Notícias Falsas, Dano Real: Levantamento, Análise e Discussão de Phishing, Malware e Fake News sobre COVID-19

Tamy Beppler
Natalia Yada
DInf – Universidade Federal do Paraná (UFPR)
Curitiba, Paraná, Brasil
tebeppler@inf.ufpr.br
ntyada@inf.ufpr.br

Luis Carlos de Bona
André Grégio
DInf – Universidade Federal do Paraná (UFPR)
Curitiba, Paraná, Brasil
bona@inf.ufpr.br
gregio@inf.ufpr.br

RESUMO

Coronavirus pandemic (COVID-19) has been one of the most trending topics in 2020's overall media. The virus' first registers date back to December 2019 in China, and its spread has affected more than 50 million people around the world. Since social distance is the most advisable recommendation by health organizations, companies massively adopted remote work. The Internet became a huge allied for several jobs maintenance, but it also increased social engineering attacks based on the COVID-19 topic to steal sensitive information and/or spread malicious code. In this paper, we review the literature about phishing, malware and fake news that take advantage of COVID-19 to distress users and organizations in order to accomplish cyber attacks, and discuss their implications.

KEYWORDS

Fake news, Malware, Phishing, Covid-19, Coronavírus

1 INTRODUÇÃO

A pandemia do Coronavírus tem afetado o mundo todo desde dezembro de 2019. Até o final de novembro de 2020, mais de 62 milhões de casos e 1 milhão e 400 mil mortos foram confirmados [1]. Para He et al. [2], a doença pode ser vista como uma exploração *zero-day* (vulnerabilidades ainda não bem compreendidas e sem *patch* disponível para mitigá-las) biológica, onde o vírus se infiltrou em quase todo o planeta e parece compreender as "vulnerabilidades sociais" das pessoas. A medida de prevenção mais segura ainda é o distanciamento social, o que fez com que muitas empresas e instituições adotassem o trabalho remoto. A Internet foi a grande aliada para a adaptação das pessoas a esse novo cenário de estudo/trabalho, tendo seu uso e dependência aumentados exponencialmente [3–8]. Entretanto, boa parte das informações digitais não é regulamentada e sua qualidade é questionável, o que dificulta julgamento apropriado delas, principalmente as que se referem à saúde, por uma pessoa leiga. Portanto, cada vez mais fazem-se necessários avaliação crítica, curadoria/triagem de conteúdos de qualidade e ferramentas para o combate das *fake news*, bem como o desenvolvimento e aprimoramento de medidas de combate a *malware* e *phishing* [9].

Há uma correlação entre a pandemia e o aumento de crimes cibernéticos [4, 10], inclusive estatísticas de que atividades maliciosas aumentaram 2.000% por causa da dela [11]. A migração para o trabalho remoto foi, inclusive, um dos grandes facilitadores para maior suscetibilidade das pessoas a serem enganadas, somada a propensão à distração com assuntos relacionados sobre a doença e ao pânico pela falta de informação [7, 8, 12–16]. Para Eian et al. [3], atividades *online* como aulas, trabalho remoto, compras, entretenimento, entre outrossão fáceis de serem atacadas, e o COVID-19 abriu oportunidades para novos ataques [6, 12, 13, 17]. Além disso, há o problema da denúncia: estudos mostram que apenas 37% dos crimes cibernéticos acabam sendo conhecidos pela polícia [18], e muito disso se dá pela insolubilidade do problema, pois muitos ataques são originários de outros países (possuindo diferentes leis) e as polícias e justiça brasileira são sobrecarregadas para tratar de crimes tradicionais, que dirá cibernéticos. Os tipos de ataques mais comuns citados por alguns autores são: *phishing mail* e *malware* (para [3]); *scam* e *phishig*, *malware* e *distributed denial-of-service* - DDoS (para [4]); *phishing, malware, scamming*, e *spamming* (para [19]); entre outros. Para a grande maioria [15, 20–22], *phishing* e *malware* seguem como uma das maiores ameaça à segurança, e se tornaram tópico para nossa pesquisa. Conforme Duggal [8], o espaço virtual está tão cheio de informações e desinformações que as pessoas não sabem em qual fonte devem confiar.

Neste trabalho foi realizada uma ampla revisão sistemática da literatura atual sobre *malware*/*phishing* e *fake news* durante a pandemia do COVID-19. O objetivo principal foi identificar os impactos da pandemia na propagação de *fake news* e aumento dos crimes cibernéticos, bem como recomendações para evitá-los. Esta é a primeira revisão sobre o impacto da pandemia no mundo virtual de que temos notícia, e pode oferecer uma visão mais abrangente do estado da arte para pesquisas futuras.

2 CRIMES CIBERNÉTICOS E COVID-19

Embora muitas pesquisas apontem expressivo aumento no número de casos de crimes cibernéticos após o início da pandemia, ataques direcionados relacionados a um incidente de grande escala não são exclusivo dela. Lallie et al. [12] mostram vários casos de ataques oportunísticos no passado, como em catástrofes ambientais ou mesmo em eventos, como olimpíadas. Porém, um grave problema é que os crimes relacionados ao COVID-19 estão evoluindo e se adequando às mudanças situacionais da pandemia [23], o que facilita ludibriar os usuários. Isso é ressaltado por Bhardwaj et al. [24], que afirmam que 60% das brechas de dados são causadas por erro humano, e corroborado por outros autores, que mapeiam os seguintes problemas relacionados: número de usuários inexperientes usando o espaço cibernético com maior frequência [7, 25, 26]; idosos que são inseguros ao lidar com questões de segurança cibernética [27]; pessoas que escolhem ignorar a atualização de seus dispositivos [3, 25]; questões quanto ao trabalho remoto, como dispositivos próprios que normalmente são menos seguros que os da empresa [8, 13, 25];

funcionários remotos que acessam contas corporativas por meio de Wi-Fi público, fazem *login* em dispositivos sem nunca fazer *logoff* quando não estão em uso, e podem permitir que familiares e amigos usem os dispositivos do trabalho em casa [14]; falta de treinamentos educativos para usuários [23].

Eian et al. [3] afirmam que cerca de 60.000 e-mails relacionados à pandemia contêm links e anexos maliciosos. Conforme mencionado anteriormente, a maioria dos crimes cibernéticos envolve *phishing* e/ou *malware*, que são o foco deste trabalho. A seguir, serão mostradas explicações e exemplos sobre ambos.

2.1 *Phishing*

Ataques por *phishing* são o tipo de crime com maior taxa de aumento [28] e representam mais de 80% dos incidentes cibernéticos [5, 29]. O objetivo é atrair e enganar uma vítima para obter o máximo de informações possível [24] e os ataques mais eficazes são aqueles que afetam emoções e preocupações [28]. *Phishing* é geralmente associado a *malware*, pois muitas vezes a engenharia social é utilizada para que a vítima faça o *download* de programas maliciosos [11]. Bhardwaj et al. [24] afirmam que 90% dos e-mails de *phishing* são detectados pelos *gateways* dos próprios servidores de e-mail, mas os 10% restantes foram responsáveis por mais de 170.000 incidentes dentro de organizações dos EUA. Para ele, servidores de e-mail só impedem os níveis mais básicos de *phishing*. Os ataques são, em geral, de baixo custo [12], com taxa de sucesso razoavelmente alta (cerca de US$17.700 são perdidos por minuto) [5]. No Brasil, em 10 meses de 2019, esses ataques cresceram 232% [24].

