Proceedings of the 2nd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/74/20240421

Empowering college students with personal privacy protection and anti-fraud on the internet: A comprehensive learning approach

Yihui Zhang

Faculty of Science and Engineering, University of Nottingham Ningbo China, Ningbo, Zhejiang, 315100, China

smyyz15@nottingham.edu.cn

Abstract. As college students increasingly navigate their academic pursuits and social lives through the digital realm, safeguarding personal privacy on the internet becomes a pressing concern. For example, deep forgery technology has further increased personal privacy concerns. This technique can produce fake videos, pictures, and sounds that are highly realistic, making it a tool for the misuse of personal and sound data. Several artificial intelligences (AI) systems require large amounts of data for training and improvement, which can involve collecting and storing sensitive personal information. If this data is not adequately protected, and there is no clear privacy policy, it may lead to the misuse or disclosure of personal information. In response to the rapid development of artificial intelligence and the impact of deep forgery technology on privacy and security, this research first tested the students' understanding of deep forgery technology, then introduced the dangers of this technology, and finally gave them a reasonable and effective solution. To promote active learning, activities are integrated to simulate real-world scenarios that college students might encounter. These include creating strong passwords, identifying phishing attempts, and understanding the implications of oversharing on social media platforms. Additionally, students are encouraged to examine case studies documenting privacy breaches and their impact on individuals and society. This essay aims to present an effective learning approach for college students to enhance their understanding of personal privacy protection online and provide an effective way of solving personal problems.

Keywords: Personal privacy, Anti-fraud, Artificial intelligence.

1. Introduction

In today's digital age, university students are increasingly dependent on the Internet for all aspects of their lives, including academic research, communication, and social networking. However, as they navigate this vast online world, personal privacy protection becomes imperative. Not only do college students need to understand how to protect their personal information from potential threats, but they also face the new challenge of avoiding fraudulent behavior associated with deep forgery techniques. And college students, as a large group of people who use the Internet, know little about how to protect personal privacy on the Internet. Data show that the proportion of college students with Internet use is very high, and at the same time, the probability of fraud cases is also relatively high [1]. How to popularize the importance of network security and how to use effective means to protect personal

DOI: 10.54254/2755-2721/74/20240421

privacy to prevent Internet fraud has become a critical issue. The first part of this paper aims to explore how to empower college students to protect their privacy on the Internet. Firstly, the level of awareness of Internet privacy protection among college students is investigated to obtain a comprehensive view of college students' perceptions of online security and privacy protection in this population. Then, emphasizing the importance of equipping students with the necessary knowledge and tools to maintain personal privacy in an interconnected world. Knowing about the risk associated with indiscriminate sharing of personal information, they can take proactive steps to ensure their safety online. The second part of the essay delves into the rising concern of deep forgery technology, a sophisticated form of manipulation that utilizes artificial intelligence algorithms to create deceptive content, including forged images, videos, and audio recordings. College students, as active consumers and contributors to online platforms, must gain awareness and critical thinking skills to avoid falling victim to these fraudulent practices. Moreover, the ethics of AI has always been one of the hot issues in society, and the article will illustrate with examples how the improper use of the Internet and AI can have dire consequences. For instance, when we interview for a job, artificial intelligence software used in employment that analyses the voice and facial expressions of job interviewees raises concerns about privacy and discrimination [11]. College students must learn how to verify the authenticity of online content and distinguish between genuine and manipulated information. Educating them about the ethical implications and societal consequences of sharing deep-forged content is crucial to promoting responsible digital citizenship. In conclusion, empowering college students with personal privacy protection on the internet and educating them on avoiding deep forgery fraud is paramount in today's technological landscape. Universities can provide students with vital knowledge and skills, whilst promoting a mindful and responsible attitude towards safeguarding personal privacy. Ultimately, this approach will enable students to navigate the online world with confidence, be aware of the risks of the use of artificial intelligence, protect their privacy, safeguard against fraudulent manipulation, promote a harmonious network environment, and facilitate the digital development process.

