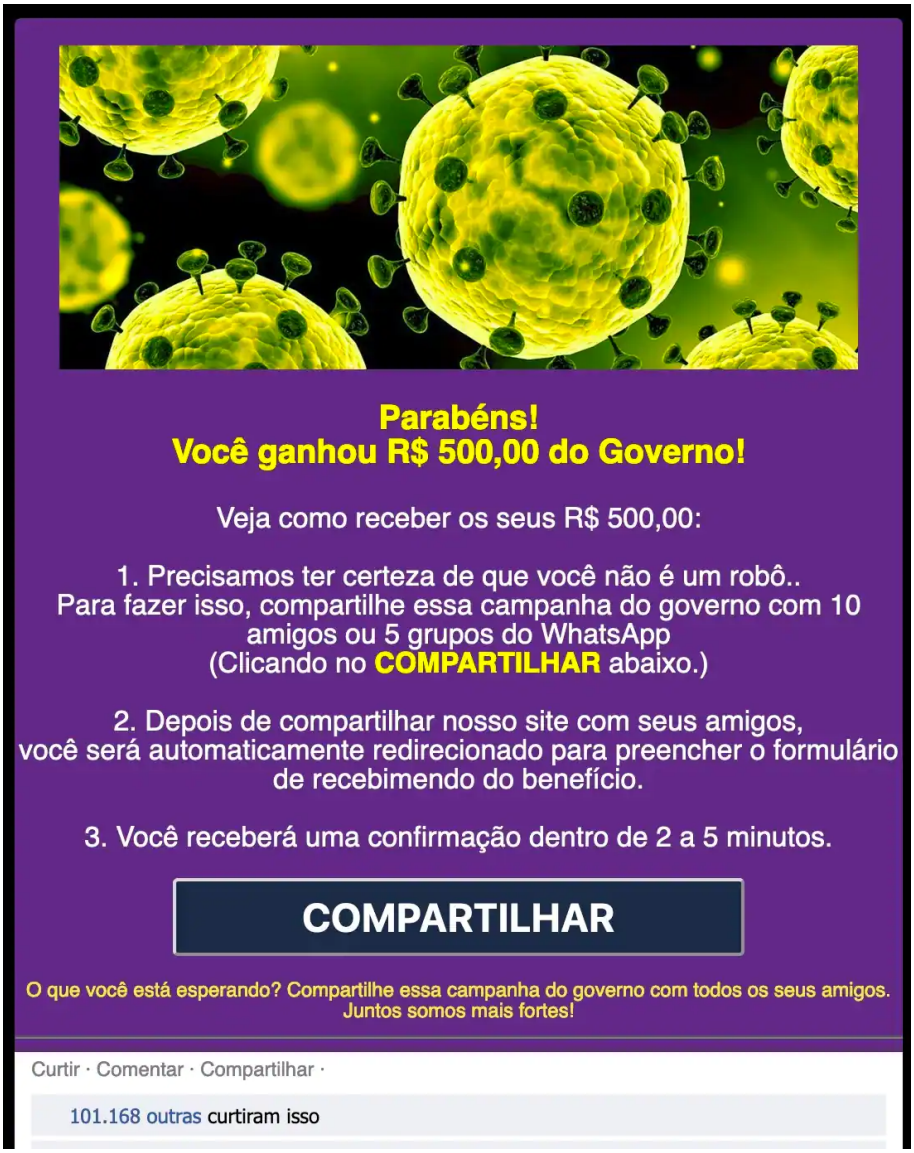


Fonte: YAHOO (2020).

Pesquisadores da Akamai, empresa de Internet americana fornecedora de software e soluções de segurança em nuvem, identificaram uma campanha de *phishing* direcionada aos usuários no Brasil que queriam se beneficiar do auxílio oferecido pelo estado para suprir suas necessidades durante a pandemia do COVID-19. Cerca de 850.000 vítimas foram atingidas pelo ataque e que tiveram suas informações pessoais fraudadas. Os criminosos por trás do golpe se aproveitaram diretamente de domínios, usando variantes do nome coronavírus ou COVID-19 em sua *Uniform Resource Locator* (URL). Abusando ainda mais elementos de engenharia social, os golpistas começaram a incluir comentários falsos de redes sociais sobre os questionários de três perguntas, utilizando artifícios que forneçam a sensação de que aquela é uma página legítima. Contudo os cibercriminosos apostam na ansiedade, insegurança e medo da vítima em torno da crise para prosperar, visto que as pessoas estão preocupadas com suas finanças ou com sua saúde e de seus entes queridos, então uma promessa em relação ao apoio financeiro ou de

informações relacionadas as vacinas, terá um impacto para a vítima, ganhando uma atenção imediata e relevando a possibilidades de golpes.

