Open Access License Notice

Positioning Cybersecurity as a Pillar of Safety in Occupational Therapy

Heather T. Bednarz
School of Education
Wilkes University
Wilkes-Barre, PA
heather.bednarz@wilkes.edu
0009-0006-9867-3060

Jane Blanken-Webb
School of Education
Wilkes University
Wilkes-Barre, PA
jane.blankenwebb@wilkes.edu
0000-0003-4656-5739

Abstract—The rapid digitalization of society has transformed occupational therapy practice, introducing both opportunities and challenges. As occupational therapists increasingly rely on electronic documentation, telehealth, and assistive technologies, cybersecurity is emerging as a critical concern. This position paper argues that occupational therapy is a vital domain for the integration of cybersecurity education, emphasizing the need to safeguard sensitive patient information, enhance digital literacy, and address the unique vulnerabilities faced by occupational therapy clients. The paper outlines the key intersections of occupational therapy and cybersecurity education, highlighting the impact of cyber threats on healthcare, the importance of digital literacy, and the role of occupational therapy in educating and protecting vulnerable populations. Recommendations are provided for integrating cybersecurity education into occupational therapy curricula and fieldwork education to better prepare practitioners for the evolving digital landscape. By integrating cyber safety principles into occupational therapy education, the field can fulfill its mission of enhancing individuals' participation in meaningful activities by equipping practitioners with the skills necessary to protect patient data, manage evolving digital risks, and ensure safe, effective care in a technology-driven world.

Keywords—*occupational therapy, cyber safety, digital citizenship, cybersecurity education, healthcare*

I. INTRODUCTION

In 1969, the precursor to the Internet was launched to support the moon landing, and it crashed before a complete message was sent [1]. In the fourth industrial revolution, 4.5 billion people used the Internet daily for shopping, business, social interaction, and education [1]–[3]. Technology has drifted from a tool to enhance life to a crucial aspect of daily living [4]. With the rapid growth of technology, cybersecurity has become an integral part of safety for all [5]. Cybersecurity threats affect most industries, private individuals, and governments [6]. Between 2019 and 2022, internet fraud increased by 8% [7]. In 2023, 353,027,892 people were affected by data breaches [8]. Cybersecurity threats are expected to grow, rising from millions of dollars of damage to an estimated 10.5 trillion dollars of damage by 2025 [8]. The necessity of using technology in daily life has grown due to the expansion of digitalization of the world [9]. As a result, cybersecurity is becoming more critical to daily life, and its importance will only increase in the coming years.

As the digital and physical worlds converge, industries like healthcare, education, and commerce are profoundly impacted, with cybersecurity becoming a critical aspect of safety [10]. Occupational therapy, a healthcare domain focused on enhancing participation in daily activities, is significantly affected by these changes. Occupational therapists now use electronic documentation, telehealth, and therapeutic technologies, all of which present cybersecurity risks. This paper argues that cybersecurity education is essential within occupational therapy, highlighting how it enhances patient safety, supports digital literacy, and prepares practitioners to navigate the complexities of the digital age.

II. CYBERSECURITY IN HEALTHCARE

Not only has daily life been changed by the collision of the physical and digital worlds, but many industries, such as agriculture, commerce, healthcare, and education, have also changed [10]. These technological advancements have significantly impacted occupational therapy [11]. Practitioners now rely on electronic documentation, underscoring the critical need for understanding cybersecurity, particularly concerning HIPAA regulations [11].

As the digital world expands, cybersecurity risks have permeated all fields. Healthcare, including occupational therapy, faces unique cybersecurity risks due to its reliance on electronic health records, telehealth, and assistive digital technologies. Breaches in this sector not only compromise patient confidentiality but also disrupt critical healthcare services [12]. Unlike other industries, cyberattacks in healthcare can lead to immediate patient harm, such as ransomware attacks delaying emergency care [12]. It is imperative that all healthcare professionals and students have a clear understanding of safety procedures and cybersecurity laws as they relate to patient privacy. Procedures to safeguard information are vital for all healthcare professionals and students [13].

