# An Empirical Analysis of Undergraduate Information Systems Security Behaviors

José A. García-Berná[1][a], Sofia Ouhbi[2][b], José L. Fernández-Alemán[1][c]
and Ana B. Sánchez-García[1][d]

[1]*Department of Computer Science & Systems, University of Murcia, Murcia, Spain*
[2]*Department of Information Technology, Uppsala University, Uppsala, Sweden*
*fi*

Keywords: Privacy, Security, Nursing Education, Empirical Study.

Abstract: The growing concern within healthcare organizations about the privacy of personal health data emphasizes how critical it is to address security and privacy issues, especially for nurses who handle sensitive data on a daily basis. In order to understand the habits and awareness of nursing degree students with regard to the protection of patients' personal data, this study focuses on evaluating their security behavior. The purpose of the 21-item questionnaire was to provide insight into the data security practices of 95 fourth-year nursing students and 167 second-year nursing students. The findings indicated that students in their second year of study had more robust password practices than those in their fourth year, who in turn showed a propensity to click on potentially hazardous links more frequently. In light of the fact that nursing professionals will unavoidably work with large amounts of medical data in their future positions, the findings point to the necessity of raising awareness of and providing education on data protection.

## 1 INTRODUCTION

The scientific community is aware of how crucial human and technological factors are to protecting the security and privacy of health data (Bauer et al., 2009; Mammadova, 2015; Ishikawa et al., 2007; Aanestad, 2017). The difficulty is in digitizing health data and providing all medical personnel with the necessary training to enable them to successfully implement digital health solutions. It is worth noting that the healthcare industry is more vulnerable to incidents stemming from human error or cybercrime due to its growing reliance on information systems (US-CERT, 2016; Evans et al., 2019; McDermott et al., 2019).

There has been an increase in the number of data breaches discovered in healthcare organizations, according to the European Network and Information Security Agency (ENISA). In Europe, employee negligence accounts for approximately 41% of health record breaches. This occurs when staff members treat sensitive data like precious commodities, despite its invisibility. Information security best practices, when adopted and followed, could have prevented over 90% of these breaches (Kierkegaard, 2012; Corallo et al., 2022).

Effective non-technical ways to reduce risks and threats to security and privacy are education and awareness campaigns. Research indicates that improving healthcare personnel's knowledge of security requirements and raising their level of awareness has a positive impact on healthcare organizations' security performance, protecting patient privacy. Additionally, security behaviors training improves healthcare personnel's ability to identify information that needs to be protected and to decide what steps need to be taken to protect patient information. Designing effective awareness campaigns and training programs requires an understanding of user security behavior (Colwill, 2009; Fernando and Dawson, 2008; Craig, 2009; Murphy et al., 2004; Fernández-Alemán et al., 2015).

In order to identify and address insufficient security practices, this paper presents an empirical study on nursing students' security practices. By doing so, it provides insights into how to improve security knowledge in nursing education. Based on earlier studies assessing the security and privacy policies

[a] https://orcid.org/0000-0002-9526-8565
[b] https://orcid.org/0000-0001-7614-9731
[c] https://orcid.org/0000-0002-0176-450X
[d] https://orcid.org/0000-0003-3258-6088

García-Berná, J., Ouhbi, S., Fernández-Alemán, J. and Sánchez-García, A.
An Empirical Analysis of Undergraduate Information Systems Security Behaviors.
DOI: 10.5220/0012430700003657

In *Proceedings of the 17th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2024) - Volume 2*, pages 620-627
ISBN: 978-989-758-688-0; ISSN: 2184-4305

of medical staff in a public hospital, this study uses a 21-item survey given to 252 nursing students. The expectation that these students will handle significant volumes of vital medical data in the future led to the selection of this target group. Notably, no prior research has evaluated and examined nursing students' security-related behaviors. Three research questions in all were put forth in the experiment.

- *RQ1:* Which security practices are most common for managing medical data?
- *RQ2:* How does gender affect the management of medical data?
- *RQ3:* What effect does the course level have on medical data management?

The structure of the paper is as follows. The experiment's methodology is explained in Section 2. The survey results are provided in Section 3. The main findings are discussed in Section 4, and the conclusions are addressed in Section 5.

## 2 MATERIALS AND METHODS

An explanation of the features of the experiment is carried out in this section. To aid in a better understanding of the study, the major components, such as the setting, the subjects, the ethical issues, and the data analysis, are described below.

