ISBN: 978-65-83849-06-9

Aurum EDITORA

CAPÍTULO 23

A IMPORTÂNCIA DA EDUCAÇÃO DIGITAL NA PREVENÇÃO DE CRIMES CIBERNÉTICOS

THE IMPORTANCE OF DIGITAL EDUCATION IN PREVENTING CYBERCRIME

https://doi.org/10.63330/aurumpub.012-023

David Aguiar
Curso MBA Executivo em Segurança Cibernética.

RESUMO

O presente trabalho aborda a importância da educação digital como estratégia fundamental na prevenção de crimes cibernéticos. A pesquisa, de natureza bibliográfica e qualitativa, foi desenvolvida a partir da análise de produções teóricas recentes sobre criminalidade digital, perfis de criminosos virtuais, impactos sociais e medidas educativas voltadas à segurança da informação. O estudo evidencia que os crimes cibernéticos têm se diversificado e aumentado em escala global, atingindo desde usuários comuns até grandes corporações, sendo praticados por agentes com diferentes perfis, como hackers, crackers, carders e cyberterroristas. Diante desse cenário, destaca-se a educação digital como um mecanismo de empoderamento e proteção para indivíduos e comunidades, por meio do desenvolvimento de competências críticas, éticas e técnicas relacionadas ao uso seguro da tecnologia. A alfabetização digital, desde a infância, se mostra imprescindível para o reconhecimento de ameaças, prevenção de fraudes, combate à desinformação e proteção de dados pessoais. Os resultados apontam que uma abordagem educativa contínua e articulada entre escola, família, instituições públicas e privadas é capaz de reduzir vulnerabilidades, conscientizar usuários sobre seus direitos e deveres no ambiente digital e promover uma cultura de segurança cibernética. Conclui-se que investir em educação digital é investir na construção de uma sociedade mais segura, ética e consciente na era da informação.

Palavras-chave: Educação digital; Crimes cibernéticos; Segurança da informação; Cidadania digital; Prevenção.

ABSTRACT

This paper addresses the importance of digital education as a fundamental strategy in the prevention of cybercrime. The research, which is bibliographic and qualitative in nature, was developed based on the analysis of recent theoretical works on digital crime, profiles of cybercriminals, social impacts, and educational measures aimed at information security. The study shows that cybercrime has diversified and increased on a global scale, affecting everyone from ordinary users to large corporations, and is committed by agents with different profiles, such as hackers, crackers, carders, and cyberterrorists. Given this scenario, digital education stands out as a mechanism for empowering and protecting individuals and communities through the development of critical, ethical, and technical skills related to the safe use of technology. Digital literacy, starting in childhood, is essential for recognizing threats, preventing fraud, combating misinformation, and protecting personal data. The results indicate that a continuous and coordinated educational approach between schools, families, and public and private institutions can reduce vulnerabilities, raise awareness among users about their rights and duties in the digital environment, and promote a culture of cybersecurity. It is concluded that investing in digital education is investing in building a safer, more ethical, and more conscious society in the information age.

Keywords: Digital education; Cybercrime; Information security; Digital citizenship; Prevention.

1 INTRODUÇÃO

A crescente expansão do uso da internet e das tecnologias digitais tem transformado profundamente os modos de viver, trabalhar, aprender e se comunicar. No entanto, essa transformação digital também tem gerado novos riscos e desafios, entre os quais se destacam os crimes cibernéticos. Tais delitos, que envolvem o uso da tecnologia da informação como meio ou como fim das infrações, vêm se tornando cada vez mais sofisticados e impactantes, atingindo desde usuários comuns até grandes corporações, além de instituições públicas e privadas. A diversidade e a complexidade dessas ameaças demandam, mais do que nunca, estratégias eficazes de prevenção e conscientização, sendo a educação digital uma das mais promissoras nesse sentido. A presente pesquisa parte da premissa de que a formação digital crítica, ética e técnica é fundamental para reduzir a vulnerabilidade dos cidadãos diante dos riscos do ambiente virtual, promovendo uma cultura de segurança cibernética e responsabilidade digital.