Many healthcare fields, including occupational therapy, have been affected by the opportunities and challenges created by rapidly changing technological developments [14]. The expansion of technology has created an increased need for cybersecurity awareness among occupational therapy practitioners [15]. This is further underscored by the fact that electronic documentation is now standard and required by law [16]. New practice areas have also emerged, such as telehealth, which has had an increasing role since the outbreak of COVID19 [17]. Due to this, occupational therapy practitioners and all healthcare professionals, in general, have an increased responsibility to understand cybersecurity principles for securing confidential information [18].

The expansion of technology will continue to change healthcare. For example, the integration of the Vennue chatbot in pharmacy has expanded access to screening by pharmacists for diabetes to people in under-developed countries [19]. The advancement and use of chatbots have also created new cybersecurity concerns [19]. Healthcare needs not only to meet the challenges currently created by advancements in technology but also to be prepared to meet the cybersecurity concerns that will arise from future technological developments.

III. THE EXPANDING ROLE OF CYBERSECURITY IN OCCUPATIONAL THERAPY PRACTICE

The integration of cybersecurity in occupational therapy is an emerging and essential focus in response to the increasing digitalization of society [15]. Beyond the clerical need to understand cybersecurity for safeguarding sensitive information, occupational therapists have seen an increase in the clinical need to evaluate patients' technological skills, as they are employed to maximize participation in meaningful activities and interpersonal interactions.

Indeed, the use of assistive technologies has been a cornerstone of occupational therapy practice for many years [15]. With the digitization of society, digital assistive technologies have taken hold in occupational therapy practice to maximize independence [15]. Digitalization has already changed how occupational therapy practitioners evaluate, treat, and make recommendations for improved safety and independence [20]. Occupational therapy practitioners leverage artificial intelligence, the Internet of Things, and virtual reality to improve patient outcomes [20]. For example, 3D printing has been used to create splints and prosthetics [21]. In addition, virtual reality has been used to simulate situations patients will need to function upon discharge [21].

According to the World Federation of Occupational Therapy, the role of occupational therapy practitioners in digital assistive technology is expanded to the education of caregivers and other professionals as well as clients [15]. Digital technology has been noted to have a role in self-care and leisure [22]. Concerning self-care, occupational therapists use technology for online shopping and banking [22]. Other applications of digital technology in occupational therapy treatment include leisure activities such as downloading music and videos [22]. Social media participation has emerged as a new and significant occupation for many individuals, influencing various aspects of daily life [4]. As people increasingly engage with social media platforms, the role of occupational therapy expands to encompass the promotion of safe and independent technology use [4].

As technology advances, occupational therapy practitioners need to adapt to the changes [21]. Assessments will need to be modified to meet the changes [21]. For example, the clock test, which is common to assess visual field cuts, may need to be changed or eliminated due to the use of the creation of an analog clock [21].

IV. OCCUPATIONAL THERAPY'S UNIQUE ROLE IN SUPPORTING PATIENT SAFETY

At the same time, occupational therapy practitioners are uniquely qualified to understand and respond to the safety concerns of patients [23]. Thus, we argue that the unique talent of occupational therapy practitioners to address safety concerns can and should be extended to an explicit focus on cyber safety.

People with cognitive disabilities or cognitive decline face the same threats as the public [24]. However, people with decreased cognition risk falling victim to cybersecurity risks more than others [25]. For example, tasks essential to decreasing cybersecurity concerns require increased cognitive efforts such as problem-solving and memory [26]. Since 2014, older Americans have been defrauded, hacked, or otherwise victimized, leading to an estimated $650 million per year in damages [27]. The currently available research finds a need for intervention regarding digital literacy in older adults [28]. According to the Federal Trade Commission, older Americans are the most targeted for frauds masquerading as tech support [29]. Occupational therapy professionals strive to foster independence and safety across all functional tasks in various settings. Drawing a parallel between occupational therapy and cyber safety can help bolster safety and autonomy in both physical and virtual environments.