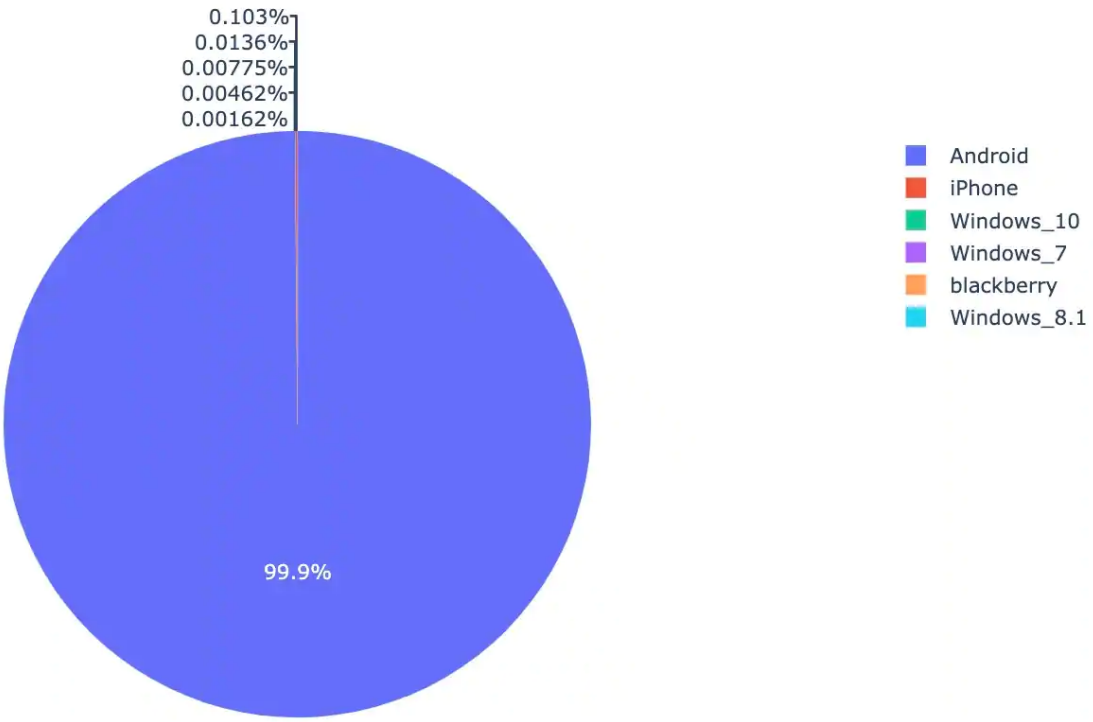
Figura 10 – Golpe de COVID-19 em rede social que exige o compartilhamento de questionário para supostos pagamentos do governo.



Fonte: AKAMAI (2022).

Quando se trata de dispositivos, a maioria das vítimas eram usuários de celular com o sistema operacional Android. A Figura 11 ilustra a informação vítimas por dispositivos. Parte do motivo disso se deve aos próprios sites que foram desenvolvidos apenas para aceitar vítimas que usavam dispositivos móveis, visto a alta quantidade de usuários de dispositivos móveis em comparação aos de computadores. Segundo (SZARVÁK *et al.*, 2021), as interfaces móveis, de uma forma simplificada, prejudicam o usuário ao não permitirem o fácil reconhecimento das iscas criadas pelos cibercriminosos.

Figura 11 – Vítimas por dispositivo



Fonte: AKAMAI (2022).

Independentemente dos tipos de abordagens utilizadas ao realizar o ataque de *phishing*, a COVID-19 forçou muitos a trabalhar em casa, aumentando os riscos virtuais e impulsionando a quantidade de ataques cibernéticos. Portanto, torna-se essencial que o usuário aja de forma rápida e proativa para proteger suas informações ao se tornarem presentes no ciberespaço e para isto, torna-se necessário preparar o indivíduo para o meio digital, fornecendo o conhecimento necessário para obter o total controle sobre o ciberespaço alocando recursos para sua proteção.

Como já definido, o *phishing* é uma junção de engenharia social e técnicas de *hacking* funcionando apenas se a vítima acreditar no conteúdo do e-mail ou mensagem, clicar em algum *link* e fornecer dados ou baixar arquivos infectados, ou seja, o ataque prioriza o usuário como alvo principal, já que o lado humano, segundo a segurança da informação, sempre será o elo mais fraco, sujeito a vulnerabilidades e fácil de ser explorado pelos *hackers*. Podemos citar algumas medidas para a proteção do usuário, tais como: proteção de e-mail, evitando a transmissão de informações pessoais pela rede, com exceção de casos no qual se estará utilizando sites seguros; confirma se o domínio é condizente com o nome da loja; tomar cuidado com esquemas de *phishing* via telefone; cuidado com downloads, e; atenção na utilização de *links*.

