International Journal of Evaluation and Research in Education (IJERE)
Vol. 11, No. 1, March 2022, pp. 224~238
ISSN: 2252-8822, DOI: 10.11591/ijere.v11i1.22059

Home quarantined: Privacy at risk in technologically-oriented learning amidst COVID-19 pandemic

Client William Melchor Malinao[1], Mark Mata Sotto[2]
[1]College of Business and Management, Ifugao State University, Ifugao, Philippines
[2]College of Business and Accountancy, Cagayan Valley Computer & Information Technology College, Inc., Santiago, Philippines

Article Info

Article history:

Received Apr 23, 2021
Revised Dec 1, 2021
Accepted Dec 30, 2021

Keywords:

Philippines
Privacy
Privacy risk management
Private higher education
Technologically-oriented learning

ABSTRACT

The COVID-19 triggers technologically-oriented learning and is critical in ensuring that education continues after schools close physically. The internet has a plethora of learning opportunities but may invite privacy risks to users. Using descriptive-comparative research design, the study determined the contents and artifacts exchanged in online portals, the extent of use of social media sites, teaching-learning platforms, and educational websites. The sample was 341 college students of a family-owned private higher education institution. Finally, the difference in online privacy risk management practices was determined when grouped by selected demographic variables. Using means, t-test, and ANOVA, findings from an online survey showed that personal information is shared the most in online portals. For online learning, students heavily relied on Facebook, Microsoft Teams, and Google. To protect their privacy, respondents from all classes follow online management practices. Generally, the respondents' good affordances and decorum in the online media imply that they have good behavior and value creation. Still, a comprehensive strategy to safeguard data among learners in the utilization of online productivity platforms is a must.

Corresponding Author:

Client William Melchor Malinao
College of Business and Management, Ifugao State University
Boliwong, Poblacion East, Lagawe, Ifugao, 3600 Philippines
Email: clint13william@gmail.com

1. INTRODUCTION

The world commemorated the first anniversary of the World Health Organization's official notice of the COVID-19 pandemic. Individuals are exposed to a new standard kind of culture in which lockdowns, social distancing/isolations, covers such as personal protective devices, hand washing, taking vitamins and nutrients to maintain wellbeing, covering mouth, sniffling nose, and the unavoidable assistance of technology is an unquestionable necessity to continue for a lifetime is simply natural and expected [1], [2].

The pandemic's new standard has resulted in a massive change in education among the affected industries. School closures have an effect on educational frameworks all over the world. Today's teaching differs from the old show-and-tell method. Schools are closed and students are forbidden to go to class until vaccinations are available. Students can continue to study while staying at home, using a variety of learning modalities. The seeds of such radical change in education are being sown, sparked by massive shifts in knowledge, data innovation, and a desire to learn better. The closing of educational institutions resulting from COVID-19 prevention initiatives has affected the schooling, wellbeing, and functioning of all parties participating in and benefiting from educational systems worldwide. Students experience a learning deficit during the lockdown, so the introduction of distance learning aided by technologies is critical to ensuring the quality of education after the physical closing of schools [3], [4].

COVID-19 has forced the campus learning structure to move dramatically from face-to-face meetings to a technologically-oriented type of learning. Many universities that do not yet have an online learning system must hold online lectures due to their constraints. After discovering positive COVID-19 patient cases in mid-March, 2020, the government has mandated that employees operate from home. COVID-19 has required campuses to develop and adapt through distance learning in line with the progression of information and communication technology (ICT). Online learning is one alternative method of learning that can be used during the COVID-19 emergency. Learning that takes place over the internet is referred to as online learning. It includes connectivity, networking, versatility, and the ability to construct a range of learning experiences. The use of web and multimedia technologies can revolutionize the way knowledge is delivered and can be a viable alternative to traditional classroom learning [5]–[7].

Smartphones, tablets, and laptops are needed to implement internet-based learning since having access to information anytime and from any place. To promote the introduction of online learning, virtual platforms such as Google Classroom, Edmodo, and Schoology can be used. Instant messaging apps like WhatsApp and social networking sites (SNS) like Facebook and Instagram can be highly beneficial [8]. The growing use of digital material and delivery platforms uniquely capacitated to track, retain, and scrutinize learner's usage, exchanges, and academic outcomes at a high level has appeared as an opportunity and a source of concern. [9].

Surprisingly, there has been a record-breaking increase in online activity [10]. As people discover new ways to use online services to remain linked personally and professionally, much of the increased traffic goes beyond traditional internet browsing and video streaming. People are increasingly using video conferencing and social media to sustain their daily social activities [11]. COVID-19 has influenced how people function, live and communicate with one another all over the world. Working from home, quarantining at home, and maintaining social distance are all recommended or needed [12], [13].

Different web-based applications such as SNS provide a wealth of resources for learning support. Additionally, using SNS to maintain mental wellbeing is a viable choice. On social media sites, people create content, comment on it, forward it, and engage with others. People share details of their lives via email, pictures, videos, live video streaming, and other means to increase their sense of intimacy with others. The content will disclose personal details such as age, gender, place, and race to a large extent. Self-disclosure information can be spread, scanned, saved, and even processed more quickly on social media than it can in the real world. Increased and more widespread self-disclosure could result in users' online privacy being exposed in unpredictable and inappropriate ways. Additionally, learners view the privacy risk as a stumbling block to its maximum usage for learning. Users of these sites also create hundreds of online social networks (OSN) with other users with whom they connect and collaborate daily.

The privacy problem is one of the controversial issues that arise when interactions are mediated by a SNS [13], [14]. SNS users freely collect confidential information with their internet friends. If users include their real names and personal information, their privacy may be threatened. By providing personal information, users put their privacy at risk. They are vulnerable to cyber-attacks due to their increasing popularity and vast amounts of personal information (the most extensive database). Although users consider social media sites educational, the looming privacy problem can restrict their ability to communicate and collaborate online [15] thoroughly. For example, Facebook users' personal information was being shared with advertisers without consent and subsequently raised questions about Facebook's security [16].

SNS privacy threats are divided into two categories: risks faced by the SNS provider and risks resulting from user social interactions. The majority of students are concerned about privacy threats such as identity theft, cyberbullying, and impersonation, affecting their online learning engagement on social media sites. SNS providers allow their customers to actively connect in their network because the fundamental concept of SNS is knowledge sharing. As a result, the greater the number of (especially active) users, the greater the SNS's value. This is why, to have better connectivity to their customers, SNS providers emphasize service quality. Imposing a "true name policy" to achieve this, allowing the user to sign up using their real names and details [17].