2. Methodology

First, a literature review: First, an extensive review of academic articles, books, and research papers related to Internet personal privacy protection and deep forgery techniques. The second step is to collect information about the current status of personal privacy risks, prevalent cyber threats, and emerging trends in deep forgery techniques. In this study, we employed surveys and questionnaires to investigate the knowledge and awareness levels of university students regarding personal privacy protection and deep forgery techniques when using the Internet. The questionnaire collected various information from participants, including their age, duration of time spent online, awareness of risks associated with sharing personal information online, self-perceived level of knowledge about personal privacy protection and anti-fraud measures on the Internet, and the privacy protection measures they practiced, such as using strong passwords and adjusting privacy settings on social media accounts. Additionally, we assessed whether participants had experienced any incidents of fraud or privacy breaches while using the Internet, their awareness of deep forgery techniques, and the main sources through which they obtained knowledge on personal privacy protection and anti-fraud measures online. The questionnaire design was structured in a way that ensured the collection of valuable and relevant data. The data gathered provides crucial insights into the current state of affairs and facilitates the provision of effective solutions. Below is a content outlining the survey:

1. Introduction: Provide a brief introduction to the purpose of the survey and reassure participants about the confidentiality and anonymity of their responses.

2. Personal Information: Collect basic demographic information, such as age and gender, to understand the characteristics of the participants.

3. Awareness of Risks: Determine participants' awareness of the risks associated with sharing personal information online, including the potential consequences of identity theft and privacy breaches.

DOI: 10.54254/2755-2721/74/20240421

4. Self-Perceived Information: Evaluate participants' self-perceived level of knowledge about personal privacy protection and anti-fraud measures on the Internet to gauge their understanding of the subject matter.

5. Privacy Protection Measures: Investigate the privacy protection measures adopted by participants, such as the use of high-strength passwords, adjustments to privacy settings on social media accounts, and other cautious practices regarding personal information sharing.

6. Incidents Experience: Determine whether participants have ever encountered incidents of fraud or privacy breaches while using the Internet, in order to highlight potential vulnerabilities and areas for improvement.

7. Awareness of Deep Forgery Techniques: Assess participants' awareness of deep forgery techniques, including their familiarity with methods used to manipulate digital content for deceptive purposes.

8. Sources of Awareness: Identify the main channels through which participants acquire knowledge about personal privacy protection and anti-fraud measures on the Internet, such as online articles, social media platforms, or educational institutions.

This questionnaire avoids the use of leading questions, which can help to collect a large amount of reliable data that can lead to a comprehensive understanding of the current situation. This data can provide a valuable basis for the development of effective strategies and solutions to improve the protection of personal data and to fight against counterfeiting techniques in the cyber domain. Subsequently, evaluation and feedback: Feedback from students, educators, and experts on the design and implementation of the educational program will be collected, and suggestions for improvement will be incorporated. The program is also continuously evaluated and updated based on the feedback, along with new trends and technologies in personal privacy protection and deep forgery detection. This essay employs a comprehensive methodology to offer insights into empowering college students with personal privacy protection on the Internet, equipping them with knowledge and skills to avoid deep forgery fraud.

3. Results

College students are heavy internet users, with almost all using the internet. (Aaron, 2019). According to the literature, A study conducted in Kashmir Valley found that students of computer science use the internet more frequently than students of other disciplines [2]. The impact of internet usage on students' success in selected senior high schools in Cape was also studied, and it was found that most students get relevant information, such as educational materials, from the internet [3]. A comparative study of internet usage among university students found that the percentage of internet usage among students from Business Studies, Science, and Arts backgrounds is 100%, 92%, and 96%, respectively [4]. Similarly, the results of the first survey were similar. First of all, all the participants in the questionnaire were between 18 and 23 years old, and all of them answered that they use the Internet, browse information on the Internet and rely on the Internet to solve problems. It can be seen that college students rely heavily on the Internet. Of the 112 questionnaires, 82 responses showed more than 3 hours of browsing and using information on the Internet per day, a proportion of more than 70%, and another 8 responses showed more than 6 hours. However, in the next question, although more than 90% of the responses showed an awareness of protecting personal privacy, only two responses listed in detail how they protected their personal privacy information, with one of the answers being: For example, when using some WeChat mini-programs, the mini-programs use personal information, and this article will pay attention to whether the program applies to retrieve personal information in too much detail. Therefore, the investigator randomly selected ten people to be interviewed again in response to this answer: Will the college students pay attention to what personal information is used by different software or programs that apply for access? Surprisingly, none of the ten people had checked that information. However, College students still use some common means to protect personal privacy; the most popular choice is to use a high-strength password combination. More than 90% of students will set up a password combination that they think is complex, of which there are also 16 responses to the use of the highest-strength passwords: uppercase and lowercase letters, numbers, and characters in the form

DOI: 10.54254/2755-2721/74/20240421

of a combination of passwords, followed by adjusting the privacy settings of the social media account this option, there are 98 responses to this option, and the third is to avoid clicking on the unfamiliar links, more than 80% of the students approved of this option. Subsequently, in a survey about deep faking techniques, students from different majors gave very different feedback. The survey received a total of 116 responses, and the survey was divided into two groups, in which group A, for majors belonging to science engineering, received 60 responses, and group B, for the liberal arts majors, received 56 responses from students. All those who filled out the questionnaire were concentrated in the age group of 18-23 years old. In the first question, "Do you know or have you heard of deep faking technology?" 58 respondents in Group A answered yes, while only 17 respondents in Group B said they knew or had heard of it (see Figure 1).