The experiment was conducted at the University of Murcia (UMU). This institution offers cutting-edge study programs that include contracts to conduct clinical practice in the city's and the surrounding provinces' public and private centers. Students can increase their practical understanding of health issues by using a variety of facilities, including computer rooms, labs, technical skills rooms, and simulations of clinical scenarios.

The research team informed the students about the study at the start of the lecture where the survey was conducted by giving an oral presentation. More precisely, the experiment was carried out during the second-year nursing student's Clinical Practices I course. The 292 teaching hours in this subject are broken down as follows: 260 hours, or 6 weeks, are spent on clinical visits at the hospitals; 2 hours are spent on mentoring; 10 hours are spent on seminars; and 20 hours are spent on laboratory exercises and simulations. The survey was administered for both students enrolled in the second and fourth year. For the fourth-year students, the survey was conducted during a training lecture at the Queen Sofia hospital in the Region of Murcia (Spain). This hospital is one of the most important healthcare buildings in the province.

For both second- and fourth-year students, the experiment was carried out during the first semester of the course. There were 167 second-year students (137 females and 30 males, mean age 21 years, SD = 4.42) and 95 fourth-year students (78 females and 17 males, mean age 23 years, SD = 4.97). It is important to note that prior to taking part in this study, the students had no prior instruction in information systems security practices.

The study, which aims to safeguard students' privacy and human rights, was approved for revision purposes by the Institutional Review Board at the Nursing Faculty of the UMU. All subjects were given explanations regarding the aim of the study, its methods, and how the study's findings would be used prior to the experiment. Additionally, they were informed that they could choose not to answer any of the experiment's questions or to stop participating altogether. Every student gave their verbal informed consent.

## 3 RESULTS

Table 1 displays the study population's demographic characteristics. The study's results are shown below. The results are divided based on the research questions in order to better organize the data.

Table 1: Characteristics of the study population.

| Course | Characteristics | N | % |
|---|---|---|---|
| $2^{nd}$ year | Age | | |
| | 18-20 | 124 | 74% |
| | 21-25 | 31 | 19% |
| | 26-30 | 4 | 2% |
| | 31-35 | 4 | 2% |
| | 36-40 | 2 | 1% |
| | 41-45 | 1 | 1% |
| | 46-50 | 1 | 1% |
| $2^{nd}$ year | Gender | | |
| | Female | 137 | 82% |
| | Male | 30 | 18% |
| $4^{th}$ year | Age | | |
| | 20-25 | 84 | 88% |
| | 26-30 | 7 | 7% |
| | 31-35 | 0 | 0% |
| | 36-40 | 1 | 1% |
| | 41-45 | 2 | 2% |
| | 46-50 | 1 | 1% |
| $4^{th}$ year | Gender | | |
| | Female | 78 | 82% |
| | Male | 17 | 18% |

*RQ1: Which security practices are most common for managing medical data?*

While most of individuals have strong passwords, students in the $2^{nd}$ year performed better than those in the 4$^{th}$ year in terms of password strength. Answering ”Yes” to Q6 and ”No” to Q7 indicates that the password is weak. There was only one student with a weak password from the 2$^{nd}$ year and nine students from the 4$^{th}$ year. 16% of students in the 2$^{nd}$ year and 24% of students in the 4$^{th}$ year reported that they have occasionally emailed or written down their passwords in a place that is easily accessible. Password sharing was more common among students in the 4$^{th}$ year (32%) than it is in the 2$^{nd}$ year (10%). Of the students enrolled in the 4$^{th}$ and 2$^{nd}$ degree programs, 11% have used the browser's 'Save Password' feature.

Regarding email use, only 7% of respondents in the 2$^{nd}$ year and 20% in the 4$^{th}$ year reported having opened potentially dangerous email attachments or links, and a small percentage of participants (11% in the 2$^{nd}$ year and 9% in the 4$^{th}$ year) reported having sent or received personal health information (PHI) via email at some point.

The majority of participants have linked a personal device to the hospital's intranet (78% in the 2$^{nd}$ year and 66% in the 4$^{th}$ year). A small percentage of participants (4% in 2$^{nd}$ Year and 11% in 4$^{th}$ Year) had PHI copied onto electronic devices or storage media. This data was downloaded without the responsible staff member's consent and used for work at home. Thus, none of the healthcare professionals should implement this crucial practice.