Autores como Castells (2003), Lévy (2010) e Floridi (2013) apontam que a sociedade em rede exige uma nova ecologia cognitiva, na qual o domínio das tecnologias deve ser acompanhado de consciência crítica, ética e cidadã. A cibercultura, longe de ser apenas um conjunto de ferramentas, configura-se como um campo complexo de relações, onde o conhecimento técnico deve andar lado a lado com a compreensão dos impactos sociais do uso da tecnologia. A ausência de educação digital contribui para a proliferação de práticas nocivas como phishing, roubo de identidade, cyberbullying, fraudes online, entre outros. Segundo Almeida e Araújo (2021), muitas vítimas de crimes virtuais poderiam ter evitado prejuízos significativos caso tivessem recebido orientações prévias sobre segurança na internet e proteção de dados. Nesse contexto, a educação digital aparece como uma ação preventiva, que capacita indivíduos a reconhecerem e evitarem riscos, protegendo-se de práticas maliciosas e atuando com responsabilidade nas redes.

O objetivo deste trabalho é analisar a importância da educação digital na prevenção de crimes cibernéticos, destacando como o conhecimento e a formação crítica em segurança da informação podem contribuir para a construção de uma cidadania digital consciente. A hipótese que orienta esta pesquisa é a de que quanto maior o nível de alfabetização digital de um indivíduo, menor sua exposição a crimes cibernéticos, visto que estará mais preparado para identificar ameaças, proteger seus dados e adotar comportamentos seguros no uso das tecnologias. A justificativa para o desenvolvimento deste estudo reside na crescente incidência de delitos virtuais e na necessidade urgente de promover uma cultura de segurança digital que não se limite a soluções técnicas, mas que envolva também processos educativos contínuos.

A metodologia utilizada na elaboração deste trabalho é de natureza qualitativa e bibliográfica, baseada na análise de produções acadêmicas, relatórios institucionais e publicações de autores renomados da área da segurança digital, educação e sociologia da tecnologia. A estrutura do artigo está organizada em três partes principais. Na primeira, são apresentados os principais tipos de crimes cibernéticos, suas características e consequências, bem como os perfis dos criminosos envolvidos. Na segunda parte, discute-

se o papel da educação digital como ferramenta preventiva, relacionando conceitos como letramento digital, cidadania digital, ética e responsabilidade no uso das TICs. Na terceira e última parte, são analisadas as estratégias e políticas públicas que podem ser adotadas para promover a educação digital em larga escala, com foco na formação de educadores, na integração curricular e na atuação conjunta entre escola, família e sociedade.

Dessa forma, o trabalho pretende contribuir com o debate acadêmico e social sobre a segurança cibernética, ressaltando que soluções tecnológicas, por mais avançadas que sejam, não substituem a formação crítica e consciente dos usuários. Conclui-se que investir em educação digital é investir na prevenção de crimes, na proteção da integridade dos cidadãos e na construção de um espaço virtual mais seguro, democrático e inclusivo.

1.1 CRIMES CIBERNÉTICOS

Os crimes cibernéticos podem ser classificados em duas categorias principais: os ataques sofisticados e os crimes viabilizados pela tecnologia**.** Os primeiros se caracterizam pelo uso de técnicas avançadas e ferramentas complexas, como invasões (hacking), malwares e ações de extorsão por meio de ataques DDoS. Tais práticas exigem elevado conhecimento técnico. Já os crimes viabilizados pela tecnologia correspondem a delitos tradicionais que se utilizam do meio digital para sua execução, como fraudes virtuais, ciberterrorismo e furtos online. Embora nem sempre dependam de habilidades especializadas, esses crimes se valem da tecnologia para fins ilícitos e representam ameaças relevantes, variando em sua sofisticação técnica (Interpol, 2017).

Conforme Nascimento (2016), os cibercriminosos utilizam uma diversidade de softwares maliciosos para cometer delitos digitais. Dentre eles, os "cookies" têm capacidade de coletar dados sensíveis, como senhas e números de cartões de crédito. Já os "spywares" funcionam como programas de espionagem, repassando informações do usuário a terceiros sem autorização. Os "spammings" consistem em e-mails não solicitados, que comprometem a privacidade e congestionam caixas de entrada. As mensagens falsas conhecidas como "hoaxes" disseminam desinformações e geralmente vêm acompanhadas de vírus. Os "sniffers", por sua vez, acessam dispositivos para extrair dados. "Cavalos de Troia" são malwares que se infiltram em sistemas por meio de arquivos aparentemente inofensivos, roubando informações sigilosas. Os "backdoors", semelhantes aos cavalos de Troia, se aproveitam de brechas no sistema e podem ser inseridos de forma dolosa ou acidental. Os vírus danificam softwares e configurações, enquanto os "worms" se replicam entre computadores sem intervenção humana, podendo deletar arquivos.