Outras ações preventivas estão relacionadas ao controle do acesso a *pop-ups*, ma-

nutenção dos sistemas atualizados, adoção de *firewall*, filtros de *spam*, antivírus e software *anti-spyware*. Estas soluções propõem como requisito um alto conhecimento do usuário sobre o meio a qual está inserido, porém nem sempre o indivíduo estará apto a estar na rede, seja pelo despreparo, pela rápida digitalização ou pelo temor de que algo vá acontecer com o usuário ou com pessoas próximas.

Portanto, soluções mais básicas devem ser apresentadas a fim de garantir a segurança de pessoas com pouco conhecimento tecnológico. Primeiramente, devemos verificar a veracidade do site consultando sempre a mídia original ou fontes de confiança, minimizando assim os riscos e eficiência dos ataques. Devemos evitar compartilhar informações pessoais ou de conhecidos na Internet, mesmo que o local de compartilhamento pareça seguro, pois eles também estão propícios a serem alvos de ataques cibernéticos e, por fim, devemos validar as informações recebidas com as fontes de origem, como por exemplo: Um usuário recebeu em seu e-mail uma mensagem de um determinado banco solicitando a confirmação de seus dados pessoais. Antes de mandar tais informações, é imprescindível que o usuário entre em contato diretamente com algum órgão de gerenciamento do banco em questão para verificar se a solicitação é oficial.

Ações como essas são simples de serem aplicadas e permitem ao usuário se prevenir de ciberataques, principalmente os ataques de *phishing*. É fundamental ao indivíduo ter a capacidade para manipular de forma adequada os sistemas de informação. Saber da existência dos perigos existentes, a forma como são feitos e suas soluções, garantem ao indivíduo um arsenal de formas e meios para se estar preparado, caso seja alvo ou mesmo vítima de uma desses ciberataques. O conhecimento acaba por induzir a prevenção, e um desses meios para adquirir conhecimento e que vem se desenvolvendo junto da gradual imersão da sociedade no mundo virtual é a cibereducação.

As TICs - originaram novos espaços para a aprendizagem que não necessariamente estão vinculados a um espaço físico, já que atualmente vivemos em uma sociedade que dispõe de uma grande fonte de informação virtual como a Internet. Essa evolução do Ciberespaço cria a cibercultura, como o "[...] conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço" (LÉVY, 2010). Lévy (2010) também aponta que a relação e a troca de conhecimento não param de crescer, sendo cada vez mais importante a produção de conhecimento e a sua transmissão. É por meio dessa relação de transmissão e consumo de informação que há o surgimento da cibereducação como também de diversos outros tipos de

