



MAINTAINING FAMILY PRIVACY AND SECURITY IN THE DIGITAL AGE

Aldi Akbar^{1*}, Arif Kuswanto², Budi Rustandi Kartawinata³

¹Business Administration, School of Economi and Business, Telkom University Bandung, Email: aldiakb@telkomuniversity.ac.id

² Business Administration, School of Economi and Business, Telkom University Bandung Telkom Bandung, Email : arifkuswanto@telkomuniversity.ac.id

³ Business Administration, School of Economi and Business, Telkom University Bandung Bandung, Email : budikartawinata@telkomuniversity.ac.id

*email Correspondent: aldiakb@telkomuniversity.ac.id

DOI: <https://doi.org/10.62567/jpi.v1i2.877>

Abstract

This activity aims to provide parents and teachers of Pandanwangi PAUD with a basic understanding of the importance of maintaining privacy and security in the use of digital technology, as well as providing practical guidance on how to protect personal information and secure digital devices used by family members. The methods used in this educational activity are lectures, group discussions, and case simulations. The results of this educational activity show that the participants have a better understanding of the importance of maintaining family privacy and security in the digital era, are more aware of the risks in cyberspace and are able to identify and overcome these threats better. The conclusion of this activity is that education about digital privacy and security is very important to be given to the community, especially parents and teachers who have a big role in educating children.

Keywords: Digital privacy, Family safety, Education, Digital literacy

1. INTRODUCTION

The digital era has provided many conveniences and benefits for people in various aspects of life, from communication, education, to the economy. (Xia et al., 2024). However, this technological development also brings new challenges, especially related to digital privacy and security. (Nair & Tyagi, 2021). Therefore, it is important for people, especially parents and teachers, to have a good understanding of how to maintain family privacy and security in the digital age.

This community service activity was carried out with the aim of providing education on how to maintain family privacy and security in the digital era. The main targets of this activity are parents and teachers in the Pandanwangi Kindergarten/PAUD environment in Bandung City. The selection of this target is based on the important role that parents and teachers have in educating and protecting children from various threats in cyberspace. By providing education to parents and teachers, it is hoped that they can become agents of change who are able to increase digital literacy and awareness of the importance of privacy and digital security in the surrounding environment.

This educational activity covers several important aspects, including an introduction to the basic concepts of digital privacy and security, the types of threats that can lurk in cyberspace, and practical



steps to protect personal information and secure digital devices. The educational material was delivered using lectures, group discussions, and case simulations, so that participants could understand and apply the knowledge they had gained in their daily lives.

Quach et al. (2022), Digital privacy is the right of every individual to control their personal information and determine who can access it. In a family context, digital privacy includes protecting the personal information of family members, including children, from misuse by irresponsible parties. Digital security, on the other hand, includes measures taken to protect digital devices and the data stored on them from threats such as hacking, malware and phishing. These two aspects are interrelated and equally important to keep families safe and comfortable in the digital age. (LADO, 2024). Threats to digital privacy and security can come from a variety of sources, including insecure websites and apps (Asaad & Saeed, 2022), malicious software (Chopra et al., 2024), fraud and cyberattacks (Afaq et al., 2023). Therefore, it is important for parents and teachers to have adequate knowledge on how to recognize and address these threats. One of the first steps is to identify safe websites and apps before giving children permission to use them. In addition, parents and teachers also need to teach children about the importance of keeping their personal information private, such as full names, addresses, phone numbers and financial information.

In this digital era, the use of social media has become an integral part of everyday life. Social media allows users to share information, communicate with friends and family, and get various useful information (Jain et al., 2021). However, social media can also be a source of threats to digital privacy and security if not used wisely (Bhattacharya et al., 2023). Therefore, in this educational activity, participants were given an understanding of how to use social media safely, including how to set account privacy, recognize unsafe content.

(Huang et al., 2022) The more personal information we share online, the greater the potential for data leakage. This can result in financial loss, false identities, and further misuse of data (DeLiema et al., 2021). It is important for us as individuals, families and communities to raise awareness of the importance of personal data protection in the digital era.

Companies, and individuals need to take proper precautionary measures to protect personal data. Electronic devices such as smartphones, computers, or tablets that are connected to the internet are an entry point for various security threats. To keep our devices safe, we need to ensure that they are always updated with the latest security patches, use strong passwords, and be on the lookout for suspicious links or files.