Severe other security issues relating to e-learning systems were also identified. They are including software attacks (viruses, worms, macros, denial of service); technical software failures and errors (bugs, coding problems, unknown loopholes); acts of human error or failure (accidents, employee mistakes); trespass (unlicensed data access); and acts of human error or failure (accidents, employee mistakes); sabotage (information and system destruction); technical hardware failures or errors (equipment failure); acts of theft (illegal repossession of information); compromises to intellectual property (piracy, copyright, infringement); quality of Service deviations from service providers (power and wide area network (WAN) service issues); technological obsolescence (old-fashioned or outdated technologies); and deliberate acts of information extortion (blackmail for information disclosure) [18].

Online learning relies on the internet for its execution as an internet-based learning approach. As a result of interactions between students/teachers and resources or platforms, personal data is created during

the online learning process. On the internet, there is a slew of criminal activities and security dangers. As a result, the technologically focused learning environment is invariably vulnerable to security threats, dangers, and attacks. Because online learning takes place over the internet, any component of an online learning system can be hacked or attacked. Unauthorized modification and destruction of educational assets may result as a result of this. The inherent security threats on the internet, such as identity theft, impersonation, and insufficient verification, must be considered in technologically focused learning. Cybercriminals are interested in online learning systems because they can profit from their ability to hack into them. The risk is high; as online learning systems' capabilities and features become more complex, online learning becomes more vulnerable to security risks. Unfortunately, many schools and universities are rushed to implement online technology for teaching without rigorous planning and a complete grasp of online learning security.

Security has not been a high priority for online learning suppliers and practitioners. Personal privacy protection has become a significant issue for online learning as it has grown in popularity. To prevent any security breaches in online learning before it is too late, learners, online learning providers, and practitioners must pay more attention and exert more effort. Before integrating technology-driven alternatives to classroom instruction, it's critical to think about security and privacy. Students and instructors face significant security and privacy hazards if cybersecurity and privacy are not considered until the end of the planning and implementation phase or forgotten entirely.

Higher education is finding it more challenging to maintain control over how data is used, kept, and shared inside and beyond the virtual classroom as e-learners, need for flexibility, mobility, and empowerment grows. To defend themselves from various cybersecurity threats, learners should be taught particular personal information protection measures from three perspectives: before, during, and after learning. Building secure, standardized, highly available e-learning environments, centralized application management, policy, and practices governing the utilization of learning platforms making learners comfortable and secure are all required to meet demanding user needs [19]–[21]. Before the outbreak, many university rules and practices, educators, scholars, and instruction would all be present on campus. As a result, existing policies and procedures frequently fail to guide online learning [22]. The Commission on Higher Education issued guidelines for flexible learning. However, there is no provision on how learners, teachers, and school administrators manage and protect the data and privacy of learners in this new normal of schooling [23]. While student data has traditionally been used to aid retention and institutional decision-making, COVID-19 pandemic has introduced new and often problematic applications for data in higher education, posing a significant challenge to institutions. As a result, better instruction for learners on protecting their data in this technologically driven learning style is critical [24].

Educational institutions in Philippines have strived to ensure students can continue their studies despite the crisis and social distancing. With the spread of COVID-19, many students are forced to learn online and many educational institutions have moved into a type of learning that is technologically oriented. In reality, everyone is becoming a life-long learner as a result of online learning. The presence of private information and the willingness to disclose is often confronted with numerous dilemmas. There are many ways to reveal sensitive private information that can harm a person, most of all, university students in this pandemic.

Considering the aforementioned aspects, researchers believe that the sudden transition of Philippines higher education institutions from traditional face-to-face teaching and learning to only technologically oriented learning institutions is not well equipped to protect students' data sets. This has a significant influence on educational processes and student perceptions of the usage of the online environment, and these notions are the foundation of this endeavor. However, determining what is and is not confidential is never as straightforward as it appears. Vulnerability, sadness, and conflict can all result from the release of private information. Moreover, the disclosure of such material can expose the subjects to a barrage of abuse. As a result, learners, parents, and governments are becoming increasingly worried about how personal data and privacy are protected in online learning.

Using an online survey questionnaire among students in a private higher educational institution that adopted pure online learning, this study explored the contents and artifacts exchanged in online portals and the extent of use of social media sites, teaching-learning platforms, and educational websites. Finally, college students' online privacy risk management practices and the differences among them when grouped by demographic variables will be used as the foundation for developing a comprehensive strategy to protect data sets of learners in this period of new mode schooling. This also serves as a reference for stakeholders on securing personal data in online learning to avoid cybersecurity concerns.

The communication privacy management (CPM) theory is the theoretical underpinning for this endeavor, which gives a data protection system coordinated among individuals involved. Figure 1 shows the CPM's fundamental premises. By focusing on specific elements and creating a particular viewpoint, this theory guided the breadth of the relevant data in this inquiry. CPM is a rigorous research paradigm aimed at

establishing an evidence-based knowledge of how people make decisions about sharing and keeping private information private. According to the CPM, privacy boundaries are maintained and coordinated with various contact partners [25], [26].

When others are engaged, CPM theory is an adaptive privacy rule management framework that describes the dialectics of controlling the disclosure and protection of private information. The idea explains how people make decisions about sharing personal information that has been entrusted to them. The theory also analyzes the impact of functioning as a confidant on interpersonal relationships and the impacts of privacy turbulence. The idea is founded on eight axioms that define how people deal with confidential information [25], [27]. Thus, the observations were forwarded: i) Making decisions on what to announce and what to keep private is a constant balancing act; ii) Both disclosure and privacy have costs and benefits; disclosing and hiding personal information has consequences for both partnerships and individuals; iii) The right combination between privacy and transparency is essential for how we handle our relationships [25].

Figure 1. CPM's fundamental premises

The act of telling and reflecting private knowledge about others and ourselves is referred to as private disclosure. Knowledge about items that are important to them is considered private information. When examining the concept of boundaries, selecting what is private and who to share it with is vital because personal data might be about oneself or others. The privacy rule management system's decision to disclose is eventually made, which incorporates guidelines for information synchronization, disclosure characteristics, and boundary attributes. Unlike conventional self-disclosure, private disclosure places a greater focus on the unique content of the disclosure. People feel they are the only ones who have access to their information. People likely to reveal private details when there's a thin and permeable metaphorical barrier. When people breach privacy boundaries and allow access to the private information of others, they are granting others as joint owners of that data.