Durante o 8º Congresso da ONU sobre Prevenção do Delito e Justiça Penal, realizado em Havana em 1990, foi elaborada uma lista de crimes relacionados ao uso de computadores, incluindo fraudes digitais, falsificações e alterações em dados e programas. Já em 2000, no 10º Congresso da ONU em Viena, essa

lista foi ampliada para abarcar crimes mais recentes, como espionagem industrial, sabotagem de sistemas, lavagem de dinheiro, jogos ilegais, fraudes contra consumidores, pornografia infantil, invasão de sistemas protegidos e obtenção indevida de senhas (Nascimento, 2016).

O phishing é considerado um dos ataques cibernéticos mais comuns e danosos (Deloitte, 2019). Segundo Pinheiro (2020), trata-se de uma estratégia baseada em enganar o usuário para que este interaja com conteúdos falsos, como sites clonados ou links maliciosos, levando ao roubo de dados ou à violação de acesso. Essa técnica é uma forma de engenharia social, onde a manipulação psicológica tem papel central na exploração da confiança da vítima. Entre as variações da prática estão o *scam*, *blind phishing* e *clone phishing*, que utilizam mensagens e páginas falsas para extrair dados pessoais e bancários. O *spear phishing* tem como alvo grupos específicos, enquanto o *whaling* visa executivos de alto escalão. Já o *vishing* utiliza ligações telefônicas, o *smishing* envolve mensagens de texto enganosas, e o *pharming* redireciona usuários a sites falsos por meio da manipulação de DNS (Salviano, 2021). Tais métodos podem causar prejuízos financeiros consideráveis para indivíduos e organizações.

O ransomware, por sua vez, é um tipo de malware que bloqueia o acesso ao sistema ou criptografa dados do usuário, exigindo pagamento para liberar as informações. Usuários domésticos são frequentemente vítimas, por possuírem sistemas de segurança mais frágeis. Alguns ransomwares são relativamente simples de neutralizar, enquanto outros utilizam técnicas complexas, como persistência pós-reinicialização e criptografia robusta. Existe ainda o chamado *ransomware falso*, que não realiza a criptografia de fato, mas utiliza mensagens intimidadoras para extorquir dinheiro (Simoiu, 2019).

No campo da fraude financeira, destacam-se crimes como roubo de identidade, clonagem de cartões de crédito e fraudes em pagamentos online. Esses delitos estão entre os mais recorrentes na esfera cibernética e movimentam bilhões de dólares todos os anos (Chen, 2023). Com a pandemia da COVID-19, houve uma explosão no número de denúncias de fraudes online, com aumento de até 400% em 2020, segundo o FBI (2021).

Outro problema significativo é o cyberbullying**,** definido pelo uso de dispositivos eletrônicos com a intenção de causar sofrimento psicológico contínuo às vítimas. Apesar da internet proporcionar inúmeras possibilidades de interação, muitas pessoas acabam compartilhando conteúdos ofensivos sem considerar as consequências emocionais que podem provocar nos outros (Hinduja, 2021).

Por fim, os ataques DDoS (Distributed Denial of Service) têm como objetivo sobrecarregar servidores para torná-los inacessíveis a usuários legítimos. Os tipos mais comuns são os ataques por inundação, que enviam volumes massivos de dados a um servidor até que ele colapse (Zargar, 2013). Também há ataques de baixa taxa, como o "Slowloris", desenvolvido pelo grupo Anonymous, que explora falhas na camada de aplicação. Esses são mais difíceis de detectar e demandam menos recursos, mas continuam sendo altamente prejudiciais.

1.2 EXEMPLOS DE CRIMINOSOS

Existem diferentes perfis de indivíduos envolvidos com práticas ilícitas no ambiente virtual. Os hackers, conforme Nogueira (2008), são pessoas com amplo domínio sobre informática e que se motivam por desafios intelectuais, não tendo, necessariamente, a intenção de cometer crimes. Muitas vezes, eles se dedicam a identificar falhas em sistemas digitais, não para explorá-las ilegalmente, mas como forma de demonstrar vulnerabilidades. Em diversos casos, são contratados por empresas justamente para garantir a segurança de informações sigilosas e prevenir fraudes eletrônicas. O conhecimento técnico desses indivíduos costuma ser ampliado por formação acadêmica na área de tecnologia, o que lhes permite criar e modificar softwares e hardwares, bem como descobrir novas utilidades em sistemas computacionais.

