



Circulação de golpes no WhatsApp entre jovens universitários e o papel da literacia digital na prevenção de *phishing*

Circulation of scams on
WhatsApp among
university students and the
role of digital literacy in
phishing prevention

Daniela Osvald Ramos

Doutora em Ciências da Comunicação pela Universidade de São Paulo. Docente do curso de Educomunicação e do Programa de Pós-Graduação em Ciências da Comunicação da Escola de Comunicações e Artes da Universidade de São Paulo (PPGCOM ECA-USP). É líder do grupo de pesquisa Observatório de Comunicação, Liberdade de Expressão e Censura (OBCOM), e integrante do grupo de pesquisa COM+ (ECA-USP). E-mail: dosvald@gmail.com

Egle Müller Spinelli

Doutora em Ciências da Comunicação pela Universidade de São Paulo. Docente do curso de Jornalismo e do Programa de Pós-Graduação em Comunicação e Práticas de Consumo da ESPM (PPGCOM, ESPM-SP). É líder do grupo de pesquisa Comunicação, Literacia Digital e Consumo (DIGICOM), vice-coordenadora da Cátedra Maria Aparecida Baccega e integrante do grupo de pesquisa COM+ (ECA-USP). E-mail: egle.spinelli@gmail.com



Resumo

Com o isolamento social imposto pela pandemia do Covid19 em 2020, cresceram os golpes na internet. Neste relato desenvolvemos a noção de espaço e literacia digital como abordagem teórica a este fenómeno que está na intersecção do cibercrime e da comunicação digital. O objetivo foi o de identificar como os golpes de *phishing* circularam e se apresentaram para jovens universitários no *WhatsApp* a partir de um questionário online que obteve 356 respostas sobre golpes na internet, realizado de maio a junho de 2020. A observação dos dados demonstra que a noção do espaço no ambiente digital pode ser aplicada para reconhecimento de links falsos, e que a literacia digital tem um papel crucial neste context.

Palavras-chave: Golpes. *Phishing*. Espaço digital. Literacia digital.

Abstract

With the social isolation imposed by the Covid19 pandemic in 2020, scams on the internet grew. In this report we develop the notion of space and digital literacy as a theoretical approach to this phenomenon that is at the intersection of cybercrime and digital communication. The objective was to identify how phishing scams circulated and presented themselves to university students on WhatsApp from an online questionnaire that obtained 356 responses about scams on the internet, carried out from May to June 2020. The observation of the data demonstrates that the The notion of space in the digital environment can be applied to the recognition of false links, and that digital literacy plays a crucial role in this context.

Keywords: Scams. Phishing. Digital space. Digital literacy.

1 Introdução

No isolamento social imposto pela pandemia do Covid19 a partir de março de 2020 até final de 2021 no Brasil, o uso da internet para as mais diversas atividades aumentou. A empresa de hospedagem de arquivos em nuvem Akamai, responsável por 30% do tráfego online no mundo, registrou no Brasil aumento de 112% de acesso à internet em abril de 2020, em relação ao ano anterior (SILVA, 2020).

Desde então, o noticiário tem relatado frequentemente uma ocorrência de golpes por *phishing*: uma técnica que visa “pescar” o usuário através de um site, link, mensagens no *WhatsApp* e plataformas digitais. Os ataques de *phishing* por e-mail:

[...] buscam induzir os destinatários a acreditar que um e-mail é legítimo, a fim de solicitar informações confidenciais (por exemplo, nomes de usuário, senhas, números de cartão de crédito) ou instalar malware. Os ataques de *spear phishing* usam informações pessoais (por exemplo, contatos conhecidos, linguagem da indústria, nomes das vítimas) para criar mensagens mais realistas e persuasivas. (CANFIELD; FISCHHOFF; DAVIS, 2019, p. 2).

Spear pode ser traduzido como “lança” e define os ataques direcionados às vítimas já previamente mapeadas. Essa dinâmica se torna preocupante depois da notícia de vazamento de 200 milhões de dados pessoais de brasileiros em janeiro de 2021, que estão sendo vendidos no mercado clandestino da internet (LOUREIRO, 2021). De posse destes dados verdadeiros, é mais fácil convencer as pessoas que o contato não tem intenção criminosa, e persuadi-las a ceder dados. Este relato tem o objetivo de identificar como os golpes circularam entre jovens universitários no *WhatsApp*, entre maio e junho de 2020 com o objetivo de indicar ações de literacia digital que possam minimizar os golpes na internet. A metodologia é baseada em uma abordagem qualitativa e quantitativa e em uma fundamentação teórica sobre o conceito de espaço e literacia digital.