CPM uses the border metaphor to show the difference between being public and being private. People hold private information to themselves on one side of the boundary; on the other side, people show some private information to those in social relationships with them. When private information is shared, the boundary surrounding it is referred to as a mutual boundary, and the information is not just about the self; it belongs to the relationship. On the other hand, personal boundaries are established when private information stays with an entity and is not revealed.

Control and ownership theory is founded on the assumption that people believe they possess personal knowledge about themselves. Therefore, owners of information should be able to keep track of who else has access to it. In CPM theory, information is considered owned. Therefore, they have the authority to decide if they are willing to share knowledge with a confidant, i.e., a co-owner. Co-ownership of information entails a high level of accountability and knowledge of the regulations for a given disclosure. On the other hand, ownership can be perceived differently and how disclosure rules are interpreted differs from one owner to the next.

Furthermore, sharing is accompanied by the recognition that borders have broadened and will never be restored. The co-owners are in charge of deciding whether, when, and how knowledge is shared. When someone shares personal information with another person, they wish to maintain complete control over it. As a result, when someone else gets access to private information, they assume co-ownership of it and the responsibility to keep it safe. To manage the hazards involved with the transmission of private information, people employ laws to govern it.

Rule-based management system serves as a mechanism for comprehending how people make decisions about personal information. The rule-based management structure is a dynamic arrangement that allows for individual and collective management. To illustrate the privacy protection mechanism, Petronio

uses a boundary metaphor. Privacy borders demarcate the difference between private and public information. According to this notion, when people divulge private information, they rely on a rule-based management structure to control accessibility. Their privacy boundary governs the self-disclosure of a person. If there has been a disclosure, the two parties must negotiate privacy laws. People believe that they are the owners of their data and have the right to access it. People have control over their personal information thanks to personal privacy legislation. When others are informed, they become co-owners [25], [28]. The study's research paradigm is depicted in Figure 2.

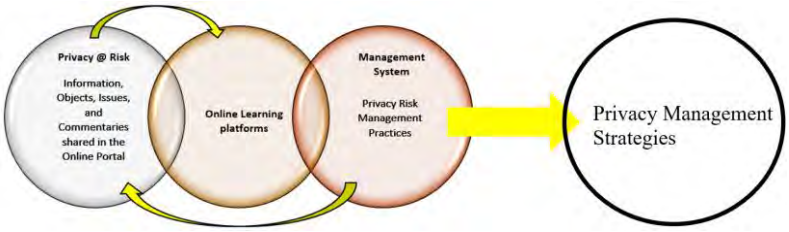

Figure 2. Schematic diagram of operational framework

College students trade various knowledge to obtain access to numerous learning sites for studying in this era of modern normal education. Students think they own their personal information and are entitled to manage how it is accessible, shared, and used on various online learning platforms. They are empowered to monitor how it is accessible, traded, and used. For sharing private information with others, co-owners must agree on mutually acceptable privacy norms. The disclosure of sensitive privacy online is a concern that is increasingly attracting the attention of academics. CPM theory also looks at how people handle their privacy in various communication situations and various channels. The basic premise that all personal information belongs to a single entity. College students encourage the construction of decision-making norms in managing, owning, and creating metaphorical boundaries of personal information in online learning platforms. College students are likely to be taught a set of privacy regulations. It will establish a complete privacy management policy to protect students' data in a technologically driven learning environment [25].

This study aims to determine how college students handle their online privacy risks in this era of new normal education. Specifically, it presents the following: i) Information, objects, issues, and commentaries are shared in the online portals during home quarantine; ii) The extent of utilization of SNS for online learning; iii) The extent of utilization on other educational sites; iv) The extent of utilization on other teaching-learning platforms; v) Online privacy risk management practices of college students; vi) The significant difference in the online privacy risk management practices of college students when grouped according to select demographic variables; vii) Recommend a comprehensive privacy management strategy for learners to safeguard their data in technologically-oriented learning in this time of the pandemic.

2. RESEARCH METHOD

This analysis used a descriptive-comparative research design. Students from Cagayan Valley Computer and Information Technology College, a family-owned private higher education institution in Santiago City, Philippines were randomly assigned to a data set. In this period of the pandemic, the college uses purely online learning, both synchronous and asynchronous. Students at the college are called socially active users because the majority (if not all) of them use social media. Furthermore, the majority of subjects relied on the purchased online productivity platform (OPP) and social media as part of their academic practices, such as Microsoft Teams, Zoom, Google Classroom, Facebook group chat, Twitter, YouTube, and microblogging, to name a few. A total of 341 student-respondents was calculated using the Lynch formula. Using stratified sampling technique, the following were known: 78 BSIT, 66 BSBA, 50 BSA/BSAT, 14 BSOA, 35 BSHRM, 35 CHS, and 53 BSECE/BSEE.

Expert pooling, refinement, field testing, and final refinement were used to create a researcher-made questionnaire based on various eminent authors. In addition, the reviews and advice of three experts were incorporated into the instrument before it was field-tested with 30 students. The instrument's reliability was determined using Cronbach's alpha of .893. According to eminent scholars, an alpha value greater than 0.8 indicates acceptable reliability. As a result, it is a secure and valid instrument. The questionnaire was divided into five parts, each of which was designed to address the study's stated goal. The questions also elicited perceptual and specific responses, which may help add specificity to the results after gathering data.

Through a channeled internal contact with the college officials, data was collected among Cagayan Valley Computer and Information Technology College students in Santiago City, Philippines. This attempt was made for academic purposes, and the identities of the respondents were kept private. The college president's approval was sought. The actual questionnaires were distributed via Google Forms to Cagayan Valley Computer and Information Technology College students who were chosen. As a result, 341 users have completed the online questionnaire within the period of lockdown. The frequency counts, ranking, weighted mean, t-test, and f-test were employed in this study to shed light on the formulated research issues. Data were tallied, treated, and analyzed using SPSS 21.