Em contraste, de acordo com Oliveira (2006), os crackers compartilham um nível semelhante de conhecimento técnico com os hackers, mas suas intenções são distintas. Eles não apenas acessam sistemas indevidamente, mas também causam prejuízos, deixando mensagens ofensivas e, em alguns casos, danificando seriamente os sistemas invadidos.

Assunção (2008) introduz a figura do "Hacker White-Hat", também conhecido como “hacker ético” ou “hacker de chapéu branco”. Este profissional se destaca por seu vasto conhecimento técnico, muitas vezes adquirido de forma autodidata e movido por paixão pela área. Sua atuação é voltada à segurança da informação, realizando testes autorizados de intrusão com o objetivo de fortalecer os sistemas e não para causar danos.

Já Silva (2021) distingue outros perfis especializados em crimes cibernéticos. Os phreakers são peritos em telecomunicações e se envolvem em fraudes relacionadas a chamadas telefônicas, utilizando linhas convencionais ou celulares clonados. Os carders, por sua vez, concentram-se na obtenção de dados de cartões de crédito, normalmente por meio de programas espiões instalados nos dispositivos das vítimas. Por fim, os cyberterroristas desenvolvem códigos maliciosos, como vírus e bombas lógicas, capazes de comprometer sistemas inteiros, afetando especialmente grandes servidores e gerando prejuízos econômicos significativos ao provocar a indisponibilidade de serviços. Dessa forma, cada uma dessas categorias exerce um papel específico — muitas vezes ilícito — dentro do vasto e complexo universo dos crimes virtuais.

1.3 A IMPORTÂNCIA DA EDUCAÇÃO DIGITAL NA PREVENÇÃO DE CRIMES CIBERNÉTICOS

No contexto da sociedade contemporânea, marcada pela interconectividade global e pelo crescimento acelerado das tecnologias da informação e comunicação (TICs), a educação digital emerge como uma necessidade urgente e estratégica para a prevenção de crimes cibernéticos. A ascensão da cultura digital tem proporcionado inúmeros benefícios, como o acesso facilitado ao conhecimento, novas formas de interação social e avanços em setores como saúde, economia, educação e segurança pública. No entanto,

paralelamente a essas conquistas, também se intensificaram os riscos e ameaças provenientes do uso indevido ou inconsciente da tecnologia, revelando a vulnerabilidade de indivíduos, instituições e sistemas frente aos delitos cibernéticos.

Segundo Castells (2003), vivemos na era da sociedade em rede, na qual a informação circula de forma dinâmica e massiva, transformando não apenas as estruturas econômicas, mas também os modos de vida e relações sociais. Nesse cenário, a educação digital se configura como uma ferramenta essencial para preparar os cidadãos a exercerem uma participação crítica, ética e segura no ambiente virtual. De acordo com Lévy (2010), a cibercultura não pode ser compreendida apenas como um conjunto de técnicas ou plataformas, mas como uma nova ecologia cognitiva e social, exigindo novos modos de aprendizagem e de conscientização.

A carência de conhecimento técnico e crítico sobre o funcionamento das redes, sobre privacidade digital, segurança de dados e legislação cibernética contribui significativamente para o aumento da exposição a fraudes, golpes, roubo de identidade, assédio virtual, cyberbullying, phishing, ransomware e outras formas de ataque. Conforme relatado por Almeida e Araújo (2021), muitas das vítimas de crimes digitais poderiam ter evitado as situações de risco caso tivessem acesso prévio a conteúdos educacionais voltados à segurança cibernética. Isso revela a importância da alfabetização digital não apenas em termos operacionais — saber usar uma ferramenta —, mas também formativos, desenvolvendo habilidades de análise crítica, responsabilidade digital e conduta ética.

A educação digital preventiva deve começar desde os anos iniciais da educação básica e se estender ao longo da vida, considerando que o acesso à internet ocorre cada vez mais precocemente e os riscos acompanham essa tendência. Crianças e adolescentes são especialmente vulneráveis, pois muitas vezes não possuem discernimento suficiente para identificar condutas maliciosas ou conteúdos prejudiciais. Segundo o relatório da SaferNet Brasil (2023), houve um aumento expressivo de denúncias relacionadas ao aliciamento online, exploração sexual infantil e discurso de ódio praticados em ambientes virtuais. A ausência de orientação adequada nas escolas e em casa contribui para esse cenário alarmante.