Atualmente o tema Coronavírus tem sido altamente explorado pelos criminosos. Naidoo [23] e Swasey [22] afirmam que os ataques de *phishing* relacionados ao vírus aumentaram 667%. Só em abril foram enviados 18 milhões de de e-mails relacionados ao COVID-19 [12, 22–24]. Muitas campanhas utilizam o remetente do e-mail de organizações da saúde reconhecidas, como da OMS (WHO em inglês). Utilizam uma extensão enganosa, como por exemplo `who.org`, parecendo realmente legítimos, quando o original é `who.int` [5, 12, 23, 30]. Andrade et al. [5] explicam que são encontradas com frequência palavras como *vaccine-trials* (testes de vacina) ou *free tests for covid19* (testes grátis para COVID-19). Em [31] pesquisadores notaram um aumento nos modelos de sites de *phishing* que imitam organizações governamentais e não governamentais, como Governo do Reino Unido, Organização Mundial da Saúde (OMS), Centros para Controle de Doenças (CDC), entre outros. De acordo com Eboibi [14], no Reino Unido pessoas foram alvos de e-mails de *phishing* sobre Coronavírus com anexos infectados contendo medidas de segurança fictícias, o que nos retorna às situações onde *phishing* e *malware* são apresentados em conjunto.

2.2 *Malware*

Malware é qualquer código projetado para causar perda de dados e danos indesejados a sistemas/dispositivos/usuários-alvo. Muchnik et al. [32] afirmam que o ecossistema do *malware* exibe mecanismos de disseminação semelhantes aos de sistemas biológicos. Eian et al. [3] e Lallie et al. [12] afirmam que Ransomware (tipo de *malware* que sequestra dados em troca de pagamento) é atualmente a forma mais comum de *malware* pois custa menos e é mais fácil de executar, o que aumenta o pagamento do ataque. Pesquisas mostram que organizações de saúde são os principais alvos, já que acabam pagando o resgate mais rapidamente para evitar o tempo de inatividade e ter acesso aos dados críticos do paciente, tratando-se, por vezes, de casos de vida ou morte [7, 22]. Entre 2019 e o início de 2020, 491 ataques desse tipo foram bem sucedidos contra provedores de saúde dos Estados Unidos [22].

Os exemplares de *malware* cresceram expressivamente durante o COVID-19 [11, 11, 12]. Em apenas um dia (16 de março de 2020), entre 10h e 17h do horário europeu central, houveram 2.500 infecções de *malware* relacionado ao COVID-19 como resultado de golpes de e-mail [22]. Esses números também têm aumentado em relação a aplicativos de *smartphones*, como apresentado por He et al. [2], que mostram que *phishing* está presente nos principais comportamentos do *malware* de Android com o tema COVID-19. A análise foi feita até 26/05/2020 e 277 aplicações maliciosas foram encontradas. O primeiro registro (26/01/2020) foi de um ransomware com o tema COVID-19, o que mostra quão rápido os criminosos se adaptam às situações. Cita-se também o ransomware CryCryptor, que se disfarça como um aplicativo de rastreio de contato de COVID-19 em dispositivos Android [4] e um Trojan bancário que se mascara como um aplicativo móvel desenvolvido pela OMS [28].

2.3 *Fake News*

O uso de notícias falsas para manipular a opinião pública tornou-se normal nos últimos anos e pode claramente ser definida como informação imprecisa e falsa que é espalhada intencionalmente ou não, podendo influenciar as respostas comportamentais das pessoas em relação aos eventos, como eleições e/ou desastres naturais [33]. Informações enganosas por si só, podem ter como objetivo perturbar a economia dos países, reduzir a confiança das pessoas em seus governos ou promover um produto específico para obter lucros enormes e com a pandemia do COVID-19 os números de *fake news*, tem aumentado dia após dia [34].

Segundo Al-Rakhami and Al-Amri [33], no mês de abril de 2020, foram espalhadas mais de quatro mil alegações falsas sobre a pandemia. Em um estudo feito por [35], foi feita a análise de 1 milhão de twittes relacionados a pandemia e 83,9% desses twittes foram classificados como informações médicas enganosas. Devido a grande quantidade delas, plataformas de mídia social foram forçadas a implementarem ferramentas e verificadores para reduzir a disseminação da desinformação [36]. Ainda detectaram perfis anônimos publicando notícias falsas que vão diretamente contra a orientação de fontes oficiais de informações de saúde pública, com o objetivo de influenciar as pessoas a agirem contra as orientações [37].

Esta alta disseminação de conteúdos falsos, acarretou em um fenômeno chamado de Infodemia, onde a Organização Mundial da Saúde (OMS) alegou que não estamos apenas lutando contra a pandemia do COVID-19, mas sim contra uma infodemia, que é como uma doença que se espalha e circula rapidamente na forma de informações enganosas [34]. Junto com este grande volume de conteúdos falsos, surgiu o medo e o pânico da população, gerando assim um impacto negativo perante a saúde da população mundial, com prescrições médicas erradas, dicas e concelhos errôneos e crenças em remédios caseiros acarretando problemas de saúde como envenenamento ou até mesmo a morte [33, 35].

3 METODOLOGIA

Para identificar os trabalhos atuais sobre os crimes cibernéticos explicados na Seção 2, foram realizadas duas revisões da literatura utilizando o modelo proposto por [38], que inicia-se com a fase do planejamento, segue pela condução e finaliza com a análise de dados. Na fase do planejamento é definida a formulação das questões de pesquisa (QP's) relacionadas ao assunto a ser abordado. Para uma cobertura mais abrangente dos estudos relevantes à uma revisão da literatura, é necessário realizar uma busca por bases de dados digitais. Para facilitar esse processo e retornar estudos que agreguem ao ao tema pesquisado, pode-se utilizar uma *string* de busca, a qual tem como objetivo a identificação e concatenação de termos chaves que juntos podem responder as QP's. Para que a busca seja certeira, é necessário que esse termos sejam diretamente ligados ao tema de pesquisa.

Durante o processo de busca foi aplicado o filtro de ano de publicação, onde foram mapeados apenas estudos publicados a partir de de dezembro de 2019, data do primeiro registro da de Covid-19, na China, até novembro de 2020.

Para garantir a qualidade dos resultados da revisão é importante definir critérios de seleção dos estudos, pois dessa forma é possível estabelecer a relevância de um estudo para o contexto da revisão sistemática a ser conduzida. Esses critérios são definidos levando em consideração as QP's, e com eles é possível identificar quais estudos contribuem na resposta das mesmas. Chamaremos de CI para os critérios de inclusão e CE para os critérios de exclusão.