Occupational therapy's involvement in promoting safe and meaningful social media participation aligns with its broader mission of supporting clients in leading fulfilling lives [4]. By integrating digital literacy, safe routines, and strategies for maintaining identity and privacy, occupational therapists empower individuals to engage with technology and social media to enhance their well-being and protect them from potential harm [4].

Occupational therapist practitioners must accept the new challenges presented by the expansion of digital technology by traversing beyond traditional clinical settings to encompass digital literacy and cyber safety education to enhance safety and independence [30]. By promoting safe technology use and incorporating cybersecurity principles into practice, occupational therapists can improve their clients' independence, participation in meaningful activities, and

overall well-being [20]. Incorporating cyber safety in occupational therapy education is critical for preparing future practitioners to meet the challenges of the digital age [30]. As technology continues to evolve, so too must the skills and knowledge of occupational therapists. Integrating cyber safety and digital literacy into the curriculum will ensure that occupational therapy professionals are equipped to provide comprehensive care that addresses the technological aspects of daily life [30].

V. A CURRICULAR GAP IN OCCUPATIONAL THERAPY EDUCATION

Technology is integral to all human occupations [30]. Therefore, as technology advances, the education of occupational therapy students must be redefined to progress in the profession and prepare students for new and ever-changing demands as professionals [30]. The need to integrate technology in occupational therapy education has been recognized since the 1990s [30]. The Accreditation Council for Occupational Therapy Education (ACOTE) has outlined the need for technology to be included in the educational standards of occupational therapists and occupational therapy assistants [31].

However, Nunez-Canal et al. [32] identified a gap in the literature regarding educators' ability to meet digital literacy needs. A lack of preparation for technology use has been identified in occupational therapy, as reports indicate that practitioners feel inadequately prepared to integrate emerging technologies into their treatments [33]. Some reports suggest that only two-thirds of occupational therapy practitioners feel adequately trained to incorporate technology into intervention [30] safely.

Integrating cyber safety into occupational therapy practice and education is vital when developing the skills of current and future occupational therapy professionals [14]. One aspect of digital literacy is evaluating information and ensuring cyber safety [15]. The role of digital literacy in occupational therapy is well documented [15]. However, McKinstry et al. [14] report a lack of integration of cyber safety concepts in occupational therapy practice, noting a lack of research in occupational therapy education.

Research regarding cybersecurity has been limited in occupational therapy. Much of the currently available research areas have concentrated on simulated educational experiences, education pertaining to 3D printing of adaptive devices, and hybrid education [34]-[36]. While the need to integrate technology into occupational therapy practice and education has been well documented, a lack of research nevertheless remains in terms of how to utilize technology safely within occupational therapy practice and education [14], [15]. As it stands, integrating cyber safety into occupational therapy education has been treated in the literature largely as a footnote—it now requires a dedicated focus to address the critical gaps in preparing occupational therapy practitioners for the digital challenges of modern healthcare.

VI. RECOMMENDATIONS FOR INTEGRATING CYBERSECURITY INTO OCCUPATIONAL THERAPY EDUCATION AND PRACTICE

Integrating targeted cybersecurity education into occupational therapy curricula can address the existing gaps by equipping students and practitioners with the necessary skills to manage digital risks, protect patient data, and foster a culture of digital literacy essential for modern healthcare practice. To effectively bridge these gaps, we propose several key recommendations.

Various professions have made efforts to incorporate cybersecurity into their curricula. One approach currently being utilized is project-based learning, which integrates cybersecurity and digital literacy concepts into education [37]. Unlike traditional lecture-based methods, project-based learning emphasizes student-completed projects as the primary teaching strategy [37]. This approach has been shown to significantly enhance digital literacy among the students evaluated [37]. Additionally, another technique used in K-12 education to promote digital literacy is 1:1 computing [38], which aims to provide technological education to students who might not otherwise have access to such resources [38].