Nesse sentido, iniciativas de educação digital devem integrar currículos escolares, ações comunitárias, campanhas públicas e políticas educacionais, promovendo um letramento digital amplo que abarque temas como proteção de dados, identidade digital, ética nas redes, verificação de informações, combate à desinformação, e prevenção a golpes e fraudes. Como destaca Brito (2020), a educação digital crítica pode capacitar os usuários a reconhecerem vulnerabilidades, a questionarem práticas duvidosas e a adotarem medidas proativas de proteção, reduzindo substancialmente o número de vítimas de crimes online.

Ademais, é essencial que os professores, gestores escolares e familiares também estejam preparados para mediar essas aprendizagens. A formação continuada de educadores sobre segurança digital é uma condição básica para que a escola cumpra seu papel formativo nesse campo. O Ministério da Educação

(MEC), em diversas diretrizes curriculares, já reconhece a necessidade de integrar as competências digitais ao ensino, mas a aplicação prática ainda encontra entraves, como a falta de infraestrutura tecnológica, ausência de programas formativos e resistência institucional (Silva & Ramos, 2019).

Além da dimensão educacional, a conscientização digital deve ser compreendida também como uma questão de cidadania e de responsabilidade social. Conforme Floridi (2013), filósofo da informação, viver na era digital exige não apenas novos saberes técnicos, mas uma nova ética informacional, na qual os sujeitos reconheçam os impactos de suas ações nas redes e desenvolvam uma consciência crítica sobre o uso das tecnologias. Nesse contexto, a educação digital se articula com os direitos humanos, o combate às desigualdades tecnológicas (exclusão digital) e a construção de uma cultura de paz no ciberespaço.

Para que essa transformação seja efetiva, é necessário que os governos invistam em políticas públicas integradas, incentivando a criação de programas de educação digital comunitária, a inclusão digital de populações vulneráveis, a ampliação da conectividade com segurança e a articulação entre os setores público, privado e acadêmico. A segurança cibernética não pode depender apenas de firewalls, softwares antivírus ou legislações repressivas: ela depende, sobretudo, da formação crítica e consciente dos usuários.

Em suma, a educação digital representa uma das principais estratégias de prevenção aos crimes cibernéticos, pois capacita indivíduos a reconhecerem riscos, se protegerem de ameaças e agirem com responsabilidade ética no ambiente digital. Como afirma Almeida (2021), o investimento em educação digital é o caminho mais eficaz para promover segurança, liberdade e cidadania na era da informação.

2 CONCLUSÃO

Diante do cenário contemporâneo marcado pela crescente dependência das tecnologias da informação e comunicação, este trabalho evidenciou que os crimes cibernéticos representam uma ameaça real e crescente à segurança de indivíduos, organizações e instituições públicas. A pesquisa demonstrou que tais delitos vêm se sofisticando com o avanço tecnológico, o que exige não apenas soluções técnicas e legais, mas também estratégias educativas que promovam uma cultura de responsabilidade, criticidade e ética no uso da tecnologia. Nesse sentido, a educação digital mostrou-se uma ferramenta indispensável para a prevenção de crimes virtuais, ao capacitar os usuários a identificar riscos, proteger seus dados e agir de forma consciente no ambiente digital.

A análise bibliográfica realizada apontou que os crimes cibernéticos não são homogêneos, abrangendo desde ataques técnicos sofisticados, como phishing, ransomware e DDoS, até crimes tradicionais adaptados ao meio digital, como fraudes financeiras e assédio online. Também foram discutidos os diferentes perfis de criminosos digitais, destacando-se a importância de reconhecer essas tipologias para formular estratégias preventivas mais eficazes. A partir disso, reforçou-se a necessidade de uma formação digital contínua e abrangente, que vá além do domínio técnico e inclua aspectos éticos, sociais e legais do

uso da internet.

A alfabetização digital, desde a infância, e o envolvimento de todos os agentes sociais — escolas, famílias, governos e setor privado — foram apontados como fundamentais para a construção de uma sociedade digital mais segura e justa. A hipótese de que a educação digital pode reduzir a vulnerabilidade frente aos crimes cibernéticos foi confirmada ao longo do estudo, uma vez que usuários mais bem informados tendem a adotar comportamentos preventivos, evitando cair em armadilhas digitais ou se tornar vítimas de fraudes e ataques virtuais.