In addition to keeping electronic devices safe, it is also important to educate family members, especially children, about safe internet usage. Children's digital literacy skills do not grow on their own but require guidance and direction from parents and family (Barnes & Potter, 2021). Maintaining family privacy and security in the digital age requires vigilance and proactive measures from all parties. By raising awareness, keeping devices secure, and educating family members, we can minimize risks and keep our family safe when using digital technology.

In an effort to overcome this problem, community service activities through counseling are one of the effective solutions. This activity aims to improve financial management skills for those in the environment of Pandangwangi PAUD, as well as provide information on how to improve family welfare. One of the locations chosen for this activity is around Pos PAUD Pandanwangi, which is a gathering place for many families with preschool children.

Pos PAUD Pandanwangi is an early childhood education institution established since 2011 with the National School Principal Number (NPSN) 69759716 under the auspices of the Pandanwangi Jaya Foundation and located on Jl. Kencana Wangi No. 3 Cijawura Village. Buahbatu Sub-district, Bandung City. Pandanwangi PAUD was established in 2011 and began to obtain an operational permit on July 20, 2011, issued by the Office of Investment and One-Stop Integrated Services of Bandung City with register number: 0084/IPSPNFI/IX/2022/DPMPTDP.



Pandanwangi Kindergarten/PAUD is a place to learn to play and have fun with the vision of becoming a superior school that builds children's character from an early age. Pos PAUD Pandanwangi believes that every child is an individual who must be nurtured and nurtured with love. Pos PAUD Pandanwangi's mission is to create a learning environment that supports children's development holistically and encourages them to grow confidently into various creative and blessings. Here children learn through project-based learning and play designed to stimulate their curiosity creativity and thinking ability. Entitas also prides itself on providing an inclusive environment where every child is accepted and valued without exception. Not only learning inside the classroom, we also organize class outings, providing a fun learning experience outside at night while introducing them to the wider world. And don't forget that we also support parents through special parents learning environment programs to help you accompany your child's development in a fun and effective way.

Overall, this community service activity on maintaining digital security and privacy succeeded in achieving its goals in empowering young families in the Pandanwangi PAUD environment in Bandung City. This success cannot be separated from careful planning, effective implementation, and continuous evaluation. This activity is expected to be a model for other community service programs that aim to increase the productivity and welfare of young families.

2. RESEARCH METHOD

This social activity is in the form of consultation and education services to the target group which is divided into two stages. The target group consists of teachers/educators and parents of students at PAUD Pandanwangi. The first step is planning in the form of coordination between the organizers and the target community, starting with administrative materials such as referral forms and letters of willingness from the target community that contain roles, responsibilities, rules and functions. This phase also determines the date of implementation, the number of participants and other implementation techniques. So the method used is qualitative by utilizing relevant and up-to-date reference sources.

The second stage is the implementation in the form of counseling delivered offline (outside the network) which takes place in the school hall. The technical implementation included: (1) Opening or welcome; (2) Delivery of counseling material; (3) Questions and answers; (4) Closing or closing in the form of a summary of activities.

3. RESULT AND DISCUSSION

Result

This series of community service programs was carried out onsite on Wednesday, May 28, 2025 (10.30-13.00 WIB) which was attended by 28 participants consisting of teachers and parents of Pos PADU Pandanwangi students. The activity was divided into four agendas consisting of providing material, question and answer / discussion, closing, and ending with a group photo session. The provision of material begins with current issues that are rampant in the community related to digital financial security platforms.



Figure 1. Material Presentation to Participants



Many participants have not realized that the security of digital platforms is currently very necessary considering that smartphones owned by individual families can be more useful and not just for social media networking but also function as a financial transaction tool through various financial applications available. In this era of advanced technology, children are exposed to devices and the internet from an early age, which requires an in-depth understanding of the risks and how to keep them safe in the digital world. Parents and preschool teachers should be aware that children are vulnerable to inappropriate content, online scams or even exploitation.

Discussion

One important step in improving digital safety is to introduce limits on the use of devices. Parents and preschool teachers need to work together to set rules for screen time duration and select safe and educational apps or platforms. In addition, active supervision is needed, for example by accompanying children when playing gadgets or using parental control features. (Sihombing et al., 2024). Family privacy in the digital age includes: (i) data protection, (ii) online activities, and (iii) smart devices (Citron, 2022; Ibrahim et al., 2023; Payton & Claypoole, 2023). Data protection means protecting the personal information of all family members from misuse (including identity, photos, and location). While online activities are securing digital traces when surfing the internet in the form of search history and online interactions. As for smart devices, it ensures that gadgets and IoT (internet of things) at home do not collect excessive data and maintain optimal security settings. Thus, children can continue to enjoy the benefits of technology without being exposed to unwanted dangers.