A. Accreditation Bodies and Licensure Requirements Should Address Cybersecurity Education

A critical step toward integrating cybersecurity into occupational therapy practice is for education accreditation bodies and licensure requirements to address this concern explicitly. The current standards for the National Board for Certification (NBCOT) in Occupational Therapy exam do include technology [39]. However, cyber safety and cybersecurity are not listed in the areas tested [39]. Organizations like the Accreditation Council for Occupational Therapy Education (ACOTE) and NBCOT play pivotal roles in setting the standards for educational programs and professional competencies. Including digital literacy and cyber safety as part of these standards would signal the importance of digital safety in occupational therapy. By mandating that digital literacy and cyber safety be integrated into curricula, accreditation bodies can ensure that future occupational therapists are adequately prepared to navigate the complexities of digital healthcare environments. This approach not only enhances patient safety but also positions occupational therapy as a forward-thinking profession equipped to handle the technological demands of modern practice.

As a part of occupational therapy education, fieldwork educators should be empowered to incorporate cybersecurity and cyber safety into the clinical education experience. Fieldwork education combines textbook topics with real world experience. Due to this connection, fieldwork educators have a unique opportunity to educate students regarding cyber safety in a real-world situation. Fieldwork educators should be provided with a list of topics and tools which could enhance their ability to identify important cyber safety concepts with students in a clinical environment (see Appendix).

B. *Fostering Interdisciplinary Networks Between Cybersecurity and Occupational Therapy Professionals*

To address the rapidly evolving digital landscape, we propose the formation of a network of interdisciplinary collaboration between cybersecurity educators and occupational therapy professionals. Similar to the way occupational therapists work alongside physical therapists, speech-language pathologists, doctors, nurses, and teachers in clinical settings, there is a need to incorporate cybersecurity experts into the team when addressing cyberhealth concepts and digital adaptations in therapy. This collaboration would enable occupational therapy practitioners to gain valuable insights into the risks associated with digital technologies and empower them with strategies needed to mitigate them. By working closely with cybersecurity educators, occupational therapists would enhance their ability to educate patients and caregivers on safe digital practices, ultimately creating safer virtual environments. Such partnerships empower therapists to extend their expertise in promoting independence and safety into the digital realm, ensuring that clients are equipped to navigate both physical and virtual spaces confidently.

C. *Professional Associations Should Define and Advocate for the Role of Cybersecurity in Occupational Therapy*

Occupational therapy is influenced by numerous statewide, national, and international organizations that set the profession's standards and goals. As we enter a new era in human existence, the occupational therapy profession has a unique opportunity to establish itself as a leading force in ensuring cyber safety for patients, thus setting a standard of excellence in this vital aspect of healthcare. Professional associations that uphold and define the field of occupational therapy, such as the American Occupational Therapy Association (AOTA) and the World Federation of Occupational Therapists (WFOT), should take a decisive stance on the role of occupational therapy practitioners in the digital world. These organizations have the chance and responsibility to advocate for integrating cyber safety as a fundamental component of occupational therapy practice. By spearheading the effort to include digital literacy and cybersecurity in the profession's standards, these associations can position occupational therapists as leading experts in addressing the unique challenges that emerge at the convergence of the physical and digital realms. Formulating clear guidelines and best practices for securely utilizing digital technologies in treatment enhances the credibility of occupational therapy and ensures that practitioners are equipped to deliver comprehensive, technology-informed care. This proactive approach will help protect patient data, optimize therapeutic outcomes, and reinforce occupational therapy's commitment to enhancing safety and independence in all aspects of life.

D. *Recommendations for Future Research*

Extensive research is still needed in this area. Although occupational therapy recognizes the necessity of incorporating technology, current studies tend to overlook the critical role of equipping practitioners and students with the knowledge required to ensure safety. Firstly, research should investigate what is being taught to occupational therapy students regarding cybersecurity and cyber safety. Are classroom and fieldwork experiences effectively preparing students to address the new challenges posed by our increasingly digital world? Secondly, it is important to assess the level of knowledge that current practitioners and educators possess regarding cybersecurity and cyber safety. Lastly, research should explore how occupational therapy practitioners are integrating cyber safety and cybersecurity into their daily practices. Are they simply adhering to company protocols for securing patient data, or are they actively educating patients about how to maintain their safety in a digital environment?