A coleta de dados sobre a circulação e reação aos golpes no *WhatsApp*, aplicativo no qual a maioria dos golpes relatados ocorreram, foi realizada por meio de um questionário online

disponibilizado para jovens universitários, que contou com duas perguntas de dados demográficos; três perguntas sobre cinco golpes que circularam no início do isolamento social, em abril de 2020; um campo para envio de *prints* de telas dos golpes recebidos; e um campo para comentário de mensagens suspeitas. Obtemos 356 respostas entre maio e junho de 2020 que constituíram o corpus de análise deste relato e que serviram como base para responder a pergunta-chave desta pesquisa:

Q1: Como a compreensão do espaço nas práticas sociais corrobora na constituição de literacias digitais para a prevenção dos golpes pela internet?

Onde acontece o golpe? O ambiente digital e a noção de espaço

O espaço digital permite a sobreposição de diversas camadas que precisam ser conectadas para que possamos compreender a intenção das mensagens. Para Castells (2005), é possível pensar em um espaço de fluxos, que modifica a clássica conexão social do compartilhamento do espaço (contiguidade) com o tempo (simultaneidade), e é formada por três camadas. A primeira seria o suporte material do espaço de fluxos, que trata da configuração de infraestrutura técnica da rede, ponto que tocaremos mais adiante ao discutir a importância de saber decodificar a anatomia do link como literacia digital para a prevenção de golpes. A segunda camada é “constituída por seus nós (centros de importantes funções estratégicas) e centros de comunicação”, a qual Castells (2015, p. 502) comenta “não ser desprovida de lugar, embora sua lógica o seja” o que se relaciona à dificuldade de entendimento da vítima de *phishing* sobre o espaço do *WhatsApp* ou do link da mensagem recebida, ou mesmo sobre a verdadeira origem de um link ou perfil falso. Finalmente, a última camada que se refere à “organização espacial das elites gerenciais dominantes” (CASTELLS, 2005, p. 504), ou seja, “os interesses dominantes específicos a cada estrutura social”. Estas estruturas, embora em sua maioria estejam localizadas espacialmente no Vale do Silício e também na China,

contemporaneamente têm interesses globais, examinados recentemente por Zuboff (2019) e traduzidos nos termos de “capitalismo informacional”, “capitalismo de vigilância” e “economia de dados”. Castells (2005, p. 505) sugere também a hipótese de que “o espaço de fluxos é formado de micro redes pessoais que projetam seus interesses em macro redes funcionais em todo o conjunto global de interações no espaço de fluxos” e que “espaço é a expressão da sociedade” (CASTELLS, 2005, p. 499). Ou seja, este espaço de fluxos tem a projeção das micro redes de interesses escusos na macro rede brasileira.

Esta projeção pode ser melhor compreendida se pensarmos no espaço digital que opera com a lógica da transdução, de maneira a modular o espaço através do processo transdutivo, gerando uma constante renovação espacial de forma reiterativa. A partir desta perspectiva, o espaço é “um evento ou um fazer, um conjunto de desdobramentos de práticas” (KITCHIN; DODGE, 2014, p. 18). Este espaço é carente de “um plano ou uma produção social predeterminada que é ontologicamente fixa” (Ibidem, 2014, p. 18). Emerge como contingencial, relacional, produtivo e dinâmico. É espaço relacional e depende de outros contextos na sua configuração. Machado (2011) explica que “transdução” é um termo emprestado da Física e da Biologia para “(...) designar a transformação e a conformidade de fenômenos a partir de propagações, seja em processos gerais de transmissão, seja em deslocamentos de uma dimensão a outra” (MACHADO, 2011, p. 224). O espaço onde os golpes ocorrem a princípio podem parecer inofensivos, mas se transformam, a partir de um clique em um link, contingencialmente, como um espaço onde ocorre um crime.

Já sobre a localização de lugares no espaço digital, podemos pensar na direção de Gutsche e Hess (2020), que propõe o termo *placeification*, palavra em inglês sem tradução direta para o português, com o significado de “lugarização” da circulação das informações digitais. Neste caso, acessar um link é uma questão de se mover em um espaço, que pode levar a um lugar:

Os espaços podem ser entendidos como geografias demarcadas (como coordenadas em um mapa) ou representações abstratas nas quais vemos o mundo social e que possuem algum significado social - um edifício, um amontoado de terra ou sala de



aula, todos os quais podem ser representações tangíveis do espaço. Em mundos digitais, então, os espaços incluem plataformas, salas de chat ou pontos de entrada interativos para conteúdo online e são locais onde trabalhamos, nos movemos, interagimos, experimentamos, saímos e voltamos. (GUTSCHE; HESS, 2020, p. 3, tradução nossa).