3. RESULTS AND DISCUSSION

3.1. Contents and artifacts shared in online portals

Table 1 shows the information, objects, issues, and commentaries shared by learners in the online portal for online learning in this time of the pandemic. Generally, findings revealed that personal information is the most shared information to different online portals used by the students, while insights and commentaries are the least commonly shared by learners. Basic information such as name, age, place of birth, birthdate, sexuality, personal photographs, personal number, and email address, according to the respondents, is needed to access various SNS like Facebook and Messenger.

Aside from the data mentioned, identification cards such as government-issued identification, student numbers, PINs, biometrics such as fingerprints, facial features, and authenticating features such as passwords, PIN, email address, and security answers are provided to freely access different learning sites such as academia, course hero, and subscription journals. Also, students from the private higher education institution share videos such as lectures, YouTube videos for learning, and recreational use such as funny and inspirational videos. Educational links/websites, supplementary lessons/readings, web reading activities, current events about coronavirus, vaccine, typhoon, and other current events are also being disseminated for information sharing. Usually, Facebook posts that inform, inspire, and make them happy are shared in the online portal. Webinars, school activities, and conferences are some of the most commonly shared events among students. Lastly, some students share their insights and commentaries about the current situation of the school, about the rules and regulations in the community, and the government. The self-disclosing conversation focused on general information related to global and sentimental aspects of the crisis, such as managing the spread of the virus and discussions about needs, help, thanks, and support.

Learners must provide personal information to enable them sign-up. Accordingly, some sites require payment before full accessibility of the site visited. Many people are willing to give up some privacy in the hopes of continuing to learn, slowing the spread of the disease, and hastening the return to normalcy [11]. Online learning is no more an option. It is a necessity. Online teaching and online learning can be termed as the panacea for the crisis [29]. Users use social media as the primary medium for information retrieval. Support related to current situations, such as COVID-19, should be circulated to decrease the potential panic and increase users' awareness worldwide [30]. Videos, infographics, and caps will be helpful to get the user's attention. People's sensitivity and attitudes toward privacy are shifting due to the pandemic, including when and how personal details can be revealed [31]. Personal data is generated during the online learning due to interactions between students/teachers and resources or platforms. Private space, private activities, and private information that one does not want to be shared with others are personal data.

Table 1. Information, objects, issues, and commentaries shared in the online portal by the respondents

	Contents and artifacts	Frequency	Rank
1.	Personal information	331	1
2.	Pictures	141	2
3.	Events	101	5
4.	Insights and commentaries	89	6
5.	Links and other people’s post	106	4
6.	Videos	126	3

3.2. Social media for online learning

Table 2 shows the respondents' internet utilization of social media for online learning. Findings revealed that among the different SNS, students constantly use Facebook for online learning. Social media became the most extensively used contact method during the COVID-19 pandemic. Higher education has shown that social media can improve students' learning experiences by facilitating engagement with them. These organizations may use social media to communicate with their students formally, promoting online learning. According to research, Facebook is one of the most extensively used resources in higher education

for various academic reasons. Faculty and students adopted SNSs as an official platform for scholarly communication, particularly formal learning, and large or large utilization. The proper use of social media might bring in a new era of social learning, social presence, and an online learning forum. Students and academic staff are active on these social media platforms to encourage online social networking and create a productive online learning environment. Students said social networking groups were more collaborative, user-friendly, and valuable than other accessible online networks [32]–[35].

However, submissions via social media platforms are discouraged because these platforms were never intended for such purposes. Tech companies such as Instagram, Twitter, and Facebook, among others, can profit from this detailed data set by selling it, processing it to extract sensitive information, or sharing it inappropriately [13], [36].

Table 2. The extent of utilization of social media for online learning

Social media	Mean	Descriptive interpretation
Facebook	3.51	Very great extent
Twitter	1.24	Very little extent
Instagram	1.08	Very little extent
Kakaotalk	1.47	Very little extent
TikTok	1.73	Very little extent
WhatsApp	1.03	Very little extent
WeChat	1.47	Very little extent
Hangout	1.52	Very little extent
Viber	1.46	Very little extent

1.0-1.75=Very little extent; 1.76-2.50=Little extent;
2.51-3.25=Great extent; 3.26-4.0=Very great extent

3.3. Synchronous and asynchronous teaching- learning platforms used

Table 3 presents the different teaching and learning platforms used by the private higher education institution. In this time of the pandemic, the private college relies solely on distance or remote learning. Learning takes place entirely online (virtually), with no face-to-face interaction. All course materials and documents are delivered virtually, and lectures are delivered either synchronously or asynchronously. Teachers virtually meet with their students in groups or one-on-one. End-of-term exams are typically administered remotely as unattended open-book tests or closed-book tests, but with online proctoring and a webcam for real-time monitoring of the student while the exam is being administered. End-of-term exams could be replaced by coursework components as well. Because the college did not have a formal e-learning systems (LMS), the private higher education institution purchased a licensed system of Microsoft Teams, which is the most commonly used teaching and learning platform, followed by Zoom, Google Meet, and Google Classroom.

Table 3. The extent of utilization of other teaching and learning platform

Other teaching-learning platforms	Mean	Description
Google Classroom	2.15	Little extent
Google Meet	2.28	Little extent
Zoom	2.76	Great extent
Microsoft Teams	3.78	Very great extent
College learning management system	1.12	Very little extent
Edmodo	1.95	Little extent

1.0-1.75=Very little extent; 1.76-2.50=Little extent;
2.51-3.25=Great extent; 3.26-4.0=Very great extent

During this year's COVID-19 pandemic, two video applications, according to respondents, Zoom video communications and Microsoft Teams from Microsoft, were beneficial. The main reasons for this are that they are both extremely simple to use (user-friendly). The course delivery process begins with an online lecture, which can be conducted using the available platform (Microsoft Teams). These online lectures provide a detailed explanation of the topic and opportunities for students to raise questions about the overall module. Meanwhile, these online lectures are recorded and shared with students via social media. The recorded lectures will provide students with a second chance to catch up if their Internet connections are disrupted or they have limited bandwidth [37]. Video conferencing tools such as Google Meet, Zoom, and Microsoft Teams aid in the organization of online lectures and discussions. Slideshows and a chat box are standard features of such tools [38].