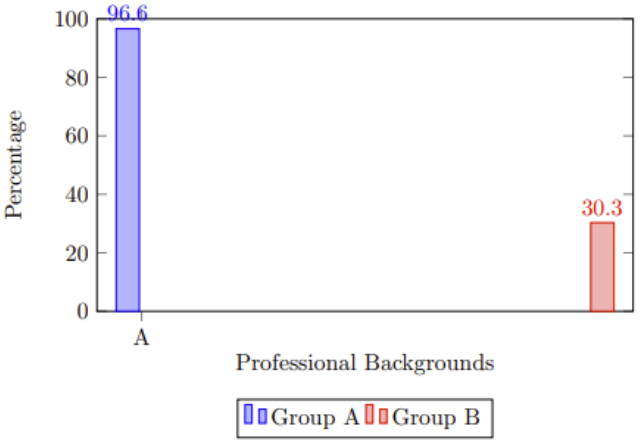

Figure 1. Understanding of Deep Forgery Technology Among College Students

Today's college students face many challenges in ensuring the protection of their privacy and guarding against online fraud. As a generation that is highly dependent on the Internet for all aspects of their lives, college students are particularly vulnerable to privacy violations and fraudulent activity. In addition, Criminals use different cyberspaces to enhance cybercrime with the development of information technology. Deep forgery techniques include face forgery, scene forgery. Because of the importance and specificity of face forgery, this technology has gradually gained more attention in society. At present, various cutting-edge deep forgery methods can easily forge fake faces that are difficult for ordinary people to distinguish, and many criminals use this technology to carry out online fraud and obtain money through illegal means.

First of all, make a brief introduction to deep forgery technology. Deepfake technology is a type of artificial intelligence used to create convincing images, audio, and video hoaxes [5]. It uses two algorithms, a generator, and a discriminator, to create and refine fake content [5, 6]. The generator builds a training data set based on the desired output, creating the initial fake digital content, while the discriminator analyzes how realistic or fake the initial version is [5]. This process is repeated, allowing the generator to improve at creating realistic content and the discriminator to become more skilled at spotting flaws for the generator to correct [5]. Deepfakes can be used for illicit purposes, including to generate non-consensual pornography, and can pose a personal security risk by mimicking biometric data [7, 8]. As technology improves, the discrepancies between real and fake content will likely become harder to detect [8].

In today's rapidly digitalized world, personal privacy protection has become a pressing concern, especially for college students who rely extensively on technology and online platforms. It is crucial to empower these students with the knowledge and tools needed to safeguard their privacy effectively. One aspect of particular importance is understanding deep forgery technology. This technology has the potential to manipulate various forms of digital content, including images, videos, and audio, making it

DOI: 10.54254/2755-2721/74/20240421

challenging to discern what is genuine and what has been altered or fabricated [9][10]. By educating college students about deep forgery technology, they can develop a critical awareness of the risks associated with manipulated content. They will learn how to identify signs of forgery and employ techniques to verify the authenticity of digital media. Furthermore, empowering students with personal privacy protection strategies will enable them to make informed decisions about sharing sensitive information online, reducing exposure to potential threats like identity theft or privacy breaches. Through workshops, courses, and awareness campaigns, educational institutions can play a vital role in enhancing students' understanding of deep forgery technology and personal privacy protection. These initiatives should focus on practical skills, such as detecting photo manipulation techniques, using reliable authentication tools, and adopting encryption methods for secure communication. Additionally, promoting responsible digital citizenship and ethical use of technology can instill a sense of accountability among students regarding their online actions, enabling them to navigate the digital landscape while maintaining their personal privacy [11]. By empowering college students with knowledge about deep forgery technology and personal privacy protection, we equip them to protect themselves and their peers from the increasingly sophisticated threats in the digital realm. This education enables them to cultivate a digital presence that prioritizes privacy, authenticity, and informed decision-making. As they enter professional environments and engage in civic discourse, well-prepared college graduates will contribute to shaping a safer and more secure digital landscape for society.