Convém lembrar que a diferença entre espaço e lugar foi bastante explorada pelo geógrafo Tuan (2013), e que é próprio da experiência cultural humana a organização e criação de lugares a partir do espaço. “O que começa como espaço indiferenciado transforma-se em lugar à medida que o conhecemos melhor e o dotamos de valor” (TUAN, 2013, p. 14), por isso nossa casa é reconhecida como “casa” e nos traz o sentimento de segurança. É a partir do lugar que damos sentido à experiência na camada física; na camada digital, podemos nos mover a partir de links e arquivos acessados em lugares como o *WhatsApp*, e-mail, sites conhecidos ou não. Aqui, a noção de espaço e de lugar no consumo midiático e no campo da comunicação pode ajudar a literalmente situar a população diante destas ameaças, pois cada link acionado na internet ocorre no espaço desta arquitetura de lugares não visíveis. “Espaços de notícias digitais também são espaços culturais, relacionados a questões de poder, agência, contestação, pertencimento e relacionamentos entre geografias físico-digitais” (GUTSCHE; HESS, 2020, p. 3-4).

Vale ressaltar que os espaços onde acontecem os golpes visam danificar o patrimônio alheio, mas também são espaços que se relacionam com poder (quem detém o código burla a segurança), agência (a vítima pode impedir o agressor de agir, se tiver competência para reconhecer a ameaça, caso da literacia digital), pertencimento (enredos dos golpes apelam para a busca de uma identidade), e certamente também perpassam relacionamentos por geografias físicas e digitais. Estes espaços são numéricos, compostos de bits 0 e 1, portanto, codificáveis em um nível inédito na cultura. Manovich (2006) já enunciou que a representação numérica¹, um dos princípios das novas mídias, torna as mídias programáveis; e assim, potencialmente, outros fenômenos de ordem social, como o estelionato. Ainda,

¹ Os outros princípios são: modularidade, variabilidade, automatização e transcodificação.

pelo princípio da transcodificação, a codificação dos golpes em espaços físicos é transcodificada para espaços numéricos ou ciberespaço (LÉVY, 2000). Queremos deixar registrado ainda a possibilidade da abordagem da experiência social com o espaço, compilada em várias escolas da sociologia e antropologia por Silvano (2010), mas não nos estenderemos neste tópico.

Literacia digital para a prevenção de golpes

Os golpes na internet se utilizam da perda do referencial espacial da mensagem propiciada pela superabundância de meios digitais como aplicativos de mensagem, redes sociais e e-mail. Para percorrer estes múltiplos locais em constante fluxo comunicacional, os indivíduos precisam ter competências as quais incluem processos de literacia digital. O termo literacia digital (POTTER; MCDUGALL, 2017) abrange distintos pontos, os quais englobam desde o agendamento de questões que envolvem tecnologia e educação até áreas que abarcam a segurança eletrônica.

Outra questão a ser pontuada é que a literacia digital traz a ideia de “várias literacias ou conjuntos de competências que devem coexistir com o objetivo de ser bem-sucedido na era do digital”, como a literacia/alfabetização midiática e informacional (SANTOS; PEDRO, 2016, p. 42). A UNESCO usa o termo Alfabetização Midiática e Informacional (oficialmente, usa-se a sigla MIL, *Media and Information Literacy*) para englobar e inter-relacionar competências informacionais, midiáticas e tecnológicas.

A alfabetização midiática e informacional (MIL) inclui um conjunto de competências para pesquisar, avaliar de forma crítica, usar e contribuir com conteúdo informativo e midiático com sabedoria; conhecimento dos direitos dos indivíduos on-line; entender como combater o discurso de ódio e o cyberbullying on-line; compreender as questões éticas que envolvem o acesso e o uso de informações; e se envolver com mídias e

TIC para promover igualdade, liberdade de expressão, diálogos entre culturas e religiões, paz etc.²