Positive responses to Microsoft Teams were noted in India. Discussions through Microsoft Teams like the use of chat conversations and voice calling facility are good. Students felt easy and comfortable submitting multiple-choice questions and assignments, including for viewing of their grades. Overall, most students felt that Microsoft Teams were a better tool than other web-based platforms, such as Zoom, Google Meets for online learning and discussion. The most dominant online lectures were real-time video conferences, followed by asynchronous forms: Sending presentations to students, video recording, and written communication using forums and chats. The rarest form was an audio recording, which is not surprising since learning platforms and videoconference systems such as Microsoft Teams are widespread and have been freely available for quite some time [39], [40]. With Microsoft Teams, educators and learners can collaborate with ease meet for free with up to 300 students or community members and access persistent chat to ensure everyone stays connected for learning or work. It engages learners by organizing classrooms and assignments, collaborates and shares files, and accesses class materials in one central location [40].

However, faculty members identified several barriers. For example, the fact that many students were unfamiliar with these platforms because they had not received any training. As a result, students and lecturers appropriate knowledge and skills and ICT equipment must be ensured [32], [41]. This implies that students have the option of having their learning sequenced, directed, and evaluated with the help of a teacher. This interaction can occur within a community of inquiry, using various synchronous and asynchronous internet-based activities (video, audio, computer conferencing, chats, or virtual world interaction). These online environments foster the development of participants' social, collaborative skills, and personal relationships.

3.4. Educational websites visited

Table 4 presents the extent of utilization of other educational websites used by learnings in this time of the pandemic. Results in the foregoing table reveal that students are very aware ion the internet function as to education. Results revealed that students use Google to a very great extent. Access to accurate and up-to-date information is essential for students in this pandemic to assist them in learning through Google and Yahoo. Internet is used as an educational tool. The internet has a lot to offer [42].

Table 4. The extent of utilization of other educational websites

Other educational sites	Mean	Description
Google	3.75	Very great extent
Yahoo	2.56	Great extent
Bing	1.46	Little extent
Wikipedia	3.05	Great extent
Academia.edu	2.55	Great extent
DOAJ.org	1.695	Very little extent
Answer.com	2.055	Little extent
Khan Academy	1.66	Very little extent
Coursera	1.61	Very little extent
Course hero	1.845	Little extent
TedEd	1.585	Very little extent
Code academy	1.67	Very little extent
Open Culture	1.67	Very little extent
Code.org	1.75	Very little extent

1.0-1.75=Very little extent; 1.76-2.50=Little extent;
2.51-3.25=Great extent; 3.26-4.0=Very great extent

3.5. Online privacy management practices

Figure 3 depicts a summary of privacy management practices among learners of the private higher education institution in a technological-oriented learning environment during the COVID-19 pandemic. Learners employ 12 distinct management practices. Before, during, and after online learning, privacy practices are essential to safeguard data provided by learners into different learning platforms.

Respondents claimed that they frequently use their devices to log in/sign up to various online learning platforms such as tablets, smartphones, laptops, and desktops. To protect personal data, they ensure that their digital devices are appropriately configured. Respondents also frequently manage their network connection on their device by connecting to a wireless local area networking or mobile data network via a private Wi-Fi or wireless network. When visiting websites and downloading learning software, students frequently check the website address with SSL/TLS encryption to ensure that the link is protected and preserve any confidential data transmitted between two systems, blocking hackers from accessing and manipulating any content exchanged, particularly possible sensitive information.

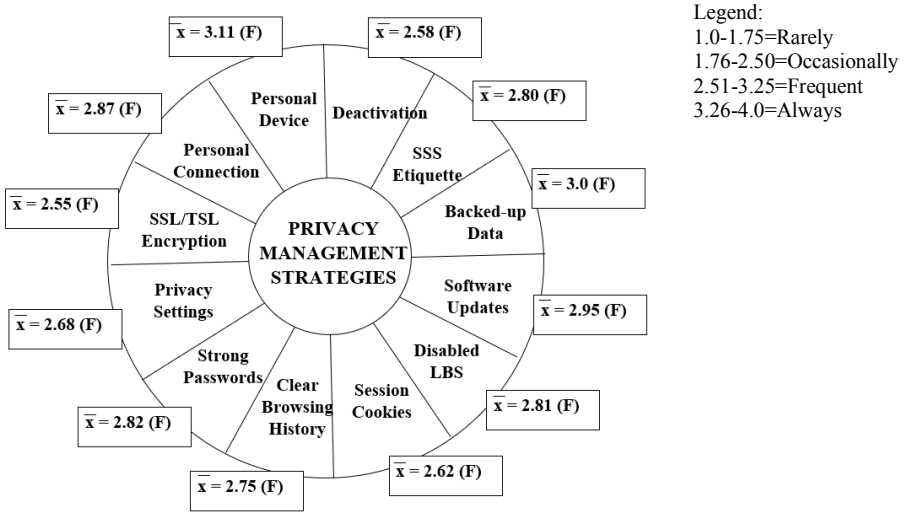

Figure 3. Summary of privacy management practices among learners of private higher education institution in techno-oriented learning amid COVID-19 pandemic

Learners from the private institution do not disregard the information in the privacy policy as they frequently read the essential legal information about their data, such as what information the app gathers, how the company uses it, with whom it shares it, and how it preserves it. To prove learners' identity, users typically provide credentials (username or e-mail address and a password) to learning platforms. Hence, the university learners create strong passwords with at least eight characters and a combination of four different types of characters: upper/lower case letters, numbers, and special characters (*/" &). When students use a public computer, students frequently clear their browsing history. Learners from the university do not save their login information, turn off the password storage function, and leave no trace of their web activity.

From a privacy sense, blocking all cookies is the best solution. On the other hand, session cookies were often utilized by students at the university because they are required to access many websites. As a result, if you close your browser, reopen it, and then return to your search engine, your search provider will not be able to correlate your current searches with past ones through cookies [34]. Learners are also aware that it is critical to protect location data. Thus, they frequently disable the location-based service (LBS) or global positioning system (GPS) option on their phone. This prevents the GPS from being enabled and as a result, providing the phone's location.

Cagayan Valley Computer and Information Technology College is a private institution run by a family, supervised by the Commission on Higher Education. Students at a computer school are well-versed in malware, and they are taught to back up the entire system as the best defense against hardware failure, software issues, and malware that can damage or corrupt files. Students frequently backup their data by copying it to external hard drives or cloud storage. They also ensure that their software is always up to date. When their devices notify them of a software update or patch, students immediately install it to help reduce the possibility of their device being vulnerable to security flaws. They are aware of the value of updating operating systems and internet security software.