Compared to 13% of students in the 4$^{th}$ year, only 4% of students in the 2$^{nd}$ year stated they did not follow procedures for discarding confidential information. This outcome is consistent with responses to Q4, in which most participants confirmed that they were aware of the security protocols established by the hospital to preserve patient privacy. Only a small percentage of respondents, 10% in the 2$^{nd}$ year and 17% in the 4$^{th}$ year, said they were aware of how to report a security incident when they were discovered.

The majority of respondents (94% in the 2$^{nd}$ year and 86% in the 4$^{th}$ year) used keyboard locking or password-protected screen savers to secure PHI on their screens, and 92% in the 2$^{nd}$ year and 86% in the 4$^{th}$ year made sure that no one else could see their computer monitor. Compared to 32% of students in the 4$^{th}$ year, only 6% of students in the 2$^{nd}$ year had access to PHI unrelated to their employment.

The vast majority (94% in the 2$^{nd}$ year and 92% in the 4$^{th}$ year) responded that information was promptly deleted from copiers, fax machines, and printers to prevent information security breaches. Additionally, they refrained from installing non-work-related programs on hospital computers (92% in 2$^{nd}$ year and 91% in 4$^{th}$ year).

*RQ2: How does gender affect the management of medical data?*

Odds ratios (ORs) were computed using gender and level of the studies as independent variables in order to respond to this and the following question. Q5 and onwards in the questionnaire had dichotomous answers (Yes or No) that were taken into account as dependent variables (see Table 2).

The results of ORs for RQ2 indicated that no statistically significant differences existed. This indicates that gender is irrelevant to the management of medical data. Although other results might have emerged given the gender diversity that is currently acknowledged, this result is a priori in line with what was anticipated.

*RQ3: What effect does the course level have on medical data management?*

Table 4 shows that there were significant differences in the ORs of RQ2 for Q7, Q13, and Q15–Q17. Specifically, the outcomes were as follows. Regarding Q7, does your password consist of a minimum of eight characters, encompassing capital and lowercase letters, digits, and unique keyboard characters like #? the odds were 10.490 (95% CI: 3.445 to 31.943). In Q13, did you ever connect a personal device (laptop, tablet, smartphone, etc.) to the hospital intranet? the results showed that the odds were 2.333 (95% CI: 1.234 to 4.409); with regard to Q15, do you adhere to the policies of your company when it comes to getting rid of private information (like patient records)? 3.295 (95 %CI: 1.247 to 8.709); regarding Q16, do you safeguard PHI on your screen by using keyboard lockups or password-protected screen savers? 5.744 (95 %CI: 1.514 to 21.797). Lastly, regarding Q17, do you make sure that unauthorized users cannot view your computer monitor when using PHI on the hospital's computer? 3.130 (1.099 to 8.918, 95 %CI). The ORs values were generally within the range of 2.3 to 3.2, with the exception of Q7, which had the highest value of approximately 10.5.

## 4 DISCUSSION

The analysis of the outcomes derived from the survey data is provided below. Every research question has its own section in the informational structure.

*RQ1: Which security practices are most common for managing medical data?*

Table 2: Responses to the security behavior questionnaire (*N_2nd year*=167, *N_4th year*=95).