No Brasil a nova Base Nacional Comum Curricular (BNCC) estabelece a educação para os meios como parte obrigatória no currículo no ensino básico. O ensino e aprendizagem sobre lógicas de produção e consumo de mídia nas escolas permite constituir cidadãos que saibam interpretar, refletir e produzir conteúdos pelas tecnologias digitais de informação e comunicação, além de contextualizar ideias e analisar criticamente o que está sendo disponibilizado e compartilhado. A literacia digital implica na reunião destas habilidades, e conforme compilação realizada a partir de Van Deursen e Van Dijck (2011), estas podem ser estabelecidas em quatro dimensões:

- a. Habilidades operacionais para internet: envolvem competências básicas no uso da tecnologia e da internet como operar páginas no navegador, salvar arquivos, fazer buscas e pesquisas, "baixar" aplicativos e softwares.
- b. Habilidades formais de internet: relacionadas com a estrutura hipermídia da internet que requer noção de navegação e orientação ao percorrer as unidades informacionais da internet.
- c. Habilidades informacionais de internet: ações executadas pelos usuários para compreensão e processamento das mensagens que envolvem a capacidade de filtrar informações para alcançar determinadas necessidades.
- d. Habilidades estratégicas de internet: uso da internet como meio de atingir objetivos que resultem em benefícios para a sociedade como estabelecer as ações corretas e decisivas para chegar ao melhor resultado.

As duas primeiras dimensões são relacionadas aos aspectos técnicos do meio e implicam literacias funcionais da internet e, neste estudo, podem se referir ao uso do *WhatsApp* para: receber e responder mensagens; "baixar" e enviar arquivos (textos, imagens, áudios), circular de links; salvar

² Definição de Alfabetização Midiática e Informacional (MIL - Media & Information Literacy) pela UNESCO. Disponível em: <https://en.unesco.org/fieldoffice/amman/Media-Information-Literacy>. Acesso em: 17 jul. 2021.

mensagens e contatos; compartilhar localização; entre outros. Já as dimensões informacionais e estratégicas retratam literacias relacionadas às competências para interpretar e avaliar como a informação é socialmente situada e produzida (LEUNG; LEE, 2012) e, no caso do *WhatsApp*, podem se relacionar a: identificação da procedência; checagem do autor original da mensagem; verificação de endereço eletrônico (URL); fazer pesquisas com palavras-chaves da mensagem; e analisar atentamente a narrativa, o enredo e construção gramatical.

A literacia digital envolve o reconhecimento de uma informação necessária na capacidade de localizar, avaliar e usar efetivamente esta informação nos espaços digitais. Conforme enfatiza Murray (2003, sem p.), "literacia implica mais do que vocabulário e consciência; requer pensamento crítico".

Observação dos dados do questionário online

A partir dos dados coletados pelo questionário online engendramos alguns apontamentos sobre literacias digitais necessárias para identificar possíveis golpes na internet, em especial no *WhatsApp*, apontado pelos participantes desta pesquisa como o lugar onde mais se recebe as mensagens de golpe (62,4%). Foram obtidas 356 respostas a partir da divulgação do questionário no site da Escola de Comunicações e Artes da Universidade de São Paulo, bem como por meio de *mailings* para os alunos do curso de Educomunicação da mesma unidade e para os alunos da Faculdade de Educação da USP. Também foi propagado na *newsletter* do Núcleo de Estudos da Violência da USP em junho de 2020. Os dados demográficos de localização dos respondentes e faixa etária confirmam o público ao qual o questionário foi direcionado, representado por jovens universitários: 43,3% têm entre 21 e 31 anos e 30,9% entre 17 e 20, moradores do estado de São Paulo (93,8%).

Com base nos golpes mais comuns reportados pela pesquisa da Apura³ (2020) sobre casos de *phishing* durante a pandemia do coronavírus, observamos que os respondentes do questionário receberam estratégias de fraudes⁴ similares às identificadas no relatório: 26,1% recebeu a mensagem sobre o álcool gel; 23,3% Netflix grátis no isolamento; 15% auxílio cidadão falso; 36,8% não recebeu nenhuma destas mensagens e 17,1% recebeu outros tipos de mensagem; 9% recebeu a da cesta básica; 5,6% a mensagens sobre o teste de Covid em casa; e 9,3% não sabiam ou não lembravam ter recebido estas mensagens ou outras similares. Mesmo com respostas bem divididas, cerca de 80% dos respondentes tiveram contato com mensagens fraudulentas, o que demonstra a forte presença destes tipos de golpes no *WhatsApp*.