VII. CONCLUSION

Positioning cybersecurity as a pillar of safety in occupational therapy is essential as the field increasingly intersects with digital technology. The profession's longstanding commitment to patient safety must now extend into the digital realm. By integrating cybersecurity education into occupational therapy, the field of occupational therapy can ensure that practitioners are equipped to protect sensitive patient data, address digital risks, and foster a culture of safety that spans both physical and virtual environments. This approach not only aligns with occupational therapy's core mission of enhancing client independence and well-being but also reinforces the profession's role as a leader in promoting safety across all aspects of life.

REFERENCES

[1] A. Kozyreva, S. Lewandowsky, and R. Hertwig, "Citizens versus the internet: Confronting digital challenges with cognitive tools," 2020.

[2] M. Núñez-Canal, M. de las M. de Obesso, and C. A. Pérez-Rivero, "New challenges in higher education: A study of the digital competence of educators in Covid times," Technological Forecasting and Social Change, vol. 174, p. 121270, Jan. 2022, doi: https://doi.org/10.1016/j.techfore.2021.121270.

[3] M. Xu, J. M. David, and S. H. Kim, "The fourth industrial revolution: Opportunities and challenges," International Journal of Financial Research, vol. 9, no. 2, pp. 90–95, Feb. 2018, doi: https://doi.org/10.5430/ijfr.v9n2p90.

[4] S. Eckberg Zylstra, K. Erler, W. Nakamura, and B. Kennell, "Social Media as Occupation: Implications for Occupational Therapy Practice," The Open Journal of Occupational Therapy, vol. 8, no. 2, pp. 1–6, Apr. 2020, doi: https://doi.org/10.15453/2168-6408.1670.

[5] C. S. Lee and D. Kim, "Pathways to Cybersecurity Awareness and Protection Behaviors in South Korea," Journal of Computer Information Systems, pp. 1–13, Feb. 2022, doi: https://doi.org/10.1080/08874417.2022.2031347.

[6] F. Cremer et al., "Cyber Risk and cybersecurity: a Systematic Review of Data Availability," The Geneva Papers on Risk and Insurance - Issues and Practice, vol. 47, no. 3, Feb. 2022, doi: https://doi.org/10.1057/s41288-022-00266-6.

[7] J. Alagood, G. Prybutok, and V. R. Prybutok, "Navigating Privacy and Data Safety: The Implications of Increased Online Activity among Older Adults Post-COVID-19 Induced Isolation," Information, vol. 14, no. 6, p. 346, Jun. 2023, doi: https://doi.org/10.3390/info14060346.

[8] A. St. John, "Data breaches in 2023: Analyzing the numbers and impacts," Cybersecurity Journal, vol. 30, no. 1, pp. 44-56, 2024.

[9] M. Larsson-Lund and A. Nyman, "Occupational challenges in a digital society: A discussion inspiring occupational therapy to cross thresholds and embrace possibilities," Scandinavian Journal of Occupational Therapy, vol. 27, no. 8, pp. 1–4, Jan. 2019, doi: https://doi.org/10.1080/11038128.2018.1523457.

[10] A. Loubier, "Is Society Moving In The Right Direction With Technology Rapidly Taking Over The World?," Forbes, Feb. 20, 2024. Accessed: Sep. 15, 2024. [Online]. Available: https://www.forbes.com/sites/andrealoubier/2021/06/01/is-society-moving-in-the-right-direction-with-technology-rapidly-taking-over-the-world/

[11] E. Masselink, "Considering Technology in the Occupational Therapy Practice Framework," *The Open Journal of Occupational Therapy*, vol. 6, no. 3, Jul. 2018, doi: https://doi.org/10.15453/2168-6408.1497.

[12] C. Abraham, D. Chatterjee, & R.R. Sims. (2019). "Muddling through cybersecurity: Insights from the US healthcare industry". Business Horizons, vol. 62, no. 4, pp. 539–548.

[13] M. J. Swede, V. Scovetta, and M. Eugene-Colin, "Protecting Patient Data Is the New Scope of Practice: A Recommended Cybersecurity Curricula for Healthcare Students to Prepare for this Challenge.," PubMed, vol. 48, no. 2, pp. 148–155, Jan. 2019.