Segundo Kitchenham et al. [38], uma fase importante na condução da pesquisa é aplicação de filtros de leitura, uma vez que auxilia o processo de seleção dos estudos retornados pelas bases de dados. Para tanto, são aplicados três filtros de leitura: I) Leitura de título e *abstract*; II) Leitura da introdução e conclusão; e III) Leitura do estudo na íntegra. Destaca-se que em todos os filtros de leitura, devem ser aplicados os CI's e CE's para cada estudo analisado.

Os artigos que não cumprem com qualquer um dos critérios de exclusão, são então descartados. Os seguintes CE's foram utilizados:

- CE_1 - **Disponibilidade:** a pesquisa deve possuir versão gratuita ou disponibilizada pela universidade brasileira.
- CE_2 - **Tema incompatível:** não diretamente relacionado ao COVID-19 e/ou não relacionado ao tema (*phishing/malware* ou *fake news*).
- CE_3 - **Idioma distinto:** idioma da pesquisa diferente de inglês ou português.
- CE_4 - **Resultado repetido:** o mesmo documento aparece em diferentes resultados da pesquisa nas plataformas de busca.
- CE_5 - **Literatura cinzenta:** diferentes tipos de documentos que não possuem teor científico ou não sejam *full paper*.

3.1 Phishing e Malware

Num primeiro momento foram analisados aqueles crimes talvez mais evidentes, relacionados ao roubo de informações e dados (*phishing* e *malware*). Essa revisão teve como objetivo responder a seguinte QP: "Qual o cenário atual do uso do tema Coronavirus para criação de *phishing mail* e *malware* a fim de explorar a sociedade em um momento de fragilidade mundial?". A busca foi realizada utilizando a base de dados eletrônica Google Scholar, por se tratar de uma base que possui uma cobertura mais ampla que outras [39], utilizando a seguinte *string* de busca: ((“Phishing mail”) OR (malware)) AND ((covid) OR (coronavirus) OR (sars-cov-2)), obtendo, dessa forma, 1257 resultados.

De acordo com os critérios de exclusão, através do primeiro filtro de leitura, a literatura foi reduzida significativamente, conforme mostra a Tabela 1. Dentre as pesquisas excluídas encontramos algumas direcionadas para segurança empresarial, invasão/gravação de videochamadas, invasão de aparelhos médicos que utilizam IoT, a polêmica da utilização da localização de *smartphones* pelo governo para identificar possíveis encontros/aglomerações, entre outros.

Tabela 1: Quantidade de exclusões de acordo com CE.

CE's	Exclusões (#)
CE_1	142
CE_2	735
CE_3	165
CE_4	011
CE_5	110

Os trabalhos restantes foram lidos completamente e avaliados. Nessa etapa, foram descartados mais 60 artigos de acordo com os critérios de exclusão anteriores e leitura completa da referência. Portanto, os 34 trabalhos relacionados selecionados serão apresentados na Seção 4, onde cada um deles é apresentado e classificado de acordo com suas similaridades.

3.2 Fake News

Nessa seção foram formuladas QP's a fim de apontar estudos existentes na literatura que apresentam impactos causados por *fake news* em tempos de pandemia, existência de protocolos de detecção precoce e maneias de combate e controle de *fake news*, sendo elas:

- QP_1: Quais são os impactos da *fake news* em tempo da pandemia do Coronavírus perante a sociedade;
- QP_2: Quais são as maneiras de controle e combate as *fake news*; e
- QP_3: Quais são as ferramentas utilizadas para detecção precoce das *fake news*.

Visando encontrar respostas para as QP's definidas anteriormente, foi definida a seguinte *string* de busca: *((“fake news” OR “misinformation”) AND (“covid-19” OR “coronavirus”))*. A *string* de busca foi utilizada nas seguintes bases de dados filtrando os dados a partir de dezembro de 2019 (primeiro registro da doença): *ACM Digital Library*[1]*, IEEE Xplore*[2]*, e Portal de periódicos CAPES/MEC*[3].

Para esse estudo, além dos CEs foram definidos 3 critérios de inclusão a fim de definir as características que levaram a inclusão de um estudo em específico, sendo eles:

- CI_1: Estudos que apresentam os impactos das *fake news* em tempos de pandemia perante a sociedade;
- CI_2: Estudos que apresentam ou propõe maneiras de controle, combates as *fake news*; e
- CI_3: Estudos que apresentam ou propõe ferramentas utilizadas para detecção das *fake news*.

[1] *https://dl.acm.org* [2] *www.ieeexplore.com* [3] *www.periodico.capes.gov.br*

A partir da *String* de busca foram retornados 599 trabalhos pelas bases de dados eletronicos, onde a quantidade de artigos obtidos em cada base, é apresentada na Tabela 2.

Tabela 2: Quantidade de estudos retornados por base de dados eletrônica

Base de Dados	Quantidade
ACM Digital Library	74
IEEE Xplore	13
Portal de periódicos CAPES/MEC	512
Total	**599**

Em uma visão geral do processo de condução da revisão de literatura, nos artigos encontrados foram aplicados os CI's e CE's, onde 1 estudo foi descartado por se tratar de um estudo na língua espanhola e 23 foram excluídos, por serem estudos duplicados. Dos 575 que restaram, 521 foram descartados por meio da leitura do título e *abstract* e aplicação dos CI's e CE's. A leitura na íntegram descartou mais 24 estudos, totalizando assim 30 estudos relevantes incluídos. Os resultados obtidos através desses 30 estudos incluidos serão apresentados na Seção 4, onde são classificados de acordo com as QP's.

4 DISCUSSÃO DA LITERATURA

Com base nos trabalhos extraídos na Seção 3, a literatura pode ser classificada em sub-grupos, conforme seu objetivo de pesquisa e resultados apontados, auxiliando, dessa forma, a responder as questões de pesquisas.

A maioria das pesquisas foram classificadas como Ciberataques por abordarem um escopo mais geral das ameaças cibernéticas, porém, como podemos ver na Figura 1, a maioria dos ataques expostos na literatura tratam-se de *malware* ou *phishing*. Exemplos desses ataques serão vistos nas próximas seções.

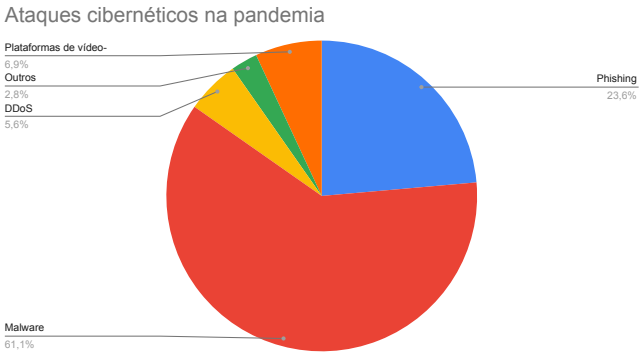

Figura 1: Quantidade de ataques cibernéticos quanto ao seu tipo.