According to the findings in Table 2, students heavily use Facebook for online learning and as a result, students frequently adhere to social networking etiquettes. Students use video conferencing tools with caution, post responsibly in forums, and sensitive in their insights and comments. Finally, when students have completed their online learning period, they deactivate/delete/disconnect/disable their account or leave the group.

The findings reveal that student at a computer school - a private higher education institution in Santiago City, Isabela, Philippines use various measures to keep their information safe while learning during this pandemic. The learners felt at ease and comfortable with the teaching and learning process in the new normal after taking various personal measures to protect the contents and artifacts that they shared in the online portal. The National Privacy Commission of the Philippines backs up the findings. The Education Data Privacy Council produced recommendations covering topics including online decorum, learning management systems, OPP, social networking, personal data storage, cameras and recording recordings of talks, and proctoring. NPC PHE Bulletin No 16 spells out the dos and don'ts of online learning for students, parents, teachers, and school officials [36].

3.6. Significant differences in privacy management practices of learners when grouped according to sex, age, area of residence, program, and year level

Table 5 presents the significant difference in online privacy management practices among private higher education institution of learnings when grouped according to select demographic variables. Results reveal that respondents, regardless of sex, age, residence, program, and year level, have similar practices on safeguarding their privacy during online learning. This suggests acceptance of all null hypotheses. This implies that demographic variables have nothing to do with their online risk management practices. All indicators revealed p-values greater than .05, which conclude insignificant results.

Table 5. The significant difference in online privacy risk management practices

Demographic variables		Composite mean	Descriptive interpretation	Decision
Gender (t-test)	Male	2.90[A]	Frequently	Accept Ho
	Female	2.83 [A]	Frequently	Accept Ho
Age (t-test)	16-19 years old	2.83 [A]	Frequently	Accept Ho
	20 and above	2.91 [A]	Frequently	Accept Ho
Residence (t-test)	Urban	2.89 [A]	Frequently	Accept Ho
	Rural	2.83 [A]	Frequently	Accept Ho
Program (t-test)	College of Engineering and Technology (BSIT/CHS/BSECE/BSEE)	2.78 [A]	Frequently	Accept Ho
	College of Business and Accountancy (BSBA/BSOA/BSHRM/BSA)	2.99 [A]	Frequently	Accept Ho
Year level (f-test)	1st	3.00 [A]	Frequently	Accept Ho
	2nd	2.77 [A]	Frequently	Accept Ho
	3rd	2.81 [A]	Frequently	Accept Ho
	4th	2.95 [A]	Frequently	Accept Ho

Legend: 1.0-1.75- Rarely; 1.76-2.50- Occasionally; 2.51-3.25- Frequently; 3.26-4.0- Always
Means of the same letter in each group shows comparable results at .05 level (t-test) (f-test)

The mean differences in gender, age, residence, and program suggest a marginal difference are .07, .08, .06, 21. The findings can be explained by the fact that female respondents aged 16 to 19, living in rural areas, are quite conservative, discreet, and conscious of what they share online under the College of Engineering and Technology. In contrast, male respondents aged 20 and up, living in urban areas, are confident in what they share online under the College of Business and Accountancy. Finally, although the entire course community is aware of online risk management activities, first-year respondents have a larger scale. This implies that, despite their lack of maturity in the first year, they are concerned about what information they share on various online platforms and, as a result, practice good privacy management.

The COVID-19 has accelerated e-commerce, online education, social media sites, mobile apps, and other virtual services. In the transition to personalized education, student data privacy and protection is a critical problem that must be addressed. Because of technology-related privacy issues as they rapidly adapt to the use of digital instructional software and services, students at a private computer school must be aware of and practice various measures to protect their personal information during these trying times.

3.7. Comprehensive privacy management strategies for learners

Data is generated during the online learning process due to interactions between students/teachers and tools or platforms. Students may not be aware of how to protect personal data in most cases. Wherever data is collected or used, privacy considerations arise. Authorized access, who has it and who determines it – is what privacy is all about. Data privacy is concerned with using and regulating personal data, such as establishing practices to ensure that users' data is secured and protected or not misused.

Higher education institutions should implement corporate approaches to managing their information security risks as part of existing governance structures. Institutions have to identify the 'controls' of data to establish clear lines of secure information sharing in a distributed environment. Implementing cybersecurity governance needs appropriate levels of understanding of the university's threats and the measures that must be put in place. Principles, heads of schools/departments, all the academic staff, and the IT support group in the higher education establishment should be clear about their responsibilities and stay alert to the emerging and evolving threats and risks to data users.

LMS or OPP should be officially implemented and used by academic institutions. All activities linked to online learning should be carried out on such a platform to the degree possible. For example, suppose the institution chooses to use OPP managed and delivered by a third party, such as Microsoft Teams. In that case, it should be safeguarded by a Data Processing Outsourcing Agreement or something similar. This can be accomplished through standard data protection measures in the contract between the educational institution and the OPP provider, along with terms and conditions governing the utilization of OPP.

The university should limit the use of online learning resources or technologies that have not been formally implemented by an educational institution (there is no formal tie between the school and the producer of these tools). Since, there has been no deliberate attempt to ensure their use is effectively safeguarded. As schools race to transfer instruction online in response to the pandemic, it is critical to ensure that appropriate policies are in place to protect student's privacy. The following (see Appendix) are recommended ways for managing privacy when using online productivity platforms for learners [43].

4. CONCLUSION

Online learning is gradually becoming a standard method of instruction for everyone, particularly during the COVID-19 pandemic. Data are collected during online learning, and personal users should be rewarded for data privacy and data security. Learners must master basic skills to protect their data and privacy while participating in online learning. Hence, the researchers shed light on contents and artifacts shared in the online portal by students from the private higher education institution in the Philippines in this paper. The identified data shared in various online portals include personal information, educational, informative, inspiring videos, significant events, links, insights, and commentaries. Social media platforms like Facebook, classroom management platforms like Microsoft Teams, and search engines like Google are the most widely used in the teaching and learning processes.

Students also identified 12 techniques that they employed before, during, and after their online learning: i) use of personal device; ii) use of personal connection; iii) search for SSL/TSL Encryption; iv) navigation of privacy policies/settings; v) set-up of strong password; vi) clearing browsing history; vii) use of short-lived cookies; viii) disable LBS; ix) regular software updates; x) consistent data backups; xi) SNS etiquette; and xii) account deletion and/or deactivation. Finally, the results show that there is no discernible difference in how students manage their online privacy. However, it should be emphasized that different people may have varied initial attitudes regarding sharing personal information and may determine how much information they are comfortable releasing. The good practice of students with online privacy risk management indicates a good observance of online behavior and etiquette. However, as cases of deviance from this phenomenon emerge, the institution must continue and expand its activities to continuously monitor student behaviors online. The defense of personal privacy should be encouraged. Privacy management strategies were recommended to protect themselves from different threats posed by online learning.