Sobre a reação a estas mensagens ou semelhantes, 53,7% ignoraram, o que indica que mais da metade desta amostra conseguiu reconhecer o potencial de falsidade nas mesmas. Um dos respondentes reportou: "*Recebi um SMS com confirmação do recebimento de auxílio emergencial, mas não havia me cadastrado para receber, logo não cliquei no link*". Outro enfatizou a relevância de se fazer pesquisas sobre o conteúdo e a URL da mensagem recebida antes de ligar ou clicar no link para saber se está caindo realmente em um golpe: "*A mensagem continha um link para o que seria um suposto aplicativo da Caixa para recebimento do auxílio emergencial. Não cliquei, optando em pesquisar sobre o link e a informação. Após tal pesquisa, descobri que o link era enganoso*".

No questionário também recebemos exemplos de mensagens suspeitas recebidas pelos respondentes, as quais puderam ser avaliadas como referência de análise para chegarmos a

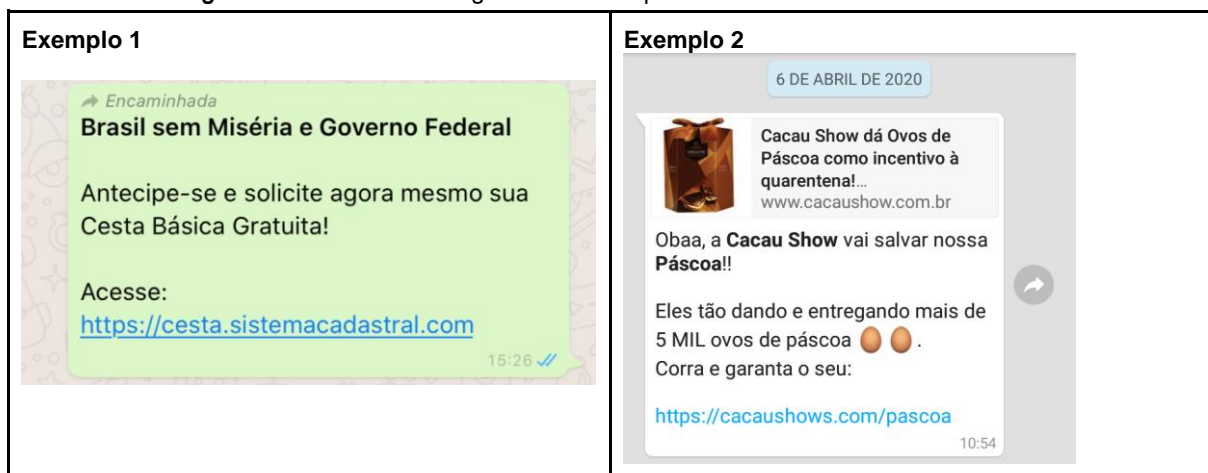
³ Cyberintelligence - Coronaware - ameaças digitais em tempos de pandemia. Report – APURA Cyberintelligence. Disponível em: <https://covidcyber.apura.com.br/Report%2018-06-20%20Edic%CC%A7a%CC%83o-13.pdf>. Acesso em: 17 jul. 2021.

⁴ Foram cinco os tipos de golpes mais frequentes enviados por WhatsApp durante a pandemia da COVID-19: 1) Mensagem do Cievs (Centro de Informações Estratégicas em Vigilância em Saúde) Municipal e Estadual divulgando números telefônicos para casos suspeitos de Covid e teste em casa (a pessoa é incentivada a ligar e a partir daí o golpe acontece); 2) Programa Auxílio Cidadão 2020 de 200 reais do governo federal; 3) Netflix grátis no período de isolamento; 4) Distribuição de álcool gel gratuitamente pela AMBEV, e 5) Distribuição de cesta básica pelo CRAS (Centro de Referência da Assistência Social). As quatro últimas apresentavam um link como armadilha para *phishing*, a "pescaria" que visa fisgar dados sigilosos do dispositivo alheio.

apontamentos sobre algumas dinâmicas e habilidades técnicas e informacionais que envolvem os golpes pela internet.

A seguir temos dois exemplos (figura 1) de mensagens enviadas pelos respondentes que apresentam golpes análogos:

Figura 1 - Links das mensagens não correspondem aos sites oficiais das marcas



Fonte: exemplos enviados pelos participantes do questionário realizado pelos autores.