A figura ainda mostra ataques classificados como "plataformas de vídeo-chamada", ataques de negação de serviço (DDoS) e outros. Devido a pandemia e a migração para o trabalho remoto, a utilização de plataformas de video-chamadas cresceu significativamente. Um exemplo de ataque a essas plataformas é o que ficou conhecido como Zoom-bombing, onde os hackers entram em reuniões e aulas que acontecem na plataforma Zoom para causar interrupções ou até investigar as conversas, através de uma ferramenta que permite encontrar IDs de reuniões sem a proteção de senhas [3, 5, 10]. Exemplo de ataque de negação de serviço pode ser visto em um caso onde os sistemas de um grupo de hospitais de Paris foram alvo de um ataque DDoS que interrompeu o acesso ao servidor e e-mail [4, 10]. Outro tipo de ataque comum envolve engenharia social, como foi o caso de alguns funcionários do Twitter que foram atingidos e resultou no comprometimento de contas de usuários pertencentes a algumas celebridades famosas, executivos de tecnologia, líderes mundiais, filantropos e políticos [15]. Utilizando essas contas, eles aplicaram golpes usando a temática COVID-19.

4.1 Phishing & Malware

Hui and Yi-Ling [29] afirmam que *phishing* é responsável por 94% dos ciberataques relacionados ao Coronavírus e mostram 16 casos de ataques relacionados ao COVID-19 usando essa técnica de disseminação. Lallie et al. [12] mostram que uma campanha de *phishing* de medidas de segurança foi utilizada para distribuir o *malware* Emotet (roubo de credenciais financeiras), também relatado em [3] como um dos mais famosos *malware* relacionados ao COVID-19. He et al. [2] analisam o aplicativo CORONA TAKIP, Trojan bancário que se disfarça como um aplicativo para fornecer informações sobre o Coronavírus, porém, requer permissões excessivas quando é instalado e ativado. Além disso, ele mostra uma interface de usuário de *phishing* (uma UI de *login* de banco) em tempo de execução para roubar a conta bancária da vítima.

Um caso mostrado por Pranggono and Arabo [4] é sobre e-mails de *phishing* que foram enviados para alto executivos de uma empresa fornecedora de equipamentos de proteção individual (EPIs). De acordo com os autores, os *links* de *phishing* foram projetados para direcionar os executivos a falsas páginas de *login* da Microsoft para roubar suas credenciais. Já Bhardwaj et al. [24], desenvolveram uma ferramenta para criar *phishing* e mostrar seu funcionamento. Com isso, os autores puderam identificar características comuns para a detecção de *phishing* e terminam alertando que os golpes podem, inclusive, conseguir controlar aparelhos IoT em casa.

O ataque de *malware* relacionado ao COVID-19 mais referenciado pela literatura recente é o CovidLock [40], uma aplicação que diz fornecer um rastreador de casos de Coronavírus em tempo real, mas, em vez disso, trata-se de um *ransomware* que bloqueia os telefones das vítimas dando 48 horas para que elas paguem 100 dólares em bitcoin pela recuperação. As ameaças incluem a exclusão dos dados do telefone e o vazamento das informações da conta nas redes sociais. Outro caso que teve bastante destaque foi o do Hospital Universitário de Brno, na República Tcheca, um dos laboratórios de teste COVID-19 do país. Foi atingido por um ataque cibernético (Ransomware) onde foi forçado a encerrar todos os sistemas de TI e cancelar todas as operações planejadas [4, 5, 12, 25].

Simoiu et al. [20] acreditam que apesar da literatura estudar apenas as causas dos ataques por *phishing* e *malware*, pode haver uma relação com a existência de um grupo mais propenso a cair em golpes e que são alvos mais frequentes. Foram analisados 1.2 bilhões de *phishing* e *malware* enviados pelo GMail durante cinco meses

entre abril e agosto de 2020), e que atingiram cerca de 17 milhões de usuários por semana (a maioria das campanhas dura em média apenas 1 dia). Nessa pesquisa é encontrada uma relação de idade, local e histórico de ataques sofridos. Apesar de ter sido explorado na época do COVID, os autores acreditam que os números seguem os mesmos para outros períodos.

He et al. [2] fizeram um estudo sistemático de *malware* de Android com tema Coronavírus, onde foram avaliados 2.016 aplicativos de COVID-19, sendo 277 *malware*. Foram ainda observados o comportamento dos mesmos, suas origens e os idiomas, o que apontou que a maioria deles (53%) são camuflados como aplicativos oficiais com os mesmos identificadores, e vários deles usam ícones semelhantes e fáceis de confundir. Em [41], foi realizada a análise forense de um aplicativo falso de Coronavírus que imita um legítimo. O estudo pode ser utilizado para detectar aplicações falsas, mesmo quando não-relacionadas a COVID-19. A relação entre vírus que atacam seres vivos com vírus de computador (*malware*) é levantada por Muchnik et al. [32] e Subba [42]. No primeiro trabalho, é feita a comparação através de um estudo de 30 milhões de infecções nas primeiras 72 horas de infecção de 139.962 amostras de *malware*, detectados durante 21 meses (abril, 2017 - dezembro, 2018) que afetaram aproximadamente 200 máquinas. É sugerido que o R0 talvez não seja o melhor dado a ser tomado em conta, e sim, a população. Já no segundo, compara-se o COVID-19 com *zero-day exploit* e constata-se que um dos problemas da área é o fato de cientistas trabalharem independente, sem informar o progresso aos demais, sendo que a cooperação poderia acelerar a descoberta e ainda trazer uma solução melhor, valendo o mesmo para o COVID-19.

Recomendações contra *phishing* e *malware*

Em [15], além se serem apresentados diversos ataques decorridos em meio a pandemia, é proposta uma "lista de verificação" para os mesmos. Dividida em seis módulos (*malware*, engenharia social, negação de serviço distribuída, controle de acesso, ética cibernética e administração cibernética), objetiva funcionar como uma ferramenta proativa e aprimorada para verificar a preparação de indivíduos e empresas na detecção, prevenção, resposta e mitigação de ataques cibernéticos.Outros autores apresentam casos de ataques durante a pandemia (ou se aproveitando dela) e também listam medidas para mitigar os riscos de comprometimento durante o período [10, 13, 16, 21, 25]. A quantidade de recomendações é exibida na Figura 2 e melhor explicadas a seguir:

- **Evitar contato com pessoas virtuais desconhecidas**: Assim como no ambiente real se deve evitar falar com estranhos, no mundo virtual segue-se a mesma ideia. *Links* e anexos de e-mail de fontes desconhecidas e não verificadas não devem ser abertos. Evite também e-mails e SMS não solicitados e chamadas que forneçam informações, suprimentos e tratamento para o COVID-19 que exijam dados pessoais;
- **Verificações de sites, contas de redes sociais e endereços de e-mail**: ferramentas como Google Safe Browsing, Google Transparency Report, Alexa ranking (estima a popularidade global de uma página ou domínio) auxiliam nesta tarefa [43];
- Educação do Usuário por meio de programas de conscientização frequentes;

Figura 2: Quantidade de recomendações por tópico.