Since the study is limited to privacy risk practices of learners, future scholars should investigate individual privacy policies for each platform used, as well as the privacy risks faced by learners, for potential research. Future researchers should also think about/incorporate the viewpoints of parents and university administrators on how they keep data, including interventions and policies about the conduct of classes online.

REFERENCES

[1] J. Francis P. Yra, R. H. Castillo Jr., R. G. Bautista, J. G. Camayang, and A. Gibson G. Camayang, "Students' Online Learning Readiness and Internet Connectivity: Bases for the Customization of QSU e-Aral," *American Journal of Educational Research*, vol. 8, no. 11, pp. 878–884, Nov. 2020, doi: 10.12691/education-8-11-8.

[2] C. W. M. Malinao and R. G. Ebi, "Business Management Competencies as the Driver of Small-Medium Enterprises' Survival during COVID-19 Pandemic," *Puissant*, vol. 3, pp. 296–315, 2022, [Online]. Available: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-76615-6.

[3] G. Di Pietro, F. Biagi, P. Costa, Z. Karpiński, and J. Mazza, *The likely impact of COVID-19 on education: Reflectionsbased on the existing literature and recent international datasets*. Luxembourg: Publications Office of the European Union, 2020.

[4] R. G. Pastores, J. D. Dacanay, M. A. Mayoya, M. V Nanglihan, and R. G. Bautista, "All by Myself with Mr. Google: The Pandemic Education from the Lenses of Secondary School Students," *American Journal of Educational Research*, vol. 9, no. 11, pp. 660–664, 2021, doi: 10.12691/education-9-11-1.

[5] B. Nadeak, "The Effectiveness of Distance Learning Using Social Media during the Pandemic Period of COVID-19: A Case in Universitas Kristen Indonesia," *International Journal of Advanced Science and Technology*, vol. 29, no. 7, pp. 1764–1772, 2020.

[6] A. H. Fansury, R. Januarty, A. W. Rahman, and Syawal, "Digital Content for Millennial Generations: Teaching the English Foreign Language Learner on COVID-19 Pandemic," *Journal of Southwest Jiaotong University*, vol. 55, no. 3, 2020, doi: 10.35741/issn.0258-2724.55.3.40.

[7] A. Alchamdani, F. Fatmasari, E. Rahmadani Anugrah, N. Putri Sari, F. Putri, and A. Astina, "The Impact of Covid19 Pandemic on Online Learning Process in the College at Southeast Sulawesi," *Jurnal Kesehatan Lingkungan*, vol. 12, no. 1si, pp. 129–136, Sep. 2020, doi: 10.20473/jkl.v12i1si.2020.129-136.

[8] V. Kumar and P. Nanda, "Social media in higher education: a framework for continuous engagement," *International Journal of Information and Communication Technology Education*, vol. 15, no. 1, pp. 97–108, Jan. 2019, doi: 10.4018/IJICTE.2019010107.

[9] W. M. Stahl and J. Karger, "Student Data Privacy, Digital Learning, and Special Education: Challenges at the Intersection of Policy and Practice," *Journal of Special Education Leadership*, vol. 29, no. 2, pp. 79–88, 2016.

[10] R. J. M. Ramos, R. G. A. Ramos, R. N. Espaldon, D. G. D. Olaño, S. E. Laranang, and R. G. Bautista, "Online education in the midst of COVID-19 pandemic: Evidences from the lenses of IT students," *Turkish Online Journal of Qualitative Inquiry*, vol. 12, no. 7, pp. 5193–5201, 2020.