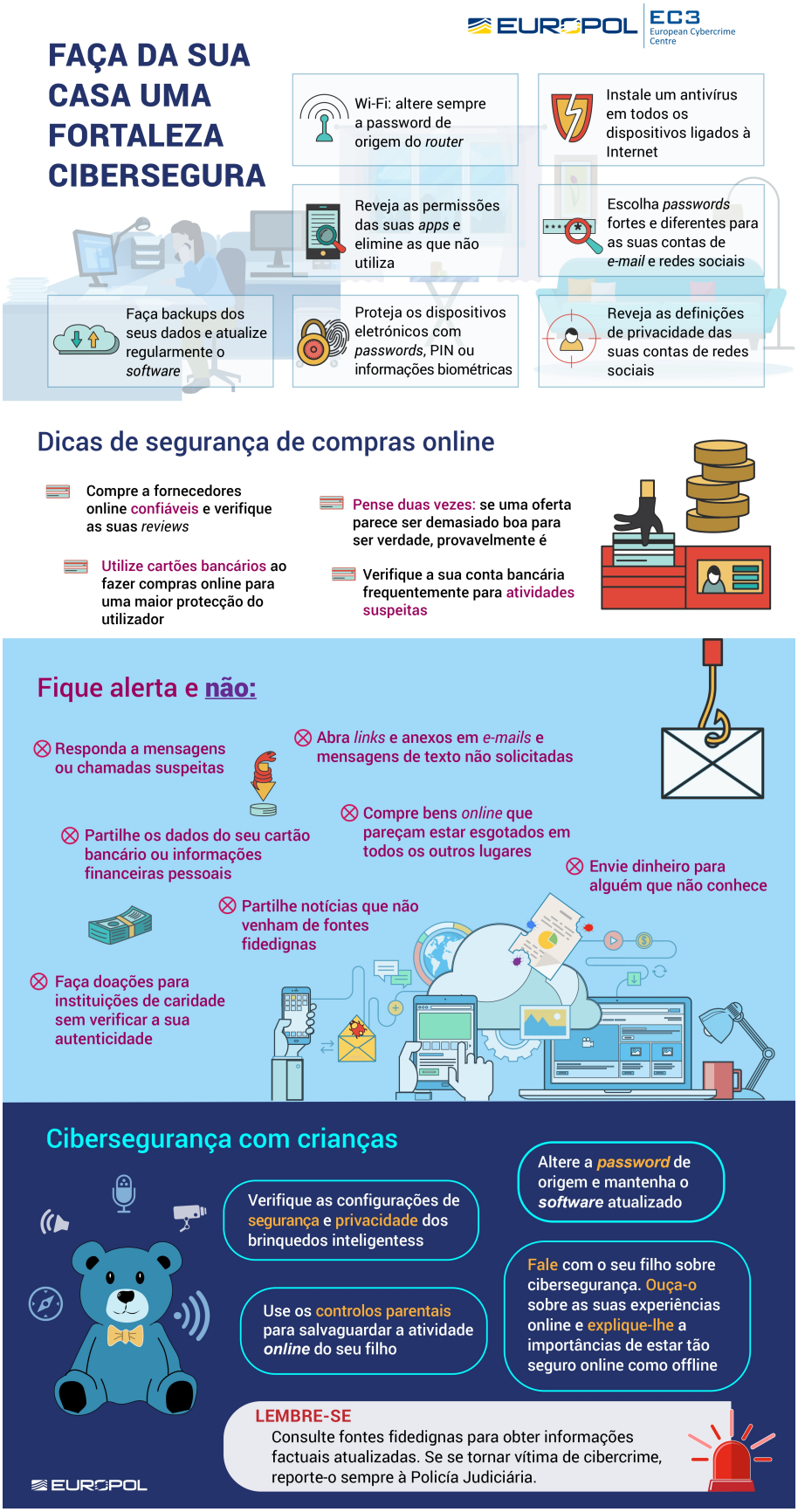
saberes (LÉVY, 2010).

A cibereducação acaba por vir a ser a educação do indivíduo imerso em uma cultura ciber a fim de consciencializar e educar os cidadãos, como por exemplo, para a importância da cibersegurança, que vai muito além do simples manusear o computador e utilizar a Internet. Conhecer os mecanismos, políticas e procedimentos de segurança pode não ser suficiente então torna-se necessário o conhecimento sobre como as tecnologias funcionam, levando em consideração o fator emocional do indivíduo, para então que ele possa garantir a sua segurança em meio digital.

A Europa já vem apresentando medidas preventivas em relação à cibereducação e conscientização da cibersegurança. A Europol realiza campanhas de conscientização como vemos na Figura 12, infográficos são disponibilizados gratuitamente para diversos idiomas falados na Europa com o objetivo de alertar a população para múltiplas ameaças que podem afetar a vida cotidiana. O boletim da Sans Ouch é outra grande fonte de avisos e dicas para reduzir o risco de um ataque bem sucedido. A *Cybersecurity and Infrastructure Security Agency* (CISA), também apoia os usuários com dicas, descrevendo e oferecendo conselhos sobre questões relacionadas à cibersegurança para pessoas com pouco conhecimento técnico sobre tecnologia. Além disso, a Comissão Europeia em parceria com a *European Union Agency for Cybersecurity* (ENISA) organizam o evento do Mês Europeu da Cibersegurança, que promove a cibersegurança entre os cidadãos e organizações da União Europeia por meio de conferências, *workshops*, treinamentos e *webnars*, fornecendo informações para segurança na rede, sensibilizando e compartilhando boas práticas digitais para então conscientizar sua população para segurança da informação e a manutenção de uma boa higiene cibernética que esta relacionada à mentalidade e aos hábitos centrados na segurança que ajudam indivíduos e organizações a mitigar possíveis violações *on-line*.

Já em nosso país, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) - apresenta estudos anuais acerca dos incidentes e oferece treinamentos para capacitação de profissionais e pessoas não-técnicas a fim de aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil. o CERT.br em parceria com o *Núcleo de Informação e Coordenação do Ponto BR* (NIC.br) e o *Comitê Gestor da Internet no Brasil* (CGI.br) divulgam infográficos e cartilhas educativas sobre a utilização da internet, conscientizando o uso correto e seguro desta ferramenta. Além de possuir uma material para o público mais geral, também apresenta um material destinado

Figura 12 – Faça da sua casa uma fortaleza cibersegura



Fonte: EUROPOL (2021).

ao público infantil, como vemos na Figura 13, que possuem um design mais lúdico permitindo que as crianças aprendam e desenvolvam o conhecimento tecnológico enquanto se divertem.