- Instalação/atualização de software de anti-vírus;
- Implantação e reforço nas política de segurança da empresa;
- Atualização de programas e sistemas;
- Conexão a rede segura e acesso de contas por meio da VPN;
- Arquivos de Backup e política de recuperação de desastres [22];
- Uso de autenticação multi-fator.

4.2 Fake News

Embora as *fake news* não sejam algo novo, visto que comumente surgem em época de eleições, cada vez mais os pesquisadores vêm estudando formas de combater este tipo de ameaça. A grande quantidade de desinformação, alinhada com a falta de conhecimento, pode acabar gerando caos, além de atrapalhar o trabalho de profissionais da saúde em situações de epidemias e pandemias.

Levando em consideração os estudos incluídos, por tratarem de temas relevantes a pesquisa, essa Subseção tem como objetivo apresentar brevemente os estudos que respondem as questões de pesquisa definidas na Subseção 3.2. Sendo assim, de modo a facilitar a leitura, os estudos foram agrupados de acordo com cada QP. Na Seção 4.2.1 são abordadas as questões referentes ao impacto das *fake news* em tempos de pandemia e na Seção 4.2.2, são discutidas maneiras de controle e combate a *fake news*. Por fim serão apresentadas ferramentas de detecção de *fake news* na Seção 4.2.3. Cada Subseção corresponde respectivamente a QP_1 com 11 estudos, QP_2 com 8 estudos e QP_3 com 12 estudos.

4.2.1 ***Impacto da fake news em tempos de pandemia.*** Diversos são os impactos causados pela desinformação, principalmente no atual momento da pandemia do COVID-19. Por ser uma doença nova e de rápido contágio as pessoas são obrigadas a recorrerem a sites, redes sociais e jornais para mais informações e assim conseguirem se proteger de forma correta e eficaz, bem como ficar a par das novidades. Porém, nem sempre as informações presentes nesses meios são confiáveis, como mostrado em [44], entre 1 de janeiro a 15 de abril de 2020, somente na Indonésia, foram identificadas 534 notícias falsas circulando no país. Em 3 meses após a primeira infecção, não havia sequer uma informação de qualidade sobre a doença [45].

Segundo Montesi [46], algumas *fake news* podem ser inofensivas, ou seja, não causam nenhum dano a saúde da população. Por exemplo, um vídeo que viralizou na internet afirmando que animais estavam tomando ruas da Itália por conta do isolamento, sendo que o vídeo foi filmado antes da pandemia. Por outro lado, há *fake news* que podem colocar em risco a saúde da população, como o caso em [9], sobre alegações que máscaras doadas pela China são contaminadas com COVID-19, álcool em gel é a mesma coisa que nada, ou utilizar álcool em gel nas mãos altera bafômetro nas blitz policiais, desincentivando assim o uso desses produtos que se mostraram bastante eficazes ao combate da propagação do vírus.

Além das *fake news* citadas acima, existem aquelas com caráter criminal, contendo difamação em suas informações. De acordo com [47] houve uma notícia em que foram divulgados posters com a foto de um homem oriental alegando que este seria responsável por espalhar o vírus, ou fotos de restaurantes chineses espalhados pelas redes sociais acusados de serem o início do contágio do vírus. Fora isso, teorias da conspiração também foram criadas, como as apresentadas em [48] e [35], de que o COVID-19 foi um vírus desenvolvido para a China dominar o mundo, que esta pandemia é uma operação comercial farmacêutica ou até mesmo que o 5G danifica o sistema imunológico, o que causou várias queimas de torres de celular na Europa.

Como consequência, informações enganosas compartilhadas sobre bloqueios, vacinações e estatísticas de mortalidade alimentaram o pânico da população em comprar mantimentos, desinfetantes, máscaras e produtos de higiene, levando à escassez que interrompeu a cadeia de abastecimento, agravou as lacunas de oferta, demanda e a insegurança alimentar [34], bem como surgimento o de algumas situações um tanto quanto perigosas, como a dos 2.100 iranianos que foram envenenados pela ingestão oral de metanol, pois viram nas redes sociais que dessa forma estariam imunes ao COVID-19 [49]e em [50], que realizou um experimento entrevistando 5 mil pessoas de 4 países diferentes, onde de acordo com os resultados a probabilidade de seguirem orientações médicas eram significantemente baixa e possuíam uma alta hesitação a vacina. Golpes também foram aplicados, como os 556 casos de fraude de máscara que foram registrados na Malásia, e causaram um prejuízo de milhões da moeda local [51].

4.2.2 ***Maneiras de controle e combate a fake news.*** Com o objetivo de diminuir a disseminação das *fake news* e os impactos causados por elas, várias estratégias e opiniões foram divulgadas para a mitigação dessa infodemia. As redes sociais são um popular meio de comunicação e informação atual, porém há grande circulação de notícias. O Twitter mostrou-se uma das mídias sociais com mais disseminação da desinformação sobre COVID-19, prevalecendo mais as notícias falsas do que as confiáveis [33].

Sendo assim, Ahinkorah et al. [52] acreditam que fornecer avisos regulares por várias plataformas de mídia social sobre a noção dos danos causados pode diminuir o compartilhamento de desinformação sobre o vírus. Já Ardèvol-Abreu et al. [53], diz que plataformas de mídias socias devem deixar claro aos usuários que conteúdo falso pode impulsionar o posicionamento da postagem no *feed* de notícia e também aborda outra medida, que seria explicar ao público, princípios e práticas comuns de verificação de fatos. Segundo Furini et al. [48] para combater essa desinformação é necessário aumentar a presença das autoridades de saúde nos canais sociais.

Em [51, 54], diz que para mitigar esta disseminação, deveria ter viabilização do conteúdo científico confiável a população ou simplesmente fazer com que as pessoas lessem e pensassem sobre as informações do título antes de compartilhar. Há também quem acredite que a melhor maneira de investigar são ferramentas capazes de detectar as *fake news*, assim como em [55] que diz que o melhor meio para isso, seria a construção de uma ferramenta com um sistema de defesa em várias camadas contra a negação da ciência "pós-verdade".