Estas duas tentativas de golpes chegaram como mensagem de *WhatsApp*, um aplicativo que envia mensagens no espaço íntimo e pessoal (HALL, 1981) por ser acessado unicamente pelo usuário e, conseqüentemente, ser avaliado exclusivamente por ele. Mesmo que hipoteticamente encaminhada por uma pessoa do círculo de confiança, a tentação de acreditar em mensagens que oferecem benefícios pode ser alta. No entanto, quando se clica em um link, mesmo a partir de um espaço que consideramos privado, mas que ao mesmo tempo está acessível no espaço de fluxos (CASTELLS, 2005), e que não é visto e acessado por muita gente como o Facebook, saímos do espaço original da mensagem e somos enviados a outro local; isso acontece por já termos aprendido e normalizado clicar em um link como uma ação sem conseqüências potencialmente perigosas. O espaço inicial se transformou em outro, através do fenômeno da transdução (KITCHIN; DODGE, 2014). O próprio termo

técnico do “link” é a sigla URL - *Universal Resource Locator*, ou “localizador uniforme de recursos”, em tradução livre, indicando que o link está localizado em algum lugar que é físico, pois ocupa o armazenamento de um computador. Não vamos entrar aqui na questão da linguagem culta, dimensão que pode ser observada especialmente na figura 2 e que envolve uma discussão mais ampla sobre alfabetização e o conhecimento da língua portuguesa; mas nos atentamos aos links, que para Gutsche e Hess (2019) levam a uma indicação do lugar de destino que será acessado pelo receptor da mensagem.

Os dois links apresentados (<https://cesta.sistemacadastral.com> e <https://cacaushows.com/pascoa>), não são endereços oficiais (respectivamente, os oficiais são <https://www.gov.br> e <https://www.cacaushow.com.br>) e não estão registrados no Brasil, pela ausência do .br, uma indicação espacial geográfica muito importante a ser observada. Outra questão é que depois do .com, no exemplo 2, é adicionada uma barra /, indicativo de um diretório dentro do computador que hospeda o site, o que se refere a uma localização do arquivo no computador e que se relaciona diretamente à arquitetura do site, o que pode confundir um olhar mais apressado. A indicação do país de origem em uma URL oficial jamais viria depois de uma barra (/), mas sempre depois de um ponto final (.br; .ar; .ru, e assim por diante). A anatomia de uma URL pode ser melhor entendida e visualizada através de um quadro (quadro 1), para que se compreenda a dimensão oculta da circulação dos fluxos dos dados; no caso, com o espaço de fluxos da camada da infraestrutura da internet, como descrito por Castells (2005):

Tabela 1 - Anatomia de uma URL

http://www.shop.com.br/cadernos/cadernosempauta.html			
http://	www.shop.com.br	/cadernos	cadernosempauta.html

<p>Se refere ao tipo de protocolo, no caso, o hipertexto, não seguro, pois não é “https”.</p>	<p>É o domínio do site – se refere à localização numérica dele no ciberespaço. No caso, o www.shop.com.br é uma máscara alfabética para o número.</p>	<p>É o caminho ou diretório no computador para achar o arquivo que vem depois. “Caderno” é como a pasta é nomeada no computador.</p>	<p>Nome do arquivo que está dentro do diretório /cadernos</p>
---	---	--	---

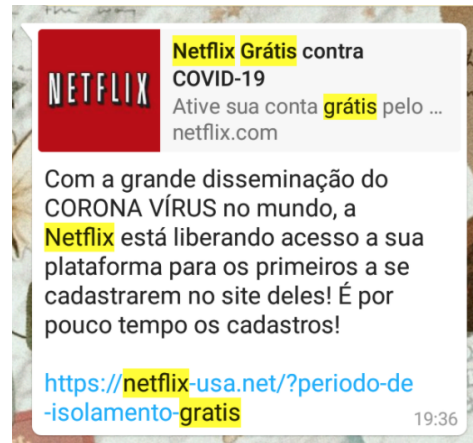
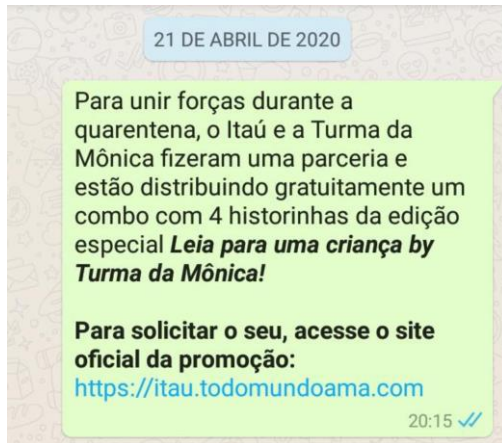
Fonte: Elaborada pelas autoras.