Figura 13 – Imagem para a aprendizagem de segurança na internet para crianças.

Fonte: INTERNET SEGURA (2022).

A cibereducação está em constante desenvolvimento, então torna-se uma solução viável e eficiente para a prevenção desses usuário, além de fornecer assistência à usuários, técnicos e não técnicos, acompanhando o indivíduo ao longo da sua relação com o ciberespaço, assim, reduzindo o risco de um ataque bem sucedido, permitindo que o usuário tenha a tenacidade e esteja preparado paras as adversidades do meio, principalmente em cenários como a pandemia de COVID-19. Porém, também cabe o incentivo do Estado para fomentar este tipo de conhecimento, ajudando assim a disseminar ainda mais a cibersegurança no Brasil. Em suma, a cibereducação é uma competência que deve não só ser lecionada nas atividades formativas de cada cidadão como também ser intrínseca a nossa sociedade.

6 CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho apresentou um estudo exploratório dos ataques de *phishing* no Brasil durante a pandemia de COVID-19. Foi elaborado uma discussão acerca do levantamento feito, além de analisar soluções técnicas no intuito de precaver ou eliminar os riscos do ciberataque em questão. Para isso, utilizou-se os aspectos teóricos sobre Ciberespaço e Segurança da Informação. Além disso, foi comentado sobre os ciberataques e o cenário dos ataques de *phishing* em um Brasil pandêmico, como soluções que suprissem a necessidade de proteção do usuário ao utilizar as tecnologias da informação. Em termos metodológicos este ensaio serviu-se da pesquisa exploratória e da pesquisa não-experimental. Na etapa da pesquisa exploratória, em particular, foi utilizado o levantamento bibliográfico para reunir os conceitos teóricos necessários para o entendimento do trabalho. Já a pesquisa não-experimental foi adotada para tirar conclusões a partir de um arcabouço teórico reunido na etapa da pesquisa exploratória.

Como resultados e discussão desta pesquisa foram identificados como ocorrem os ataques de *phishing*, como esta técnica foi utilizada durante a pandemia e soluções que minimizem a efetividade dos ciberataques. Diante dos resultados e discussões, pode-se perceber que foi possível responder à questão do problema de pesquisa definida no Capítulo 1. A cibereducação pode vir a ser uma eficiente solução para a prevenção do usuário mediante o seu constante desenvolvimento e incentivo ao usuário ao consumo e transmissão de saberes, assim, permitindo aos usuários conhecerem o meio ao qual estão inseridos, seus riscos e como se prevenir, não somente dos ataques de *phishing*, mas de todos os outros vetores de ataques que poderiam escalonar.

Como trabalhos futuros, almeja-se:

a) Realizar um estudo mais aprofundado no intuito de elencar mais ataques e enriquecer a pesquisa;
b) Realizar um estudo sobre a eficiência dos ataques de *phishing* em diversos dispositivos; e
c) Elaborar provas de conceito para validar as discussões realizadas neste ensaio, visto que os resultados e análise foram em uma perspectiva teórica.

REFERÊNCIAS

ABROSHAN, H.; DEVOS, J.; POELS, G.; LAERMANS, E. COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic. **IEEE Access**, v. 9, p. 121916–121929, 2021.

ACCENTURE SECURITY. **The cost of cybercrime**. 2019. Disponível em: <https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50>. Acessado em 24 de julho de 2022.

AKAMAI. **Brazil Targeted by Phishing Scam Harnessing COVID-19 Fears**. 2022. Disponível em: <https://www.akamai.com/blog/security/brazil-targeted-by-phishing-scam-harnessing-covid-19-fears>. Acessado em 04 de julho de 2022.

ARAÚJO, R. M. F. **Liberdade de manifestação do pensamento em colisão com outros direitos constitucionais**. 2017. Disponível em: <http://opiceblum.s3-sa-east-1.amazonaws.com/ColetaneaDireitoDigital1.pdf>. Acessado em 30 de novembro de 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799: tecnologia da informação: técnicas de segurança - código de prática para a gestão da segurança da informação**. Rio de Janeiro: [s.n.], 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2013: Tecnologia da informação – Técnicas de Segurança – Código de prática para controles de segurança da informação**. Rio de Janeiro: [s.n.], 2013.

AVAST. **Academia de Ameaças Online**. 2017. Disponível em: <https://www.avast.com/pt-br/c-online-threats>. Acessado em 28 de novembro de 2021.

BESTUZHEV, D. **CISO Advisor: Ciberataques cresceram 23% no Brasil em 2021**. 2021. Disponível em: <https://www.cisoadvisor.com.br/ciberataques-cresceram-23-no-brasil-em-2021/>. Acessado em 04 de julho de 2022.