Cyberattacks & Data Exploitation

The target community was given an understanding of terms that are often used in digital security. Phishing, where fraudsters send fake messages to steal personal information (Ambashttha & Kumar, 2023). *Ransomware*, locks the data and demands a ransom to unlock it again (Gupta & Kumar, 2024). *Hacking*, hacking of personal accounts to steal identity or information (Huseynov, 2025). *Online fraud*, tricking victims into transferring money or providing sensitive data (Udeh et al., 2024).

Digital Security Mitigation

It is important to anticipate the impact of losses from personal data theft, especially within the scope of the family. Some steps that can be taken to mitigate the adverse effects of digital security include: (i) Regular Discussions, scheduling weekly conversations about online experiences and discussing findings and challenges encountered (Adewusi et al., 2024); (ii) Skills Training, teaching how to recognize safe sites, practicing the ability to identify online scams (Abdelmajid, 2023; Dedkova et al., 2022); (iii) Set Joint Rules, in the form of a joint agreement on internet use in the family and make sure all members understand and agree to it (Quayyum & Jaccheri, 2025).

Technology and Policy (*Best Practise*)

The target community is also given the best action in the form of being wise in using the technological devices they own. The best practices that can be adopted are (i) Device Security. The actions are to enable encryption on all devices, update the operating system regularly, and use a trusted antivirus. (Liu, 2025); (ii) Account Security. The actions are to create unique and strong passwords, enable two-factor authentication, avoid using the same password (Dixit & Kaur, 2024; Jubur et al., 2025); (iii) Network Security. The actions are to set the router with a strong password, use a VPN network when outside, check the devices connected to WiFi (Ikpe & Ashigwuike, 2025; Kizza, 2024).



From a series of material presentations, the enthusiasm of the target community can be seen from the discussion in the form of questions and answers and sharing sessions between participants. In addition, it is also indicated from the response given by the level of satisfaction with the usefulness of the activity above 80% (Figure 2).

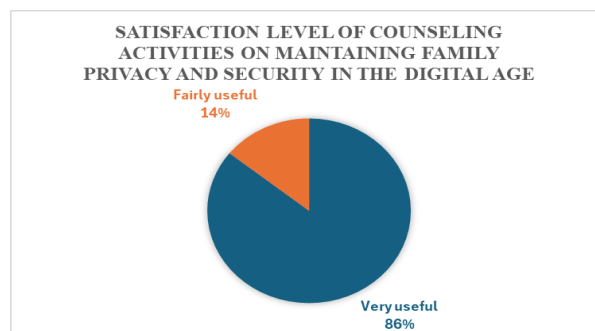


Figure 2. Satisfaction Level of Family Digital Safety Counseling Activities

The series of activities were then closed with a group photo session and the hope of the target community is that similar activities can be carried out continuously with the latest topics, especially those related to digital platforms.



Figure 3. Post-activity Group Photo Session

4. CONCLUSSION

It is important for the community, especially in the family environment, that in this era digital literacy is a must. This is none other than to protect privacy in the form of personal data so that it is always safe from misuse by irresponsible parties. Some small steps that can be taken include prioritizing open dialogue in the family about digital security, always making privacy a core value taught early on, checking privacy settings regularly, limiting camera and microphone access when not in use, and most importantly, the digital safe family mantra: “Don't just click, don't just share!”

5. REFERENCES

- Abdelmajid, N. (2023). The Necessity of Cybersecurity for Community Safety the Proposal of the Safe Family Program for Educating the Gulf Arab Community on Information Security for Both Students and Parents. *International Journal of Information & Digital Security*, 1(1), 20–31.
- Adewusi, M. A., Wasiu, A. A., & Odekeye, O. T. (2024). Understanding Online Security Perceptions and Practices: A Qualitative Study. *EDUCATIONAL PERSPECTIVES*, 13(1).
- Afaq, S. A., Husain, M. S., Bello, A., & Sadia, H. (2023). A critical analysis of cyber threats and their global impact. In *Computational Intelligent Security in Wireless Communications* (pp. 201–220). CRC Press.