Já em [56], são apresentados oito simples passos para seguir antes de compartilhar qualquer tipo de notícia:

(1) **CONSIDERE A FONTE:** Clique fora da notícia para investigar o site, sua missão e suas informações de contato.
(2) **LEIA ALÉM:** Os títulos podem ser ultrajantes no esforço de obter cliques. Qual é a história toda?
(3) **VERIFIQUE O AUTOR:** Faça uma pesquisa rápida sobre o autor. Eles são confiáveis? Eles são reais?
(4) **FONTES:** Clique nesses links. Determine se as informações fornecidas realmente apóiam a história.
(5) **VERIFIQUE A DATA:** Repostagem de notícias antigas não significa que sejam relevantes para os eventos atuais.
(6) **ISSO É UMA PIADA?:** Se for muito estranho, pode ser sátira. Pesquise o site e o autor para ter certeza;
(7) **VERIFIQUE SEU VIÉS:** Considere se suas próprias crenças podem afetar seu julgamento; e
(8) **PERGUNTE AOS ESPECIALISTAS:** Pergunte a um bibliotecário ou consulte um site de verificação de fatos.

4.2.3 ***Ferramentas de detecção de fake news.*** Como medidas de combate às *fake news*, várias ferramentas de detecção estão sendo propostas. Tais ferramentas são apresentadas na Tabela 3. A tabela está organizada levando em conta os estudos classificados anteriormente que respondem a QP_3. Dessa forma, a primeira coluna apresenta o estudo, seguida do tipo de detecção da ferramenta, qual a tecnologia utilizada pela ferramenta, os idiomas detectados e o ambiente em que foram feitos os experimentos.

Na revisão da literatura observou-se 13 propostas de ferramentas de detecção de *fake news*, nas quais 84,61% são de detecção por texto e da língua inglesa e 69,23% utilizaram aprendizado de máquina em diversas bases de dados. O Twitter foi a rede social mais utilizada pelos autores como ambiente para a extração de noticias falsas, da mesma forma que as bases de dados BuzzFeed e PolitiFact utilizadas por [60] e [65], também utilizam dados dessa rede social.

Dentre as ferramentas apresentadas, duas foram as que mais se destacaram devido as suas propostas, sendo elas a ferramenta BRENDA desenvolvida por Botnevik et al.[62], que consiste em uma extensão de navegador para detecção de *fake news* e a ferramenta FakeFinder de Tian et al.[63], que se trata de um aplicativo móvel capaz de detectar uma notícia falsa transmitida em tempo real através de *lives* do Twitter, algo que se tornou muito comum hoje em dia na internet. Essa ferramenta analisa os tweets e faz a detecção de noticias enganosas a partir de comentários dos demais usuários.

Demais autores apresentaram ferramentas distintas para detecção de *fake news* a partir de postagens no twitter, como em [57] que apresentou uma abordagem multilíngue e atingiu 81% de precisão

Tabela 3: Classificação dos estudos referente a QP_3.

Ref.	Detecção	Tecnologia	Idioma	Ambiente
[57]	Texto	Rede Neural	Hindi e Bengali	Twitter
[58]	Posição das teclas	Rede Neural	Inglês	Base de dados Univ. de Aalto
[33]	Texto	Aprendizado de máquina e conjunto	Inglês	Twitter
[34]	Texto	Aprendizado de máquina	Inglês	Base de dados próra
[59]	Imagens	Aprendizado de máquina	-	Base de dados FakeNewsNet
[60]	Texto	Aprendizado de máquina	Inglês	PolitiFact e BuzzFeed
[61]	Texto	Aprendizado de máquina	Inglês	Base de dados próra
[62]	Texto	Rede Neural	Inglês	Base de dados própria
[63]	Texto	Aprendizado de máquina	Inglês	Twitter
[64]	Texto	Aprendizado de máquina	Inglês	Base de dados LIAR
[65]	Texto	Aprendizado de máquina	Inglês	FakeNewsNet PolitiFact e BuzzFeed
[66]	Texto	Rede Neural	Inglês	Bade de dados PHEME e Weibo
[67]	Texto	Aprendizado de máquina	Inglês	Bade de dados MetaCOVID

no idioma hindi e a 78% no idioma bengali, e o framework apresentado por [33] que alcançou uma acurácia de até 98%. Por outro lado, Masciari et al. [59] propôs um *framework* de detecção de *fake news* através de imagens, que não mostrou resultados tão satisfatórios quanto o esperado, alcançando 51% de precisão. Após alterações na matriz utilizada para o experimento, o mesmo alcançou 78% de precisão, uma melhora de 27% do inicial. Outro experimento apresentado por [64], utilizando um modelo de construção mental baseado em BERT, forneceu uma precisão de 47%, resultado muito abaixo do esperado comparado aos demais.

5 CONCLUSÃO

Neste estudo, foram apresentados e discutidos os resultados de duas revisões da literatura realizados a fim de identificar o cenário atual dos crimes cibernéticos relacionados ao Covid-19. Em um primeiro momento, foi apresentado e discutido os resultados da revisão da literatura realizado sobre *Phishing e Malware*. Os resultados contribuem apontando a necessidade de constante atualização nas formas de combate, uma vez que os criminosos cibernéticos estão evoluindo suas técnicas e se aproveitam de eventos específicos, como a pandemia, para enganar pessoas em seus momentos de fragilidade e vulnerabilidade, assim como apontando outras formas de prevenção recomendadas na literatura e aqui ressaltadas. A pesquisa também abre margem para um estudo de campanhas de ataques cibernéticos situacionais, relativos à eventos tanto locais quanto globais. Identificar campanhas e possíveis fontes de ataques pode auxiliar na prevenção desses ataques, evitando inúmeras perdas. Nos trabalhos futuros pretende-se ampliar esse estudo para campanhas, identificar possíveis padrões e criar um detector de acordo com os padrões encontrados.

No segundo momento foi apresentada a revisão da literatura sobre as *fake news*, com o objetivo de identificar quais são os impactos da grande circulação da desinformação em tempos de pandemia, maneiras de controle e ferramentas de detecção neste momento de fragilidade mundial. Os resultados mostraram que as *fake news* não só são uma grande antagonista dos profissionais da saúde e órgãos responsáveis, mas também de cadeias de abastecimentos, causando alta demanda de reabastecimento, devido ao pânico gerado. Medidas de conter a disseminação de notícias falsas, como procurar saber mais sobre o assunto o qual gostaria de compartilhar, verificar fontes e autores, também são bons caminhos para resolver esta situação. Porém, ferramentas automatizadas se mostraram grandes aliadas ao combate as *fake news*, pois podem auxiliar no processo de prevenção e detecção de tais ameaças. Sendo assim, esta revisão abre caminho para ampliação da pesquisa na área de detecção das *fake news* dando espaço para criação de uma ferramenta para detecção precoce das *fake news* como trabalhos futuros a fim de mitigar possíveis situações citadas anteriormente.

AGRADECIMENTO

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001 - Ação Emergencial 2020.