| ID | Questions | 2nd Year | | | 4th Year | | |
|---|---|---|---|---|---|---|---|
| | | Yes | No | NA | Yes | No | NA |
| 1 | Age | - | - | - | - | - | - |
| 2 | Gender | - | - | - | - | - | - |
| 3 | Course year | - | - | - | - | - | - |
| 4 | Were you informed about the security procedures defined by the hospital to protect patient confidentiality? | 128 (77%) | 37 (22%) | 2 (1%) | 85 (89%) | 10 (11%) | 0 (0%) |
| 5 | Have you ever written your password down anywhere easily accessible or sent it by email? | 26 (16%) | 135 (81%) | 6 (4%) | 23 (24%) | 64 (67%) | 8 (8%) |
| 6 | Does your password include a personal name, special date, fictional character, personal information or is it easy for others to guess? | 16 (10%) | 144 (86%) | 7 (4%) | 20 (21%) | 70 (74%) | 5 (5%) |
| 7 | Is your password composed of at least eight characters, including upper and lowercase letters, numbers and special keyboard characters (such as #)? | 159 (95%) | 4 (2%) | 4 (2%) | 72 (76%) | 19 (20%) | 4 (4%) |
| 8 | Have you ever shared your password with someone (for example, a colleague)? | 16 (10%) | 142 (85%) | 9 (5%) | 30 (32%) | 61 (64%) | 4 (4%) |
| 9 | Have you ever used the browser ”Save Password” functionality? | 18 (11%) | 143 (86%) | 6 (4%) | 10 (11%) | 76 (80%) | 9 (9%) |
| 10 | Have you ever opened attachments, or links in e-mails which were dangerous? | 11 (7%) | 141 (84%) | 15 (9%) | 19 (20%) | 70 (74%) | 6 (6%) |
| 11 | Have you ever sent spam? (For example, an e-mail with false shocking news) | 24 (14%) | 124 (74%) | 19 (11%) | 8 (8%) | 83 (87%) | 4 (4%) |
| 12 | Have you ever sent or received PHI by e-mail? | 19 (11%) | 138 (83%) | 10 (6%) | 9 (9%) | 79 (83%) | 7 (7%) |
| 13 | Have you ever connected a personal device (laptop, tablet, smartphone, etc.) to the hospital's Intranet? | 130 (78%) | 23 (14%) | 14 (8%) | 63 (66%) | 26 (27%) | 6 (6%) |
| 14 | Have you ever copied PHI onto electronic storage media or electronic devices (CD, DVD, USB, external hard drives, smartphone, mobile phone, tablet, etc.) to work at home without permission from the staff member responsible for this information? | 7 (4%) | 155 (93%) | 5 (3%) | 10 (11%) | 80 (84%) | 5 (5%) |
| 15 | Do you follow your organization's procedures for discarding confidential information (e.g.: discarded patient information)? | 148 (89%) | 7 (4%) | 12 (7%) | 77 (81%) | 12 (13%) | 6 (6%) |
| 16 | Do you use the password-protected screensavers or keyboard-locking to protect PHI on your screen? | 157 (94%) | 3 (2%) | 7 (4%) | 82 (86%) | 9 (9%) | 4 (4%) |
| 17 | When working with PHI on your hospital's computer, do you ensure that your computer monitor cannot be seen by unauthorized individuals? | 154 (92%) | 6 (4%) | 7 (4%) | 82 (86%) | 10 (11%) | 3 (3%) |
| 18 | Have you ever had access to PHI which is not part of your job? | 10 (6%) | 138 (83%) | 19 (11%) | 30 (32%) | 53 (56%) | 12 (13%) |
| 19 | Do you ensure that information (documents, memory, etc.) is removed from printers, copiers, and fax machines quickly so that information is not compromised? | 157 (94%) | 5 (3%) | 5 (3%) | 87 (92%) | 5 (5%) | 3 (3%) |
| 20 | Do you avoid installing programs that are not related to your work on a hospital computer? | 154 (92%) | 7 (4%) | 6 (4%) | 86 (91%) | 6 (6%) | 3 (3%) |
| 21 | In the case of detecting a security incident, do you know the procedure to allow you to report it? | 16 (10%) | 136 (81%) | 15 (9%) | 16 (17%) | 76 (80%) | 3 (3%) |

Aiming to address current legal gaps regarding security and privacy of personal data, the General Data Protection Regulations (GDPR) were introduced. May 2018 saw the complete implementation of these laws. Taking into account the control of security and privacy issues, they had a positive impact (Hoofnagle et al., 2019) in Europe on data sharing in the healthcare systems (Price and Cohen, 2019). Nonetheless, given the concerns raised by working nurses in the use of eHealth information systems, including privacy, confidentiality, security, and patient safety, foundational knowledge should be taught in nursing programs at universities (Bani Issa et al., 2020).

In computing, using passwords created by users has become standard practices for data security (Kävrestad et al., 2020). Nevertheless, creating a strong, memorable password is a difficult task because security and usability are at odds (Guo et al., 2019). To lessen the cognitive strain of remembering strong passwords, a number of contemporary systems, including graphical passwords, password managers, and biometric features, have been proposed thus far. But these solutions are too far off to be applied to medical information systems that are used on a daily basis (Enaizan et al., 2020). This is why

Table 3: Gender OR results (95% CI).