4. Conclusion

In conclusion, empowering college students with comprehensive learning approaches focused on personal privacy protection and anti-fraud measures on the internet is of utmost importance in today's digital age. By providing students with the necessary knowledge, skills, and tools to navigate the online world safely, educational institutions can play a significant role in safeguarding their personal information and preventing fraud. Through targeted workshops, courses, and awareness campaigns, colleges can educate students about deep forgery technology and its potential risks. By understanding the techniques used to manipulate digital content, students will be better equipped to detect and respond to instances of forgery or manipulation. Moreover, teaching students how to verify the authenticity of digital media empowers them to make informed judgments when consuming or sharing information online. Additionally, a comprehensive learning approach should incorporate personal privacy protection strategies to help students develop responsible digital habits. Providing guidance on secure communication practices, recognizing and avoiding phishing attempts, and protecting sensitive information can significantly mitigate the risks of identity theft, financial fraud, or privacy breaches [12]. By imparting these skills, colleges can foster a sense of digital citizenship and responsibility among students. Encouraging ethical behavior and emphasizing the importance of respecting others' privacy and consent creates a culture that values integrity and trustworthiness in the online space. Ultimately, the goal is to equip college students with the knowledge and competencies needed to protect themselves and others from online threats. By empowering them with personal privacy protection measures and an understanding of anti-fraud strategies, educational institutions contribute to shaping a safer and more secure digital environment for future generations. This comprehensive learning approach prepares students for a digitally evolving society and reinforces the importance of privacy, integrity, and responsible online behavior.

References

[1] Smith A. College students and Technology [Internet]. Pew Research Center: Internet, Science & Tech. 2011 Jul 19 [cited 2022 Dec 21]. Available from: https://www.pewresearch.org/internet/2011/07/19/college-students-and-technology/

[2] Loan FA. Internet use by the college students across disciplines: A study [Internet]. 2011 Jun [cited 2022 Dec 21]. Available from: https://www.researchgate.net/publication/267968005_Internet_use_by_the_college_students_across_disciplines_A_study

DOI: 10.54254/2755-2721/74/20240421

[3] Amponsah KD, Aboagye GK, Narh-Kert M, Commey-Mintah P, Boateng FK. The impact of internet usage on students' success in selected ... - eric [Internet]. 2022 Jun 30 [cited 2022 Dec 21]. Available from: https://files.eric.ed.gov/fulltext/EJ1353463.pdf

[4] Hossain MA, Rahman MH. Comparative Study of Internet Usage Among University Students: A Study of the University of Dhaka, Bangladesh. European Scientific Journal, ESJ. 2017;13(34):134. Available from: https://doi.org/10.19044/esj.2017.v13n34p134

[5] Barney N, Wigmore I. What is Deepfake Ai? A definition from TechTarget [Internet]. WhatIs. com. 2023 Mar 21 [cited 2022 Dec 21]. Available from: https://www.techtarget.com/whatis/definition/deepfake

[6] What the heck is a deepfake? | Information Security at UVA. U.Va. [Internet]. n.d. [cited 2022 Dec 21]. Available from: https://security.virginia.edu/deepfakes

[7] Guardian News and Media. What are deepfakes – and how can you spot them? [Internet]. The Guardian. 2020 Jan 13 [cited 2022 Dec 21]. Available from: https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them

[8] Johnson D. What are deepfakes? how fake AI-powered audio and video warps our perception of reality [Internet]. Business Insider. n.d. [cited 2022 Dec 21]. Available from: https://www.businessinsider.com/guides/tech/what-is-deepfake

[9] Xinwei L, Jinlin G, Junnan C. An Overview of Face Deep Forgery. In: 2021 International Conference on Computer Engineering and Application (ICCEA). Kunming, China; 2021. p. 366–370. doi: 10.1109/ICCEA53728.2021.00078

[10] Abidin ABZ, Majid HBA, Samah ABA, et al. Copy-move image forgery detection using deep learning methods: a review. In: 2019 6th international conference on research and innovation in information systems (ICRIIS). IEEE; 2019. p. 1–6.

[11] Pazzanese C. Ethical concerns mount as AI takes bigger decision-making role [Internet]. Harvard Gazette. 2020 Dec 4 [cited 2022 Dec 21]. Available from: https://news.harvard.edu/gazette/story/2020/10/ethical-concerns-mount-as-ai-takes-bigger-decision-making-role/

[12] Soni VD. Role of artificial intelligence in combating cyber threats in banking. International Engineering Journal for Research & Development. 2019;4(1):7.