Por outro lado, os exemplos de golpes apresentam uso de protocolo de transferência de hipertexto “https”; o seguro é o “https” (Hypertext Transfer Protocol Secure), que indica uma adicional de transmissão de dados criptografada; ainda, a autenticidade do servidor é verificada por meio de certificados digitais⁵. No exemplo 1, o órgão responsável pela distribuição das cestas básicas no título da mensagem é o Governo Federal, que não se encontra referenciado na URL da mensagem. Já no exemplo 2, o nome da loja no link aparece errado: “cacaushows” ao invés de “cacaushow”. Se fosse uma placa em uma loja de rua, por exemplo, a falta de conexão entre o local e a grafia chamariam atenção e despertariam desconfiança. Porém, como o referencial é uma URL, pode passar despercebido. Em relação ao espaço e lugar, os mesmos cuidados do mundo off-line devem ser transpostos para o on-line. Nos casos citados a localização do estabelecimento não coincide com o lugar indicado e o nome da instituição ou empresa está escrito de forma errada ou não aparece no endereço.

Os exemplos a seguir (figura 2) evidenciam a desconexão do espaço com a simultaneidade (CASTELLS, 2005), para qual as mensagens apelam, como nos exemplos acima, a promoções de produtos e serviços gratuitos (figura 2).

Figura 2 - Mensagem enfatiza a oferta gratuita

⁵ Disponível em: https://pt.wikipedia.org/wiki/Hyper_Text_Transfer_Protocol_Secure. Acesso em: 06 mai. 2021.



Fonte: Exemplos enviados pelos participantes do questionário realizado pelas autoras.

Nestes casos, além de verificar o endereço da URL - que como no caso anterior não aparece a extensão com.br -, é importante pesquisar na internet para saber se existem estas promoções em sites oficiais, conferindo a existência do espaço midiático de origem. Por exemplo, uma rápida busca pelas palavras-chave "Itaú" e "Turma da Mônica" (três respondentes relataram ter recebido mensagens de distribuição gratuita de gibis da Turma da Mônica via Itaú) encontramos uma notícia do Uol⁶ que desmente esta parceria. Um dos respondentes relatou a necessidade de checagem em sites oficiais das empresas, órgãos ou instituições para compreender a veracidade da informação: *"Recebi sites e telefones de promoções bancárias (como pontos Dotz), empréstimos e de produtos disponíveis a preços muito baixos. Não cliço e se fico muito interessada verifico antes se é boato. Pois uma vez circulou sobre o lápis de cor com cor de pele da Faber Castell. Verifiquei que era verdade no site da empresa, me inscrevi e ganhei a caixinha de lápis de cor"*.

Outros exemplos enviados comunicam irregularidades em cadastros ou urgências em fazer atualizações. Estes tipos de golpes atingem práticas e dinâmicas referentes ao espaço do próprio usuário, pois entra em questões particulares de reputação relativas a moral e a ética de quem recebe

⁶ Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/04/23/itau-e-turma-da-monica-desmentem-noticia-falsa-que-circulada-no-whatsapp.htm>. Acesso em: 6 mai. 2021.

a mensagem. É o que se denomina uso de “engenharia social” para a aplicação do golpe: usar pontos sensíveis humanos, manipulação e persuasão para burlar dispositivos de segurança para obter informações sigilosas de uma corporação ou indivíduo (COELHO; RASMA; MORALES, 2013).

Considerações finais

Esta pesquisa indica que para a prevenir a vitimização por golpes é preciso um olhar crítico a partir de um repertório sociocultural tanto dos espaços físicos quanto dos digitais que habitamos, como pela aplicação de competências digitais adquiridas durante o processo educacional e de nossas vivências. Além disso, é crucial a compreensão de que o espaço digital pode se transformar em um espaço perigoso. O questionário online permitiu trazer um recorte da modelagem dos golpes aplicados pelo *WhatsApp* para análise a partir do envio de exemplos de *phishing* recebidos pelos respondentes, e também indicou que os golpes tendem a aproveitar um contexto social do mundo físico para se proliferarem, como a distribuição de ovos na Páscoa ou o cadastramento para receber cesta básica, bem como o uso da engenharia social para dar a falsa sensação de que se está inserido em um ambiente seguro. A amostra da faixa etária universitária indica a possibilidade destes jovens estarem razoavelmente preparados para decodificarem mensagens de golpes.