REFERÊNCIAS

[1] World Health Organization. Weekly operational update on covid-19. 2020. URL https://www.who.int/emergencies/diseases/novel-coronavirus-2019/situation-reports/. Acessado: 17 nov. 2020.
[2] Ren He, Haoyu Wang, Pengcheng Xia, Liu Wang, Yuanchun Li, Lei Wu, Yajin Zhou, Xiapu Luo, Yao Guo, and Guoai Xu. Beyond the virus: A first look at coronavirus-themed mobile malware, 2020.
[3] Isaac Chin Eian, Ka Yong Lim, Majesty Yeap Xiao Li, Yeo Hui Qi, and Z Fatima. Cyber attacks in the era of covid-19 and possible solution domains. *Preprints*, 2020. doi: 10.20944/preprints202009.0630.v1.
[4] Bernardi Pranggono and Abdullahi Arabo. Covid-19 pandemic cybersecurity issues. *Internet Technology Letters*, n/a(n/a). doi: https://doi.org/10.1002/itl2.247. URL https://onlinelibrary.wiley.com/doi/abs/10.1002/itl2.247.
[5] R. O. Andrade, I. Ortiz-Garcés, and M. Cazares. Cybersecurity attacks on smart home during covid-19 pandemic. In *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, pages 398–404, 2020. doi: 10.1109/WorldS450073.2020.9210363.
[6] Sogo Angel Olofinbiyi and Shanta Balgobind Singh. The role and place of covid-19: An opportunistic avenue for exponential world's upsurge in cyber crime. *International Journal of Criminology and Sociology*, pages 221–230, 2020.
[7] Seth Andrew Evangelista Hoffman. Cybersecurity threats in healthcare organizations. *World Libraries*, 24(1), 2020.
[8] Pavan Duggal. A new order in cyberspace awaits us. *Journal of Law and Administration*, 2020. doi: "https://doi.org/10.24833/2073-8420-2020-2-55-18-24".
[9] Rafael Christian de Matos. Fake news frente a pandemia de covid-19. *Vigilância Sanitária em Debate: Sociedade, Ciência & Tecnologia*, 2020.
[10] Alya Hannah Ahmad Kamal, Caryn Chuah Yi Yen, Mah Hui Ping, and F Zahra. Cybersecurity issues and challenges during covid-19 pandemic. 2020.
[11] Jamil Ispahany and Rafiqul Islam. Detecting malicious urls of covid-19 pandemic using ml technologies. *arXiv preprint arXiv:2009.09224*, 2020.
[12] Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R. C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, 2020.