[14] C. McKinstry, T. Iacono, A. Kenny, J. Hannon, and K. Knight, "Applying a digital literacy framework and mapping tool to an occupational therapy curriculum," Australian Occupational Therapy Journal, Feb. 2020, doi: https://doi.org/10.1111/1440-1630.12644.

[15] I. Margot-Cattin, A. Deblock-Bellamy, J. Wassmer, Ritchard Ledgerd, Claudia von Zweck, and N. World, "Worldwide Survey on Digital Assistive Technology (DAT) Provision," Occupational Therapy International, vol. 2024, pp. 1–7, Feb. 2024, doi: https://doi.org/10.1155/2024/9536020.

[16] L. F. Dmytryk, "Entry-level occupational therapy electronic health record education model," SIS Quarterly Practice Connections, vol. 7, no. 2, pp. 10-13, 2022.

[17] S. Dahl-Popolizio, H. Carpenter, M. Coronado, N. J. Popolizio, and C. Swanson, "Telehealth for the provision of occupational therapy: Reflections on experiences during the COVID-19 pandemic," Int. J. Telerehabil., vol. 12, no. 2, pp. 77-92, Dec. 2020. doi: 10.5195/ijt.2020.6328. Erratum in: Int. J. Telerehabil., vol. 13, no. 1, pp. e6382, Jun. 2021. PMID: 33520097; PMCID: PMC7757642.

[18] L. H. Yeo and J. Banfield, "Human factors in electronic health records cybersecurity breach: An exploratory analysis," Perspectives in Health Information Management, vol. 19, Spring 2022.

[19] S. Mierzwa, S. Souidi, T. Conroy, M. Abusyed,H. Watarai,and T. Allen . "On the Potential, Feasibility, and Effectiveness of Chat Bots in Public Health Research Going Forward". Online *J Public Health Inform*. 2019 Sep 19;11(2):e4. doi: 10.5210/ojphi.v11i2.9998. PMID: 31632598; PMCID: PMC6788896.

[20] American Occupational Therapy Association, "Occupational therapy profession: Scope of practice definitions," 2023. [Online]. Available: https://www.aota.org/-/media/corporate/files/advocacy/scope-of-practice-chart-10-21.pdf.

[21] L. Lui "Occupational therapy in the fourth industrial revolution," *Canadian Journal of Occupational Therapy*, vol. 85, no. 4, pp. 272-283, 2018.

[22] M. C. Verdonck and S. Ryan, "Mainstream technology as an occupational therapy tool: Technophobe or technogeek?," The British Journal of Occupational Therapy, vol. 71, no. 6, pp. 253-256, 2008. doi: 10.1177/030802260807100607.

[23] P. Roberts, M. Robinson, J. Furniss, and C. Metzler, "Occupational therapy's value in provision of quality care to prevent readmissions," American Journal of Occupational Therapy, vol. 74, no. 3, pp. 7403090010p1, 2020. doi: 10.5014/ajot.2020.743002.

[24] "Cybersecurity and Older Americans," Cybersecurity and Infrastructure Security Agency, 2012. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520and%2520Older%2520Americans.pdf.

[25] J. N. Rocheleau, H. Chalghoumi, J. Jutai, S. Farrell, Y. Lachapelle, and V. Cobigo, "Caregivers' role in cybersecurity for aging information technology users with intellectual disabilities," Cyberpsychology, Behavior, and Social Networking, vol. 24, no. 9, pp. 624-629, 2021.

[26] J. Kävrestad, J. Rambusch, and M. Nohlberg, "Design principles for cognitively accessible cybersecurity training," Computers & Security, vol. 137, 2024, Art. no. 103630.

[27] K. Fazzini, "Here's how online scammers prey on older Americans, and what they should know to fight back," CNBC, Nov. 23, 2019. [Online]. Available: https://www.cnbc.com/2019/11/23/new-research-pinpoints-how-elderly-people-are-targeted-in-online-scams.html

[28] K. Robinson-Bert, M. Jones, M. Seely, A. Turpin, M. Waller, and J. Yarn, "Bridging the digital literacy divide: Addressing the virtual context within the community-dwelling older adult population," OT Practice, vol. 25, no. 4, 2020.