BOGDAN, R.; BIKLEN, S. **Investigação qualitativa em educação: uma introdução à teoria e aos métodos**. Porto: Porto Editora, 1994. ISBN 9789720341129.

BRASIL. **Lei n. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências**. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acessado em 25 de novembro de 2021.

CARNEIRO, L. E. d. S.; ALMEIDA, M. B. Gestão da informação e do conhecimento no âmbito das práticas de segurança da informação: o fator humano nas organizações. **Encontros Bibli: Revista Eletrônica de Biblioteconomia e Ciência da Informação**, v. 18, n. 37, p. 175–202, 2013. Disponível em: <https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2013v18n37p175>.

CARVALHO, A. A. R.; MARQUES, M. R. M. Cibereducação como medida preventiva no combate ao Cibercrime. **Cyberlaw by CIJIC**, n. 4, p. 11–39, set. 2017. ISSN 2183-729. Disponível em: <http://www.cijic.org/wp-content/uploads/2017/09/Cyberlaw-by-CIJIC_edicao-n4.pdf>.

CASCAIS, F. **Dicionário de Jornalismo: as palavras dos media**. São Paulo: Verba, 2001.

CEPIK, M. Segurança nacional e segurança humana: Problemas conceituais e consequências políticas. **Security and Defense Studies Review**, v. 1, p. 01–19, 2001. Disponível em: <https://professor.ufrgs.br/sites/default/files/marcocepik/files/cepik_-_2001_-_seg_nac_e_seg_hum_-_sec_and_def_review.pdf>.

CERT.BR. **Cartilha da Segurança para Internet. Versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil**. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acessado em 25 de março de 2021.

CHECK POINT SOFTWARE TECHNOLOGIES. **Check Point Press Releases**. 2020. Disponível em: <https://www.checkpoint.com/press/2021/check-point-software-technologies-reports-2020-fourth-quarter-and-full-year-financial-results/>. Acessado em 29 de novembro de 2021.

CHECK POINT SOFTWARE TECHNOLOGIES. **Check Point Press Releases**. 2022. Disponível em: <https://www.checkpoint.com/>. Acessado em 22 de julho de 2022.

COMPUTERWORLD. **Ciberataques estão em alta na pandemia – e não devem diminuir tão cedo**. 2021. Disponível em: <https://computerworld.com.br/seguranca/ciberataques-estao-em-alta-na-pandemia-e-nao-devem-diminuir-tao-cedo/>. Acessado em 30 de novembro de 2021.

CUZZOCREA, A.; MARTINELLI, F.; MERCALDO, F. Applying machine learning techniques to detect and analyze web phishing attacks. In: **Proceedings of the 20th International Conference on Information Integration and Web-Based Applications & Services**. New York, NY, USA: Association for Computing Machinery, 2018. (iiWAS2018), p. 355–359. ISBN 9781450364799. Disponível em: <https://doi.org/10.1145/3282373.3282422>.

CYBEREDGE GROUP. **2020 - Cyberthreat Defense Report**. 2020. Disponível em: <https://cyber-edge.com/cdr/>. Acessado em 24 de julho de 2022.

DEB SOLUTIONSTI. **Conheça a ISO 27000 a família de normas que abordam a Segurança da Informação**. 2015. Disponível em: <https://debsolutionsti.com/iso-27000/iso-27000/>.

DEFINIRTEC. **Guerreiro Cibernético**. 2021. Disponível em: <https://definirtec.com/guerreiro-cibernetico/#:~:text=Defini%C3%A7%C3%A3o%20%2D%20O%20que%20significa%20Cyber,informa%C3%A7%C3%A3o%20ou%20para%20atac%C3%A1%2Dlos.> Acessado em 24 de julho de 2022.

EUROPOL. **Make your home a cyber safe stronghold**. 2021. Disponível em: <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold>. Acessado em 04 de julho de 2022.

GIBSON, W. **Neuromancer**. São Paulo: Aleph, 2003. 81-82 p.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 4a. ed. São Paulo: Atlas, 2002. ISBN 85-224-3169-8.

GÓMEZ, A. **El ciberespacio como escenario de conflictos. Identificación de las amenazas**. 2012. 171 p. Centro Superior de Estudios de la Defensa Nacional. Disponível em: <https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf>. Acessado em 29 de novembro de 2021.

HACKMAGEDDON. **May 2021 Cyber Attacks Statistics**. 2021. Disponível em: <https://www.hackmageddon.com/2021/06/08/may-2021-cyber-attacks-statistics/>. Acessado em 24 de julho de 2022.