- Ambashtha, K. L., & Kumar, P. (2023). Online fraud. In *Financial Crimes: A Guide to Financial Exploitation in a Digital Age* (pp. 97–108). Springer.
- Asaad, R. R., & Saeed, V. A. (2022). A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution. *Applied Computing Journal*, 227–244.
- Barnes, R., & Potter, A. (2021). Sharenting and parents' digital literacy: an agenda for future research. *Communication Research and Practice*, 7(1), 6–20.
- Bhattacharya, M., Roy, S., Chattopadhyay, S., Das, A. K., & Shetty, S. (2023). A comprehensive survey on online social networks security and privacy issues: Threats, machine learning-based solutions, and open challenges. *Security and Privacy*, 6(1), e275.
- Chopra, S., Kareer, I., Singh, G., & Sharma, R. (2024). PERSPECTIVES OF VARIOUS CYBER SECURITY THREATS AND DEFENSE MECHANISMS IN THE MODERN WORLD. *GNA University, Journal of Management & Technology*, 15.
- Citron, D. K. (2022). *The fight for privacy: Protecting dignity, identity and love in the digital age*. Random House.
- Dedkova, L., Smahel, D., & Just, M. (2022). Digital security in families: the sources of information relate to the active mediation of internet safety and parental internet skills. *Behaviour & Information Technology*, 41(5), 1052–1064.
- DeLiema, M., Burnes, D., & Langton, L. (2021). The financial and psychological impact of identity theft among older adults. *Innovation in Aging*, 5(4), igab043.
- Dixit, V., & Kaur, D. (2024). Development of Two-Factor Authentication to Mitigate Phishing Attack. *Journal of Software Engineering and Applications*, 17(11), 787–802.
- Gupta, S. D., & Kumar, R. (2024). waRLOCK: Countering Ransomware and Data Leak. *2024 IEEE International Conference on Contemporary Computing and Communications (InC4)*, 1, 1–6.
- Huang, L., Zhou, J., Lin, J., & Deng, S. (2022). View analysis of personal information leakage and privacy protection in big data era—based on Q method. *Aslib Journal of Information Management*, 74(5), 901–927.
- Huseynov, E. (2025). Identity Theft. In *Computer and Information Security Handbook* (pp. 993–1006). Elsevier.
- Ibrahim, I. M., Budiman, M., & PS, M. A. (2023). Business and Household Financial Management Through the Utilization of Digital Expertise. *Journal Human Resources* 24/7. *Abdimas: Abdimas*, 1(1), 23–30.
- Ikpe, K., & Ashigwuike, E. (2025). Enterprise Network Design and Security Optimization. *Open Access Library Journal*, 12(3), 1–17.
- Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, 7(5), 2157–2177.
- Jubur, M., Shrestha, P., & Saxena, N. (2025). An In-Depth Analysis of Password Managers and Two-Factor Authentication Tools. *ACM Computing Surveys*, 57(5), 1–32.
- Kizza, J. M. (2024). Computer network security protocols. In *Guide to Computer Network Security* (pp. 409–441). Springer.
- LADO, M. J. (2024). *Cybersecurity Essentials Protecting Your Digital Life, Data, and Privacy in a Threat-Driven World: Comprehensive Guide to Preventing Hacks, Phishing, Malware, and Identity Theft*. Amazon Digital Services LLC-Kdp.
- Liu, X. (2025). On the Application of Data Encryption Technology in Computer Network Information Security Protection. *International Journal of Management Science Research*, 8(4), 38–44.
- Nair, M. M., & Tyagi, A. K. (2021). Privacy: History, statistics, policy, laws, preservation and threat analysis. *Journal of Information Assurance & Security*, 16(1).
- Payton, T., & Claypoole, T. (2023). *Privacy in the age of Big data: Recognizing threats, defending your rights, and protecting your family*. Rowman & Littlefield.
- Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*, 50(6), 1299–1323.



- Quayyum, F., & Jaccheri, L. (2025). CyberFamily: A collaborative family game to increase children's cybersecurity awareness. *Entertainment Computing*, 52, 100826.
- Sihombing, L., Sidharta, V., & Arlena, W. M. (2024). Parental Communication Patterns In Reducing Children's Dependence On Playing Gadgets. *Jurnal Spektrum Komunikasi*, 12(4), 556–568.
- Udeh, E. O., Amajuoyi, P., Adeusi, K. B., & Scott, A. O. (2024). The role of big data in detecting and preventing financial fraud in digital transactions. *World Journal of Advanced Research and Reviews*, 22(2), 1746–1760.
- Xia, L., Baghaie, S., & Sajadi, S. M. (2024). The digital economy: Challenges and opportunities in the new era of technology and electronic communications. *Ain Shams Engineering Journal*, 15(2), 102411.