Neste relato partimos da premissa que a identificação do espaço no fluxo comunicacional digital ajuda a compreender qual literacia precisa ser acionada conforme a situação confrontada, aqui exemplificada pelos golpes nas mensagens que chegam por links no *WhatsApp*. Dessa maneira, apontamos a necessidade do desenvolvimento de pesquisas que demonstrem outros tipos de literacias digitais necessárias em distintos casos que envolvam as interações na internet para nos mantermos seguros.

Referências

CASTELLS, M. **A Sociedade em rede**. São Paulo: Editora Paz e Terra, 2005.



CANFIELD, C.; FISCHHOFF, B.; DAVIS, A. Better beware: comparing metacognition for phishing and legitimate e-mails. **Metacognition Learning**, v. 14, n. 6, p. 343–362, 2019. Disponível em: <https://psycnet.apa.org/record/2019-55852-001>. Acesso em: 28 jun, 2021.

COELHO, C. F., RASMA, E. T.; MORALES, G. Engenharia social: uma ameaça à sociedade da informação. **Perspectivas Online: Exatas & Engenharias**, v. 3, n. 5, p. 34-44, 2013. Disponível em: http://ojs3.perspectivasonline.com.br/index.php/exatas_e_engenharia/article/view/87. Acesso em: 01 jul. 2021.

GUTSCHE, R. E.; HESS, K. Placeification: The Transformation of Digital News Spaces into “Places” of Meaning. **Digital Journalism**, v. 8, n. 5, p. 586-595, 2020. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/21670811.2020.1737557>. Acesso em: 26 jun. 2021.

HALL, E. T. **A Dimensão Oculta**. Rio de Janeiro: Francisco Alves, 1981.

KITCHIN, R.; DODGE, M. **Code/Space**. Software and everyday life. Cambridge, Massachusetts: The MIT Press, 2014.

LEUNG, L.; LEE, P. S. N. The Influences of Information Literacy, Internet Addiction and Parenting Styles on Internet Risks. **New Media & Society**, v. 14, n. 1), p. 117–136, 2021. Disponível em: <https://journals.sagepub.com/doi/10.1177/1461444811410406>. Acesso em: 20 jun. 2021.

LÉVY, P. **Cibercultura**. São Paulo: Editora 34, 2000.

LOUREIRO, R. Vazamento pode ter exposto dados de mais de 200 milhões de brasileiros. **Revista Exame**, São Paulo, 2021. Disponível em: <https://exame.com/tecnologia/vazamento-pode-ter-exposto-dados-de-mais-de-200-milhoes-de-brasileiros/>. Acesso em 15 jun. 2021

MACHADO, I. Ressonâncias do envolvimento e participação com os meios. **Significação**, v. 38, n. 36, 2011. Disponível em: <https://www.revistas.usp.br/significacao/article/view/70954>. Acesso em: 07 jul. 2021.

MANOVICH, L. **El lenguaje de los nuevos medios de comunicación – la imagen en la era digital**. Buenos Aires: Paidós Comunicación, 2006.

MURRAY, J. Contemporary literacy: Essential skills for the 21st century. **MultiMedia Schools**, v. 10, n. 2, p. 15-18, 2003. Disponível em: <https://eric.ed.gov/?id=EJ671768>. Acesso em: 07 jul. 2021.

POTTER, J.; MCDUGALL, J. **Digital Media, Culture and Education Theorising Third Space Literacies**. London: Palgrave Macmillan, 2017.

SANTOS, R. A., PEDRO, L. J. Literacia(s) digital(ais): definições, perspectivas e desafios. **Media & Jornalismo**, v. 15, n. 27, p. 17-44, 2016. Disponível em: <https://repositorio-aberto.up.pt/handle/10216/140693>. Acesso em: 29 jun. 2021.

SILVA, V. H. Exclusivo: Akamai vê uso de internet crescer 112% no Brasil durante pandemia. **Tecnoblog**, 10 jun. 2020. Disponível em <https://tecnoblog.net/344896/exclusivo-akamai-ve-uso-de-internet-crescer-112-no-brasil-durante-pandemia/>. Acesso em: 12 nov. 2020.

SILVANO, F. **Antropologia do espaço**. Lisboa: Assírio & Alvim, 2010.

TUAN, Y. **Espaço e lugar**. A perspectiva da experiência. Londrina: Eduel, 2013.

VAN DEURSEN, A.; VAN DIJCK, J. Internet Skills and the Digital Divide. **New Media & Society**, v. 13, n. 6, p. 893–911, 2011. Disponível em: <https://journals.sagepub.com/doi/10.1177/1461444810386774>. Acesso em: 28 jun. 2021.

ZUBOFF, S. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. Londres: Profile Books, 2019.