| Q# | Gender (F=1/M=0) |
|---|---|
| Q05 | 2.145 (0.798 to 5.767) |
| Q06 | 0.756 (0.320 to 1.787) |
| Q07 | 0.675 (0.192 to 2.377) |
| Q08 | 1.636 (0.649 to 4.126) |
| Q09 | 0.429 (0.180 to 1.023) |
| Q10 | 0.653 (0.260 to 1.640) |
| Q11 | 2.315 (0.672 to 7.983) |
| Q12 | 6.672 (0.882 to 50.483) |
| Q13 | 1.572 (0.742 to 3.333) |
| Q14 | 0.478 (0.159 to 1.432) |
| Q15 | 0.867 (0.241 to 3.118) |
| Q16 | 0.886 (0.188 to 4.189) |
| Q17 | 2.100 (0.693 to 6.361) |
| Q18 | 0.866 (0.367 to 2.045) |
| Q19 | 1.136 (0.233 to 5.536) |
| Q20 | 2.095 (0.616 to 7.125) |
| Q21 | 0.330 (0.148 to 0.735) |

Table 4: Level OR results (95% CI).

| Q# | Level (2nd=1/4th=0) |
|---|---|
| Q05 | 0.536 (0.284 to 1.011) |
| Q06 | 0.389 (0.190 to 0.796) |
| Q07 | *10.490 (3.445 to 31.943)* |
| Q08 | 0.229 (0.116 to 0.451) |
| Q09 | 0.957 (0.421 to 2.175) |
| Q10 | 0.287 (0.130 to 0.637) |
| Q11 | 2.008 (0.861 to 4.684) |
| Q12 | 1.209 (0.522 to 2.799) |
| Q13 | *2.333 (1.234 to 4.409)* |
| Q14 | 0.361 (0.133 to 0.985) |
| Q15 | *3.295 (1.247 to 8.709)* |
| Q16 | *5.744 (1.514 to 21.797)* |
| Q17 | *3.130 (1.099 to 8.918)* |
| Q18 | 0.128 (0.590 to 0.280) |
| Q19 | 1.805 (0.508 to 6.406) |
| Q20 | 1.535 (0.500 to 4.713) |
| Q21 | 0.559 (0.265 to 1.180) |

there should be a greater effort made to educate college nursing students about these issues.

When it comes to safeguarding sensitive data, people are the weakest link. As an illustration, phishing emails are still successfully jeopardizing ISs security (Sharma and Bashir, 2020). According to the findings of our study, a sizable portion of students had opened the emails' attached files or clicked on dubious web links. According to these results, basic education is still vital for the silent majority of people who continue to click through (Vincent, 2019). Several methods have been suggested in the literature to identify these dangerous behaviors and fill in the ignorance of possible victims. To identify insecure web links, neural networks were used (Gajera et al., 2019). Using machine learning techniques, feature selection for effective phishing attack detection was also investigated (Zabihimayvan and Doran, 2019). Regardless of the textual language used within the web portals, phishing web pages were accurately detected by a search engine-based method (Gupta and Jain, 2020). By applying these strategies to medical ISs, the security of the medical data in emails could be ensured.

It is common practice to connect electronic devices to public WiFi networks. But a lot of users are unaware about the dangers that unidentified networks can occasionally present. According to a survey, the majority of users do not think about security precautions when connecting to open networks like VPN. Furthermore, they used to unintentionally disable security features they believed unnecessary (Breitinger et al., 2020). Even with encrypted WiFi networks, personal information can be inadvertently shared by mobile applications. This is because personal information like age, gender, and religion can be connected to an app's usage. By examining encrypted traffic patterns, a remote observer can passively and undetected infer potentially sensitive data without requiring network credentials (Atkinson et al., 2018). Default security settings are frequently insufficient, which highlights the need to investigate alternative approaches to increase user awareness and provide cybersecurity education. For this reason, serious gaming environments have been used. In these, participants had to figure out how to connect to unprotected networks, figure out passwords, and take advantage of websites. Known as Capture the Flag exercises, these drills are a common way to teach cybersecurity (Švábenskỳ et al., 2021).

When it comes to safeguarding sensitive data from network threats, businesses prioritize protecting sensitive data. Information can be compromised when using equipment found in public spaces like hotels, hospitals, universities, and airports. Globally, significant sums of money are invested in cybersecurity. Nonetheless, incidents involving human error are significant. A key component of preventing unwanted behavior and bolstering security is employee knowledge of privacy and security. This information is crucial because employees typically have little understanding of how to steer clear of these dangerous situations (Khando et al., 2021). Therefore, it is critical to prevent with safeguards in addition to encouraging user education about cybersecurity. The most popular ones include: dividing permissions into user and superuser categories, restricting device functionality based on intended use, routinely formatting computers, scanning computer hardware and software for vulnerabilities during periods of lower usage congestion, etc. Another option to consider is the implementation of strategies like Zero Trust. The goal of this approach is to completely remove any sense of boundary in internal networks. One advantage of this strategy is that it makes attackers work much harder to accomplish their objectives. Conversely, it makes managing internal security teams more difficult because they have to gather information and make decisions based on the analysis. All of the organization's systems, data, and access scenarios must take these steps (AlQadheeb et al., 2022).