Portanto, conclui-se que o investimento em educação digital não deve ser visto como um recurso secundário, mas sim como uma política pública prioritária, integrada às ações de segurança cibernética e promoção da cidadania. Formar cidadãos conscientes, críticos e responsáveis digitalmente é o caminho mais sustentável e eficaz para enfrentar os desafios impostos pela criminalidade virtual na era da informação.

REFERÊNCIAS

ALMEIDA, S.; ARAÚJO, T. Segurança digital e cidadania na era da informação. Revista Brasileira de Tecnologias Educacionais, v. 15, n. 3, p. 67-85, 2021.

ASSUNÇÃO, M. F. A. Segredos do hacker ético. 3. ed. Florianópolis: Visual, 2008.

BRITO, Carolina M. Educação digital crítica: entre os riscos e as possibilidades de uma formação cidadã. Educação & Sociedade, Campinas, v. 41, n. 151, p. 1–19, 2020.

CASTELLS, Manuel. A sociedade em rede. 6. ed. São Paulo: Paz e Terra, 2003.

CHEN, Shuai; HAO, M.; DING, F. Exploring the global geography of cybercrime and its driving forces. Humanit Soc Sci Commun, v. 10, 71, 2023. Disponível em: https://doi.org/10.1057/s41599-023-01560-x.

DELOITTE. Understanding phishing techniques. Deloitte & Touche Enterprise Risk Services Pte Ltd, 2019. Disponível em: https://www.deloitte.com/lu/en/services/consulting-risk/research/phishing- ransomware-how-to-prevent-threats.html. Acesso em: 28 jul. 2025.

FEDERAL BUREAU OF INVESTIGATION. Internet crime report. U.S. Government Printing Office, 2021. Disponível em: https://www.ic3.gov/AnnualReport/Reports/2021_IC3Report.pdf. Acesso em: 28 jul. 2025.

FLORIDI, Luciano. A revolução da informação: Ética, identidade e privacidade na era digital. Rio de Janeiro: Zahar, 2013.

HINDUJA, S.; PATCHIN, J. W. Cyberbullying Identification, Prevention, and Response. Cyberbullying Research Center, 2021.

INTERPOL. Cybercrime. INTERPOL, 2017. Disponível em: www.interpol.int/5267/file. Acesso em: 29 jul. 2025.

LÉVY, Pierre. Cibercultura. 4. ed. São Paulo: Editora 34, 2010.

NASCIMENTO, N. L. Crimes cibernéticos. Fundação Educacional do Município de Assis – FEMA, 2016. Disponível em: https://cepein.femanet.com.br/BDigital/arqTccs/1311401614.pdf. Acesso em: 29 jul. 2025.

NOGUEIRA, J. H. M. A nova face do crime. Revista Per.cia Federal, Ano III, n. 9, jul. 2001.

OLIVEIRA, W. J. Dossiê hacker: técnicas profissionais para conhecer e proteger-se de ataques. São Paulo: Digerati Books, 2006.

PINHEIRO, P. P. Segurança Digital - Proteção de Dados nas Empresas. 1. ed. São Paulo: Grupo GEN, 2020.

SAFERNET BRASIL. Relatório Anual de Atividades 2023. Disponível em: https://www.safernet.org.br. Acesso em: 5 ago. 2025.

SALVIANO, E. M.; SANTOS, J. P. R.; SILVA, M. A. Principais tipos de ataques Phishing e mecanismos de segurança. Trabalho de Conclusão de Curso (Graduação) – Centro Universitário do Planalto Central Apparecido dos Santos, 2021.

SILVA, E. C. S. Proteção contra os Crimes Cibernéticos no Brasil: A Necessidade de uma Legislação Específica e Atualizada. Pontifícia Universidade Católica de Goiás, Escola de Direito e Relações Internacionais, 2021.

SILVA, L.; RAMOS, J. Desafios da educação digital na escola pública brasileira. *Cadernos de Formação Docente*, v. 12, n. 2, p. 112–130, 2019.

SIMOIU, C. et al. "I was told to buy a software or lose my computer. I ignored it": A study of ransomware. In: *Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS*. USENIX Association, 2019.

ZARGAR, S. T.; JAMES, J.; DAVID, T. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys and Tutorials*, v. 15, n. 4, p. 2046–2069, 2013.