IBM. **X-Force Threat Intelligence Index 2020**. 2020. Disponível em: <https://www.ibm.com/downloads/cas/DEDOLR3W>. Acessado em 04 de julho de 2022.

IBM. **X-Force Threat Intelligence Index 2022**. 2022. Disponível em: <https://www.ibm.com/security/br-pt/data-breach/threat-intelligence>. Acessado em 04 de julho de 2022.

INTERNET SEGURA. **Para colorir. Autenticação**. 2022. Disponível em: <https://internetsegura.br/passatempo/>. Acessado em 24 de julho de 2022.

JAHROMI, H. Z.; DELANEY, D. T.; HINES, A. Beyond First Impressions: Estimating Quality of Experience for Interactive Web Applications. **IEEE Access**, v. 8, p. 47741–47755, 2020.

JUSBRASIL. **O que um cibercriminoso procura?** 2020. Disponível em: <https://fabriziorodriguesr.jusbrasil.com.br/artigos/870410504/o-que-um-cibercriminoso-procura>. Acessado em 24 de julho de 2022.

KASPERSKY. **Dicas de como se proteger contra crimes cibernéticos**. 2019. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime>. Acessado em 29 de novembro de 2021.

KELLNER, D. **Como mapear o presente a partir do futuro: de Baudrillard ao cyberpunk**. Bauru: EDUSC, 2001.

KOEPSELL, D. R. **A ontologia do ciberespaço: a Filosofia, a lei e o futuro da propriedade intelectual**. São Paulo: Madras, 2004. 125 p.

LÉVY, P. **Cibercultura**. 1a. ed. Lisboa: Instituto Piaget, 2000. ISBN 978-9727712786.

LÉVY, P. **Cibercultura**. 7a. ed. São Paulo: Editora 34, 2010. ISBN 978-8573261264.

LI, R.; PEI, S.; CHEN, B.; SONG, Y.; ZHANG, T.; YANG, W.; SHAMAN, J. Substantial undocumented infection facilitates the rapid dissemination of novel coronavirus (SARS-CoV-2). **Science**, v. 368, n. 6490, p. 489–493, 2020. Disponível em: <https://www.science.org/doi/abs/10.1126/science.abb3221>.

LIMA, C. **CiberCultura, CiberLinguagem e CiberEducação**. 1a. ed. São Paulo: Biblioteca24horas, 2012. ISBN 978-8541602839.

MALWAREBYTES. **Tudo sobre hacking**. 2021. Disponível em: <https://br.malwarebytes.com/hacker/>. Acessado em 25 de março de 2021.

MANAGE ENGINE. **Ciberterrorismo: um breve guia para navegar esse cenário de ameaças em constante evolução**. 2020. Disponível em: <https://blogs.manageengine.com/portugues/2022/06/29/ciberterrorismo-um-breve-guia-para-navegar-esse-cenario-de-ameacas-em-constante-evolucao.html>. Acessado em 24 de julho de 2022.

MARCONI, M. d. A.; LAKATOS, E. M. **Fundamentos de Metodologia Científica**. 5a. ed. São Paulo: Atlas, 2003. ISBN 85-224-3397-6.

MELO, U. **Ciso Adviser: Cibersegurança aplicada à segurança física**. 2020. Disponível em: <https://www.cisoadvisor.com.br/security-room-posts/ciberseguranca-aplicada-a-seguranca-fisica/>. Acessado em 30 de novembro de 2021.

MITNICK, K. D.; SIMON, W. L. **A arte de enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. São Paulo: Pearson Education, 2003. 3-4 p.

NASCIMENTO, J. V. B. do; NETO, M. M.; COUTINHO, E. F.; MOREIRA, L. O. Um Levantamento sobre os Aspectos Técnicos dos Principais Riscos de Segurança e Ataques em Aplicações Web. **Revista Sistemas e Mídias Digitais (RSMD)**, v. 6, n. 1, jul. 2021. ISSN 2525-9555. Disponível em: <http://revistasmd.virtual.ufc.br/arquivos/volume-6/numero-1/rsmd-v6-n1-6.pdf>.

OLIVEIRA, M. C. **Quantificação de vulnerabilidades em segurança da informação avaliando maturidade de pessoas**. 2019. Monografia de Graduação. Bacharelado em Redes de Computadores, Universidade Luterana do Brasil (ULBRA), Canoas, Rio Grande do Sul, Brasil.

PEIXOTO, M. C. P. **Engenharia social e segurança da informação na gestão corporativa**. Rio de Janeiro: Brasport, 2006.

PODILA, L. M.; BANDREDDI, J. P.; CAMPOS, J. I.; NIYAZ, Q.; YANG, X.; TREKLES, A.; CZERNIAK, C.; JAVAID, A. Y. Practice-oriented smartphone security exercises for developing cybersecurity mindset in high school students. In: **2020 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)**. [S.l.: s.n.], 2020. p. 303–310.