For mobile phones, one of the most popular unlocking techniques is the use of graphical patterns. Nevertheless, this method's entropy values are typically low, providing users with a low level of security (Zhang et al., 2021). In an effort to improve security, mobile phones now include the Embedded Secure Element (eSE) hardware. This part seeks to guarantee that important data is safely protected even in the event that the system as a whole is compromised. The eSE is expected to play a critical role in the security of phones of the future since it is made to withstand both physical and logical attacks (Alendal et al., 2021).

The security and privacy of personal data can be improved with the use of behavior analysis and prediction tools. In this regard, studies that use data mining techniques and in-depth interviewing have emerged to address citizens' concerns about privacy. The findings highlight a number of trending subjects where AI used in data protection can have a significant influence. These include the following: risk of behavior modification, digital surveillance, intelligence decision-making, automation of decisions, and prediction of human behavior (Saura et al., 2022). Online Health Communities (OHC) are groups that are commonly created through the use of interactive technologies. People in these communities trade social support and have similar health interests. OHCs benefit users, but privacy issues could affect how people behave in terms of social support. The findings demonstrate that in order to address privacy concerns, community engagement is necessary. The primary factors that may influence OHC members' intention to participate are information and emotional support (Tseng et al., 2022).

*RQ2: How does gender affect the management of medical data?*

This study found no appreciable variations in the management of patients' PHI when binary gender was taken into account. According to recent research, there may still be shortcomings in working conditions that make occupational safety and health management challenging, even in spite of advancements in gender research and legislation (Forssberg et al., 2022). Worker efficacy is negatively impacted by poor occupational health, endangering system safety (Braun et al., 2022). Demographic information, including age, gender, and ethnicity, is typically included in studies on health systems. Sadly, it is noted that the data examined does not accurately represent the gender complexities that are currently taken into account, which may have negative effects. The literature reviewed observations on the integration of gender into medicine, pointing out potential avenues for researchers to better integrate gender data into their investigations. Gender is not binary, static, or concordant, to name a few of these (Albert and Delano, 2022).

*RQ3: What effect does the course level have on medical data management?*

A trade-off between potential benefits and individual privacy needs to be made in e-health systems. Users generally want to have autonomy over the data they share (Zegers et al., 2021). But cloud data access is becoming more and more popular (Sivan and Zukarnain, 2021; Azeez and Van der Vyver, 2019), allowing experts to make more precise diagnoses. The security protocols utilized to gain access to the systems are crucial in this case. The strength of passwords used by nursing students was taken into consideration in Q7: Is your password composed of at least eight characters, including capital and lowercase letters, numbers, and special keyboard characters (like #)? Specifically, notable variations were observed concerning the study path. Compared to fourth-year students, second-year students used stronger passwords. Weak passwords increase the risk of identity theft, data manipulation, and unauthorized use—the three most frequent attacks on e-health systems (Ahmad et al., 2021). Relevant information is sensitively retained in human memory. There is evidence that the survival-processing advantage—a term used to describe the ability to process information related to a subject's survival—can help with subsequent recall. In the literature, this feature has been sporadically examined in relation to password generation techniques (Chong et al., 2020). Additionally, there is a dearth of research on user behavior when creating passwords (Veroni et al., 2022).

## 5 CONCLUSION

The results of a survey conducted among UMU nursing students are presented in this paper. It was possible to determine future healthcare workers' awareness when handling sensitive information thanks to this work. Students understand the significance of their actions in ensuring data protection, for the most part. To improve privacy and security best practices, some behaviors should be addressed, though. These include verifying the appropriateness of clicking on web links, utilizing VPNs when connecting to public WiFi networks, and using alternate unlocking techniques for electronic devices, like fingerprint reading or facial recognition.