[29] E. Fletcher, "Older adults hardest hit by tech support scams," Federal Trade Commission, Mar. 7, 2019. [Online]. Available: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2019/03/older-adults-hardest-hit-tech-support-scams.

[30] K. M. Dishman, J. Duckart, and L. J. Hardman, "Perceptions of assistive technology education from occupational therapists certified as assistive technology professionals," American Journal Occupational Therapy, vol. 75, no. 2, 2021.

[31] Accreditation Council for Occupational Therapy Education (ACOTE), "2018 Accreditation Council for Occupational Therapy Education (ACOTE) Standards and Interpretive Guide," July 31, 2020. [Online]. Available: https://acoteonline.org/wp-content/uploads/2020/10/2018-ACOTE-Standards.pdf.

[32] M. Núñez-Canal, M. de Obesso, and C. A. Pérez-Rivero, "New challenges in higher education: A study of the digital competence of educators in COVID times," *Technol. Forecast. Soc. Change*, vol. 174, 2021, Art. no. 121270. doi: 10.1016/j.techfore.2021.121270.

[33] American Occupational Therapy Association, Ethical Considerations Relevant to Emerging Technology-Based Interventions [Online]. Available: https://www.aota.org/member-login?redirectURL=https://www.aota.org/practice/practice-essentials/ethics. [Online; subscription required].

[34] P. Barnard-Ashton, "E-lecturer feedback of the inclusion of blended learning in undergraduate occupational therapy," *EDULEARN10 Proceedings*, pp. 492-499, 2010. [Online]. Available: https://library.iated.org/view/BARNARDASHTON2010ELE.

[35] S. Benham and S. San, "Student technology acceptance of 3D printing in occupational therapy education," *The American Journal of Occupational Therapy*, vol. 74, no. 3, pp. 7403205060p1-7403205060p7, 2020.

[36] T. Grant, Y. Thomas, P. Gossman, and L. Berragan, "The use of simulation in occupational therapy education: A scoping review," *Australian Occupational Therapy Journal*, vol. 68, no. 4, pp. 345-356, 2021.

[37] R. AlAli, "Enhancing 21st century skills through integrated STEM education using project-oriented problem-based learning.:" *GeoJournal of Tourism and Geosites*, vol 53, no. 2, pp. 421–430, 2024 https://doi.org/10.30892/gtg.53205-1217

[38] J. R. Power, A. T. Mugrove, & B. H. Nichols. "Teachers Bridging the Digital Divide in Rural Schools with 1:1 Computing". *Rural Educator*, vol. 41, no. 1, pp. 61–76, 2020

[39] National Board for Certification in Occupational Therapy, "Examination Content". 2022 [Online]. Available: https://www.nbcot.org/-/media/PDFs/2022_OTR_Content_Outline.pdf

APPENDIX

Resource Guide for Addressing Cyber Safety in Fieldwork Education

Occupational therapy fieldwork education should provide students with practical cyber safety and cybersecurity applications for occupational therapy practice. Topics to address in fieldwork education can be categorized into clerical and clinical applications.

Clerical topics include:

- Corporations are responsible for the cybersecurity education of their employees.
- Be critical of emails from unknown users
- Activities of a single user can affect an entire network.

Clinical topics include:

- Cybercriminals can record information from online games.
- Freebies can be scams
- Free WiFi can open information up to hackers
- Not all online payment systems are reliable

Important for both clinical and clerical practice:

- Software updates are essential for cybersecurity
- When possible, use two-factor authentication
- Pop-up window can be the source of viruses

Recommended practice: Students engaging in occupational therapy fieldwork education should assess and reflect upon their cybersecurity awareness and/or habits. Follow-up reflection through dialogue should be embedded within fieldwork education as relevant clerical and clinical applications present themselves.

- Examples of assessment tools include: The Cybersecurity Assessment Inventory (CAIN) :

  file:///C:/Users/scran/Downloads/jcp-03-00005.pdf
- S2Me: https://s2me.io/