QUIVY, R.; CAMPENHOUDT, L. van. **Manual de investigação em ciências sociais**. 2a. ed. Lisboa: Gradiva, 1998. (Colecção "Trajectos"). ISBN 9789726622758. Disponível em: <https://books.google.com.br/books?id=zPveQgAACAAJ>.

RIPA, S. P.; ISLAM, F.; ARIFUZZAMAN, M. The emergence threat of phishing attack and the detection techniques using machine learning models. In: **2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)**. [S.l.: s.n.], 2021. p. 1–6.

SALEOUS, H.; ISMAIL, M.; ALDAAJEH, S. H.; MADATHIL, N.; ALRABAEE, S.; CHOO, K.-K. R.; AL-QIRIM, N. COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. **Digital Communications and Networks**, 2022. ISSN 2352-8648. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2352864822001274>.

SANTOS, C. C.; COUTINHO, E. F.; PAILLARD, G. A. L.; MOREIRA, L. O. Um relato sobre os desafios das atividades remotas em um curso de graduação presencial diante das medidas de prevenção contra o SARS-CoV-2. **Revista Novas Tecnologias na Educação (RENOTE)**, v. 18, n. 1, jul. 2020. Disponível em: <https://seer.ufrgs.br/index.php/renote/article/view/106039>.

SANTOS, R. d. **Impactos da pandemia COVID-19 na indústria de transformação brasileira**. 2022. Monografia de Graduação. Graduação em Ciências Econômicas, Universidade Federal do Rio Grande do Sul, Porto Alegre, Brasil.

SINGER, P. W.; FRIEDMAN, A. **Cybersecurity and cyberwar: what everyone needs to know**. 1a. ed. New York: Oxford University Press, 2014.

SMALING, H. J. A.; TILBURGS, B.; ACHTERBERG, W. P.; VISSER, M. The Impact of Social Distancing Due to the COVID-19 Pandemic on People with Dementia, Family Carers and Healthcare Professionals: A Qualitative Study. **International Journal of Environmental Research and Public Health**, v. 19, n. 1, 2022. ISSN 1660-4601. Disponível em: <https://www.mdpi.com/1660-4601/19/1/519>.

SZARVÁK, A.; PÓSER, V.; KOZLOVSZKY, M. Simplification on mobile devices reduces personal (cyber) safety. In: **2021 IEEE 15th International Symposium on Applied Computational Intelligence and Informatics (SACI)**. [S.l.: s.n.], 2021. p. 000351–000356.

TECHTUDO. **É vírus? Veja como identificar um golpe de phishing**. 2018. Disponível em: <https://www.techtudo.com.br/listas/2018/05/e-virus-veja-como-identificar-um-golpe-de-phishing.ghtml>. Acessado em 24 de julho de 2022.

TRAILHEAD. **Identifique ameaças comuns de segurança de rede**. 2019. Disponível em: <https://trailhead.salesforce.com/pt-BR/content/learn/modules/network-security-basics/identify-common-network-security-threats#:~:text=Os%20hackers%20s%C3%A3o%20muitas%20vezes,nomes%20de%20conta%20e%20senhas.> Acessado em 24 de julho de 2022.

VERIZON. **2019 Data Breach Investigations Report**. 2019. Disponível em: <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>. Acessado em 24 de julho de 2022.

WAZLAWICK, R. S. **Metodologia de Pesquisa para Ciência da Computação**. 1a. ed. Rio de Janeiro: Elsevier Editora, 2009. ISBN 978-85-352-3522-7.

YAHOO. **Criminosos enganam internautas com domínios falsos da Netflix, Apple e outros**. 2020. Disponível em: <\protect\unhbox\voidb@x\bgroup\def.{https://blogs.manageengine.com/portugues/2022/06/29/ciberterrorismo-um-breve-guia-para-navegar-esse-cenario-de-ameacas-em-constante-evolucao.html}\let\futurelet\@let@token\let\protect\relax\edefptm{ptm}\edefcmss{cmss}\edefcmtt{cmtt}\def#1,b,{}\series@check@toks{,ulm,elm,lm,slm,mm,sbm,bm,ebm,ubm,muc,mec,mc,msc,msx,mx,mex,mux,{}{},b,}\edef{}\edefb{b}\def#1,m,{}\series@check@toks{,ulm,elm,lm,slm,mm,sbm,bm,ebm,ubm,muc,mec,mc,msc,msx,mx,mex,mux,{}{},m,}\edef{}\edefm{m}\protect\let>. Acessado em 24 de julho de 2022.