Future research aims to expand the survey by taking into account contemporary technologies like external physical security, blockchain, and cryptography. To increase public awareness of these technologies, educational events will be held that include cybersecurity-related practical exercises and oral presentations. The survey will then be conducted once more to examine the possibility of a shift in the degree of awareness. Furthermore, there's a chance to administer the survey to more students—both medical and nursing students—in an effort to analyze the variations among each cohort and include a larger sample size.

## ACKNOWLEDGEMENTS

This research is part of the OASSIS-UMU project (PID2021-122554OB-C32) and the Network of Excellence in Software Quality and Sustainability (RED2022-134656-T), all funded by MCIN/AEI/10.13039/501100011033/ and by ERDF A way to make Europe.

## REFERENCES

Aanestad, M. (2017). New Ethical Dilemmas Arising from the Growth of Personal Health Data. In *18th Annual International Conference Dilemmas for Human Services: Organizing, Designing and Managing*.

Ahmad, G. I., Singla, J., and Giri, K. J. (2021). Security and privacy of e-health data. In *Multimedia Security*, pages 199–214. Springer.

Albert, K. and Delano, M. (2022). Sex trouble: Sex/gender slippage, sex confusion, and sex obsession in machine learning using electronic health records. *Patterns*, 3(8):100534.

Alendal, G., Axelsson, S., and Dyrkolbotn, G. O. (2021). Chip chop—smashing the mobile phone secure chip for fun and digital forensics. *Forensic Science International: Digital Investigation*, 37:301191.

AlQadheeb, A., Bhattacharyya, S., and Perl, S. (2022). Enhancing cybersecurity by generating user-specific security policy through the formal modelling of user behavior. *Array*, page 100146.

Atkinson, J. S., Mitchell, J. E., Rio, M., and Matich, G. (2018). Your wifi is leaking: What do your mobile apps gossip about you? *Future Generation Computer Systems*, 80:546–557.

Azeez, N. A. and Van der Vyver, C. (2019). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. *Egyptian Informatics Journal*, 20(2):97–108.

Bani Issa, W., Al Akour, I., Ibrahim, A., Almarzouqi, A., Abbas, S., Hisham, F., and Griffiths, J. (2020). Privacy, confidentiality, security and patient safety concerns about electronic health records. *International Nursing Review*.

Bauer, D., Blough, D. M., and Mohan, A. (2009). Redactable signatures on data with dependencies and their application to personal health records. In *8th ACM workshop on Privacy in the electronic society*, pages 91–100. ACM.

Braun, S. S., Kaihoi, C. A., McDaniel, H. L., and Bradshaw, C. P. (2022). Profiles of teachers' occupational health: Associations with classroom management practices, gender, and race. *Teaching and Teacher Education*, 118:103819.

Breitinger, F., Tully-Doyle, R., and Hassenfeldt, C. (2020). A survey on smartphone user's security choices, awareness and education. *Computers & Security*, 88:101647.

Chong, I., Proctor, R. W., Li, N., and Blocki, J. (2020). Surviving in the digital environment: Does survival processing provide an additional memory benefit to password generation strategies? *Journal of Applied Research in Memory and Cognition*, 9(3):345–354.

Colwill, C. (2009). Human factors in information security: The insider threat–who can you trust these days? *Information Security Technical Report*, 14(4):186–196.

Corallo, A., Lazoi, M., Lezzi, M., and Luperto, A. (2022). Cybersecurity awareness in the context of the industrial internet of things: A systematic literature review. *Computers in Industry*, 137:103614.

Craig, J. S. (2009). The human element: training, awareness, and human resources implications of health information security policy under the health insurance portability and accountability act (hipaa). In *Information Security Curriculum Development Conference*, pages 95–99. ACM.

Enaizan, O., Zaidan, A., Alwi, N. M., Zaidan, B., Alsalem, M., Albahri, O., and Albahri, A. (2020). Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. *Health and Technology*, 10(3):795–822.

Evans, M., He, Y., Maglaras, L., and Janicke, H. (2019). Heart-is: A novel technique for evaluating human error-related information security incidents. *Computers & Security*, 80:74 – 89.

Fernández-Alemán, J. L., Sánchez-Henarejos, A., Toval, A., Sánchez-García, A. B., Hernández-Hernández, I., and Fernandez-Luque, L. (2015). Analysis of health professional security behaviors in a real clinical setting: An empirical study. *International Journal of Medical Informatics*, 84(6):454–467.

Fernando, J. and Dawson, L. (2008). Clinician assessments of workplace security training-an informatics perspective. *Electron. J. Health Inform*, 3(1):e7.