[13] Kamshad Mohsin. Cybersecurity in corona virus (covid-19) age. *Available at SSRN 3669810*, 2020.
[14] Felix E. Eboibi. Cybercriminals and coronavirus cybercrimes in nigeria, the united states of america and the united kingdom: cyber hygiene and preventive enforcement measures. *Commonwealth Law Bulletin*, 2020.
[15] Kenneth Okereafor and Oluwasegun Adelaiye. Randomized cyber attack simulation model: A cybersecurity mitigation proposal for post covid-19 digital era. *International Journal of Recent Engineering Research and Development*, 2020.
[16] Kenneth Okereafor and Olajide Adebola. Tackling the cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety. *Journal Homepage: http://ijmr. net. in*, 8(2), 2020.
[17] Navid Ali Khan, Sarfraz Nawaz Brohi, and Noor Zaman. Ten deadly cyber security threats amid covid-19 pandemic. 2020.
[18] David Buil-Gil, Fernando Miró-Llinares, Asier Moneva, Steven Kemp, and Nacho Díaz-Castaño. Cybercrime and shifts in opportunities during covid-19: A preliminary analysis in the uk. *European Societies*, pages 1–13, 2020.
[19] Alex R Mathew. Cybersecurity pros warn–covid-19 pandemic as a tool. *International Journal of Engineering and Advanced Technology (IJEAT)*, 9(4), 2020.
[20] Camelia Simoiu, Ali Zand, Kurt Thomas, and Elie Bursztein. Who is targeted by email-based phishing and malware? measuring factors that differentiate risk. In *Proceedings of the ACM Internet Measurement Conference*, IMC '20, page 567–576, New York, NY, USA, 2020. Association for Computing Machinery. ISBN 9781450381383. doi: 10.1145/3419394.3423617.
[21] Martin Jartelius. The 2020 data breach investigations report – a cso's perspective. *Network Security*, 2020(7):9 – 12, 2020. ISSN 1353-4858.
[22] Katelyn Swasey. Insufficient healthcare cybersecurity invites ransomware attacks and sale of phi on the dark web. *Center for Anticipatory Intelligence Student Research Reports*, 2020.
[23] Rennie Naidoo. A multi-level influence model of covid-19 themed cybercrime. *European Journal of Information Systems*, pages 1–16, 2020.
[24] Akashdeep Bhardwaj, Varun Sapra, Aman Kumar, Naman Kumar, and S Arthi. Why is phishing still successful? *Computer Fraud & Security*, 2020(9):15–19, 2020.
[25] Johannes Wiggen. The impact of covid-19 on cyber crime and state-sponsored cyber activities. 2020.
[26] Pengcheng Xia, Haoyu Wang, Xiapu Luo, Lei Wu, Yajin Zhou, Guangdong Bai, Guoai Xu, Gang Huang, and Xuanzhe Liu. Don't fish in troubled waters! characterizing coronavirus-themed cryptocurrency scams, 2020.
[27] Swee Leng Tan, Rossanne G. Vergara, Nasreen Khan, and Shereen Khan. Cybersecurity and privacy impact on older persons amid covid-19: A socio-legal study in malaysia. *Asian Journal of Research in Education and Social Sciences*, 2020.
[28] Tabrez Ahmad. Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. *Available at SSRN 3568830*, 2020.
[29] Jennifer Yang Hui and Teo Yi-Ling. Pandemic and beyond: Phishing in a larger pond. *Global Health Security: COVID-19 Its Impacts*, 2020.
[30] Marites V Fontanilla. Cybercrime pandemic. *Eubios Journal of Asian and International Bioethics*, 30(4):161, 2020.
[31] Ben Collier, Shane Horgan, Richard Jones, and Lynsay Shepherd. The implications of the covid-19 pandemic for cybercrime policing in scotland: A rapid review of the evidence and future considerations. 2020.
[32] Lev Muchnik, Elad Yom-Tov, Nir Levy, Amir Rubin, and Yoram Louzoun. Initial growth rates of epidemics fail to predict their reach: A lesson from large scale malware spread analysis. *arXiv e-prints*, art. arXiv:2008.00445, August 2020.
[33] Mabrook S Al-Rakhami and Atif M Al-Amri. Lies kill, facts save: Detecting covid-19 misinformation in twitter. *IEEE Access*, 8:155961–155970, 2020.
[34] Mohamed K Elhadad, Kin Fun Li, and Fayez Gebali. Detecting misleading information on covid-19. *IEEE Access*, 8:165201–165215, 2020.
[35] Azzam Mourad, Ali Srour, Haidar Harmanani, Cathia Jenainatiy, and Mohamad Arafeh. Critical impact of social networks infodemic on defeating coronavirus covid-19 pandemic: Twitter-based study and research directions. *arXiv preprint arXiv:2005.08820*, 2020.
[36] Bernard Marr. Coronavirus fake news: How facebook, twitter, and instagram are tackling the problem. *Forbes, Mar*, 2020.
[37] Alex Hern. Twitter to remove harmful fake news about coronavirus. *The guardian*, 2020.
[38] Barbara Kitchenham, Rialette Pretorius, David Budgen, O Pearl Brereton, Mark Turner, Mahmood Niazi, and Stephen Linkman. Systematic literature reviews in software engineering–a tertiary study. *Inf. and software technology*, 2010.
[39] Alberto Martín-Martín, Enrique Orduna-Malea, Mike Thelwall, and Emilio Delgado López-Cózar. Google scholar, web of science, and scopus: A systematic comparison of citations in 252 subject categories. *Journal of Informetrics*, 2018.
[40] Mariwan Ahmed Hama Saeed. Malware in computer systems: Problems and solutions. *IJID (International Journal on Informatics for Development)*, 2020.
[41] Ö. F. Yakut and F. Ertam. A digital forensics analysis for detection of the modified covid-19 mobile application. In *2020 5th International Conference on Computer Science and Engineering (UBMK)*, 2020. doi: 10.1109/UBMK50275.2020.9219416.
[42] Rajib Subba. Collective intelligence and international coordination: antidote for the novel biological zero-day exploit# covid-19. *Security Nexus Perspectives*, 2020.
[43] Chi Tran. Recommendations for ordinary users from mitigating phishing and cybercrime risks during covid-19 pandemic. 2020.
[44] Mia Angeline, Yuanita Safitri, and Amia Luthfia. Can the damage be undone? analyzing misinformation during covid-19 outbreak in indonesia. In *2020 International Conference on Information Management and Technology (ICIMTech)*, pages 360–364. IEEE, 2020.
[45] Jose Yunam Cuan-Baltazar, Maria José Muñoz-Perez, Carolina Robledo-Vega, Maria Fernanda Pérez-Zepeda, and Elena Soto-Vega. Misinformation of covid-19 on the internet: infodemiology study. *JMIR public health and surveillance*, 6(2): e18444, 2020.
[46] Michela Montesi. Understanding fake news during the covid-19 health crisis from the perspective of information behaviour: The case of spain. *Journal of Librarianship and Information Science*, page 0961000620949653, 2020.
[47] J Scott Brennen, Felix M Simon, and Rasmus Kleis Nielsen. Beyond (mis) representation: Visuals in covid-19 misinformation. *The International Journal of Press/Politics*, 2020.
[48] Marco Furini, Silvia Mirri, Manuela Montangero, and Catia Prandi. Untangling between fake-news and truth in social media to understand the covid-19 coronavirus. In *2020 IEEE Symposium on Computers and Communications*, 2020.
[49] Claudio Tinoco Mesquita, Anderson Oliveira, Flávio Luiz Seixas, and Aline Paes. Infodemia, fake news and medicine: Science and the quest for truth. *International Journal of Cardiovascular Sciences*, (AHEAD), 2020.
[50] Jon Roozenbeek, Claudia R Schneider, Sarah Dryhurst, John Kerr, Alexandra LJ Freeman, Gabriel Recchia, Anne Marthe van der Bles, and Sander van der Linden. Susceptibility to misinformation about covid-19 around the world. *Royal Society open science*, 7(10):201199, 2020.
[51] Md Al-Zaman et al. Covid-19-related fake news in social media. *COVID-19-Related Fake News in Social Media (June 30, 2020)*, 2020.
[52] Bright Opoku Ahinkorah, Edward K. Ameyaw, John E. Hagan Jr, Abdul-Aziz Seidu, and Thomas Schack. Rising above misinformation or fake news in africa: Another strategy to control covid-19 spread. *Frontiers in Communication*, 2020.
[53] Alberto Ardèvol-Abreu, Patricia Delponti, and Carmen Rodríguez-Wangüemert. Intentional or inadvertent fake news sharing? fact-checking warnings and users' interaction with social media content. *El profesional de la información (EPI)*, 2020.
[54] Gordon Pennycook, Jonathon McPhetres, Yunhao Zhang, Jackson G Lu, and David G Rand. Fighting covid-19 misinformation on social media: Experimental evidence for a scalable accuracy-nudge intervention. *Psychological science*, 2020.
[55] Sander van der Linden, Jon Roozenbeek, and Josh Compton. Inoculating against fake news about covid-19. *Frontiers in Psychology*, 11:2928, 2020.
[56] Salman Bin Naeem and Rubina Bhatti. The covid-19 'infodemic': a new front for information professionals. *Health Information & Libraries Journal*, 2020.
[57] Debanjana Kar, Mohit Bhardwaj, Suranjana Samanta, and Amar Prakash Azad. No rumours please! a multi-indic-lingual approach for covid fake-tweet detection. *arXiv preprint arXiv:2010.06906*, 2020.
[58] Aythami Morales, Alejandro Acien, Julian Fierrez, John V Monaco, Ruben Tolosana, Ruben Vera-Rodriguez, and Javier Ortega-Garcia. Keystroke biometrics in response to fake news propagation in a global pandemic. *arXiv preprint arXiv:2005.07688*, 2020.
[59] Elio Masciari, Vincenzo Moscato, Antonio Picariello, and Giancarlo Sperlí. Detecting fake news by image analysis. In *Proceedings of the 24th Symposium on International Database Engineering & Applications*, pages 1–5, 2020.
[60] Xinyi Zhou, Atishay Jain, Vir V Phoha, and Reza Zafarani. Fake news early detection: A theory-driven model. *Digital Threats: Research and Practice*, 2020.
[61] K Anoop, P Deepak, and VL Lajish. Emotion cognizance improves health fake news identification. In *IDEAS*, volume 2020, page 24th, 2020.
[62] Bjarte Botnevik, Eirik Sakariassen, and Vinay Setty. Brenda: Browser extension for fake news detection. *arXiv preprint arXiv:2005.13270*, 2020.
[63] Lin Tian, Xiuzhen Zhang, and Min Peng. Fakefinder: Twitter fake news detection on mobile. In *Companion Proceedings of the Web Conference 2020*, 2020.
[64] Jia Ding, Yongjun Hu, and Huiyou Chang. Bert-based mental model, a better fake news detector. In *Proceedings of the 2020 6th International Conference on Computing and Artificial Intelligence*, pages 396–400, 2020.
[65] Yi Xie, Xixuan Huang, Xiaoxuan Xie, and Shengyi Jiang. A fake news detection framework using social user graph. In *Proceedings of the 2020 2nd International Conference on Big Data Engineering*, pages 55–61, 2020.
[66] Youze Wang, Shengsheng Qian, Jun Hu, Quan Fang, and Changsheng Xu. Fake news detection via knowledge-driven multimodal graph convolutional networks. In *Proceedings of the 2020 International Conference on Multimedia Retrieval*, 2020.
[67] Kaize Ding, Kai Shu, Yichuan Li, Amrita Bhattacharjee, and Huan Liu. Challenges in combating covid-19 infodemic–data, tools, and ethics. *arXiv preprint arXiv:2005.13691*, 2020.