Forssberg, K. S., Vänje, A., and Parding, K. (2022). Bringing in gender perspectives on systematic occupational safety and health management. *Safety Science*, 152:105776.

Gajera, K., Jangid, M., Mehta, P., and Mittal, J. (2019). A novel approach to detect phishing attack using artificial neural networks combined with pharming detection. In *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)*, pages 196–200. IEEE.

Guo, Y., Zhang, Z., and Guo, Y. (2019). Optiwords: A new password policy for creating memorable and strong passwords. *Computers & Security*, 85:423–435.

Gupta, B. B. and Jain, A. K. (2020). Phishing attack detection using a search engine and heuristics-based technique. *Journal of Information Technology Research (JITR)*, 13(2):94–109.

Hoofnagle, C. J., van der Sloot, B., and Borgesius, F. Z. (2019). The european union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1):65–98.

Ishikawa, K., Ohmichi, H., Umesato, Y., Terasaki, H., Tsukuma, H., Iwata, N., Tanaka, T., Kawamura, A., Sakata, K., Sainohara, T., et al. (2007). The guideline of the personal health data structure to secure safety healthcare: The balance between use and protection to satisfy the patients' needs. *international journal of medical informatics*, 76(5):412–418.

Kävrestad, J., Lennartsson, M., Birath, M., and Nohlberg, M. (2020). Constructing secure and memorable passwords. *Information & Computer Security*.

Khando, K., Gao, S., Islam, S. M., and Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, 106:102267.

Kierkegaard, P. (2012). Medical data breaches: Notification delayed is notification denied. *Computer Law & Security Review*, 28(2):163–183.

Mammadova, M. (2015). The Problems of Information Security of Electronic Personal Health Data. In *7th International Conference on Information Technology in Medicine and Education (ITME)*, pages 678–682. IEEE.

McDermott, D. S., Kamerer, J. L., and Birk, A. T. (2019). Electronic health records: A literature review of cyber threats and security measures. *International Journal of Cyber Research and Education (IJCRE)*, 1(2):42–49.

Murphy, J., Stramer, K., Clamp, S., Grubb, P., Gosland, J., and Davis, S. (2004). Health informatics education for clinicians and managers—What's holding up progress? *International journal of medical informatics*, 73(2):205–213.

Price, W. N. and Cohen, I. G. (2019). Privacy in the age of medical big data. *Nature medicine*, 25(1):37–43.

Saura, J. R., Ribeiro-Soriano, D., and Palacios-Marqués, D. (2022). Assessing behavioral data science privacy issues in government artificial intelligence deployment. *Government Information Quarterly*, page 101679.

Sharma, T. and Bashir, M. (2020). An analysis of phishing emails and how the human vulnerabilities are exploited. In *International Conference on Applied Human Factors and Ergonomics*, pages 49–55. Springer.

Sivan, R. and Zukarnain, Z. A. (2021). Security and privacy in cloud-based e-health system. *Symmetry*, 13(5):742.

Švábenskỳ, V., Čeleda, P., Vykopal, J., and Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security*, 102:102154.

Tseng, H.-T., Ibrahim, F., Hajli, N., Nisar, T. M., and Shabbir, H. (2022). Effect of privacy concerns and engagement on social support behaviour in online health community platforms. *Technological Forecasting and Social Change*, 178:121592.

US-CERT (2016). How to protect your networks from ransomware. Technical report, Department of Homeland Security. United States Computer Emergency Readiness Team.

Veroni, E., Ntantogian, C., and Xenakis, C. (2022). A large-scale analysis of wi-fi passwords. *Journal of Information Security and Applications*, 67:103190.

Vincent, A. (2019). Don't feed the phish: how to avoid phishing attacks. *Network Security*, 2019(2):11–14.

Zabihimayvan, M. and Doran, D. (2019). Fuzzy rough set feature selection to enhance phishing attack detection. In *2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, pages 1–6. IEEE.

Zegers, C. M., Witteveen, A., Schulte, M. H., Henrich, J. F., Vermeij, A., Klever, B., and Dekker, A. (2021). Mind your data: Privacy and legal matters in ehealth. *JMIR formative research*, 5(3):e17456.

Zhang, L., Guo, Y., Guo, X., and Shao, X. (2021). Does the layout of the android unlock pattern affect the security and usability of the password? *Journal of Information Security and Applications*, 62:103011.