[11] T. Blose, P. Umar, A. Squicciarini, and S. Rajtmajer, "Privacy in Crisis: A study of self-disclosure during the Coronavirus pandemic," *arXiv preprint arXiv:2004.09717*, Apr. 2020, [Online]. Available: http://arxiv.org/abs/2004.09717.
[12] R. Holmes, "Is COVID-19 Social Media's Levelling Up Moment?" *Forbes*, 2020. [Online]. Available: https://www.forbes.com/sites/ryanholmes/2020/04/24/is-covid-19-social-medias-levelling-up-moment.
[13] J. Wang, "An In-depth Review of Privacy Concerns Raised by the COVID-19 Pandemic," *arXiv preprint arXiv:2101.10868*, Jan. 2021, [Online]. Available: http://arxiv.org/abs/2101.10868.
[14] S. Gurses and C. Diaz, "Two tales of privacy in online social networks," *IEEE Security & Privacy*, vol. 11, no. 3, pp. 29–37, May 2013, doi: 10.1109/MSP.2013.47.
[15] C. McLoughlin and M. Lee, "Social software and participatory learning: Pedagogical choices with technology affordances in the Web 2.0 era," in *ASCILITE - Australian Society for Computers in Learning in Tertiary Education Annual Conference*, 2007, pp. 664–675.
[16] S. Waters and J. Ackerman, "Exploring Privacy Management on Facebook: Motivations and Perceived Consequences of Voluntary Disclosure," *Journal of Computer-Mediated Communication*, vol. 17, no. 1, pp. 101–115, Oct. 2011, doi: 10.1111/j.1083-6101.2011.01559.x.
[17] J. van Dijck, "'You have one identity': performing the self on Facebook and LinkedIn," *Media, Culture & Society*, vol. 35, no. 2, pp. 199–215, Mar. 2013, doi: 10.1177/0163443712468605.
[18] N. H. M. Alwi and I.-S. Fan, "E-Learning and Information Security Management," *International Journal of Digital Society (IJDS)*, vol. 1, no. 2, pp. 148–156, 2010.
[19] Y. Chen and W. He, "Security risks and protection in online learning: A survey," *International Review of Research in Open and Distributed Learning*, vol. 14, no. 5, pp. 108–127, 2013.
[20] I. Bandara, F. Ioras, and K. Maher, "Cyber security concerns in e-learning education," *Proceedings of the International Conference of Education, Research and Innovation (ICERI2014) Conference*, 2014, [Online]. Available: http://ecesm.net/sites/default/files/ICERI_2014.pdf.
[21] N. Huu Phuoc Dai, A. Kerti, and Z. Rajnai, "E-Learning Security Risks and its Countermeasures," *Journal of Emerging research and solutions in ICT*, vol. 1, no. 1, pp. 17–25, Apr. 2016, doi: 10.20544/ERSICT.01.16.P02.
[22] L. Wallace, "Online teaching and university policy: Investigating the disconnect," *International Journal of E-Learning & Distance Education*, vol. 22, no. 1, pp. 87–100, 2007, [Online]. Available: http://www.ijede.ca/index.php/jde/article/view/58.
[23] The Commission on Higher Education (CHED), *Guidelines on Flexible Learning*. The Commission on Higher Education (CHED), 2020.
[24] K. H. Kyritsi, V. Zorkadis, E. C. Stavropoulos, and V. S. Verykios, "The Pursuit of Patterns in Educational Data Mining as a Threat to Student Privacy," *Journal of Interactive Media in Education*, vol. 2019, no. 1, May 2019, doi: 10.5334/jime.502.
[25] S. Petronio, "Brief Status Report on Communication Privacy Management Theory," *Journal of Family Communication*, vol. 13, no. 1, pp. 6–14, Jan. 2013, doi: 10.1080/15267431.2013.743426.
[26] H. Jia and H. Xu, "Measuring individuals' concerns over collective privacy on social networking sites," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 10, no. 1, May 2016, doi: 10.5817/CP2016-1-4.
[27] M. Allen, *The SAGE Encyclopedia of Communication Research Methods*. Thousand Oaks, California: SAGE Publications, Inc, 2017.
[28] K. C. C. Yang, A. Pulido, and K. Yowei, "Exploring the Relationship between Privacy Concerns and Social Media Use among College Students: A Communication Privacy Management Perspective," *Intercultural Communication Studies*, vol. 25, no. 2, 2016.
[29] S. Dhawan, "Online Learning: A Panacea in the Time of COVID-19 Crisis," *Journal of Educational Technology Systems*, vol. 49, no. 1, pp. 5–22, Sep. 2020, doi: 10.1177/0047239520934018.
[30] T. Kaya, "The changes in the effects of social media use of Cypriots due to COVID-19 pandemic," *Technology in Society*, vol. 63, p. 101380, Nov. 2020, doi: 10.1016/j.techsoc.2020.101380.
[31] T. Nabity-Grover, C. M. K. Cheung, and J. B. Thatcher, "Inside out and outside in: How the COVID-19 pandemic affects self-disclosure on social media," *International Journal of Information Management*, vol. 55, p. 102188, Dec. 2020, doi: 10.1016/j.ijinfomgt.2020.102188.
[32] A. E. E. Sobaih, A. M. Hasanein, and A. E. Abu Elnasr, "Responses to COVID-19 in Higher Education: Social Media Usage for Sustaining Formal Academic Communication in Developing Countries," *Sustainability*, vol. 12, no. 16, p. 6520, Aug. 2020, doi: 10.3390/su12166520.
[33] S. Manca, "Snapping, pinning, liking or texting: Investigating social media in higher education beyond Facebook," *The Internet and Higher Education*, vol. 44, p. 100707, Jan. 2020, doi: 10.1016/j.iheduc.2019.100707.
[34] I. T. Awidi, M. Paynter, and T. Vujosevic, "Facebook group in the learning design of a higher education course: An analysis of factors influencing positive learning experience for students," *Computers & Education*, vol. 129, pp. 106–121, Feb. 2019, doi: 10.1016/j.compedu.2018.10.018.
[35] R. Rasmitadila *et al.*, "The Perceptions of Primary School Teachers of Online Learning during the COVID-19 Pandemic Period: A Case Study in Indonesia," *Journal of Ethnic and Cultural Studies*, vol. 7, no. 2, p. 90, Jul. 2020, doi: 10.29333/ejecs/388.
[36] National Privacy Commission, "Data Privacy Education Council. Data Privacy and Online Learning." National Privacy Commission, 2020, [Online]. Available: https://www.privacy.gov.ph/wp-content/uploads/2020/10/DP-Council-Education-Sector-Advisory-No.-2020-1.pdf.
[37] A. O. Mohmmed, B. A. Khidhir, A. Nazeer, and V. J. Vijayan, "Emergency remote teaching during Coronavirus pandemic: the current trend and future directive at Middle East College Oman," *Innovative Infrastructure Solutions*, vol. 5, no. 3, p. 72, Dec. 2020, doi: 10.1007/s41062-020-00326-7.
[38] P. Chakraborty, P. Mittal, M. S. Gupta, S. Yadav, and A. Arora, "Opinion of students on online education during the COVID -19 pandemic," *Human Behavior and Emerging Technologies*, vol. 3, no. 3, pp. 357–365, Jul. 2021, doi: 10.1002/hbe2.240.
[39] D. Karthikeyan, "Assessing the effectiveness of Microsoft Teams during COVID-19 for online learning: A students' perceptive," in *Efficacy of Microsoft Teams during COVID-19- A Survey*, Bonfring, 2020, pp. 479–495.
[40] A. Aristovnik, D. Keržič, D. Ravšelj, N. Tomaževič, and L. Umek, "Impacts of the COVID-19 Pandemic on Life of Higher Education Students: A Global Perspective," *Sustainability*, vol. 12, no. 20, p. 8438, Oct. 2020, doi: 10.3390/su12208438.
[41] G. Lindberg, "How to Use Microsoft Teams for Online Learning," *Saint Leo University*, 2020. [Online]. Available: https://www.saintleo.edu/blog/how-to-use-microsoft-teams-for-online-learning.
[42] N. Dogruer, R. Eyyam, and I. Menevis, "The use of the internet for educational purposes," *Procedia - Social and Behavioral Sciences*, vol. 28, pp. 606–611, 2011, doi: 10.1016/j.sbspro.2011.11.115.
[43] R. H. Huang *et al.*, *Personal data and privacy protection in online learning: Guidance for students, teachers and parents*. Beijing: Smart Learning Institute of Beijing Normal University, 2020.

APPENDIX

Before online learning

Activity: Setting up learners' device
Related privacy: Personal data stored in devices such as personally identifiable information
Risks: Loss or theft and abandonment or switch
Strategies: i) Take care of any devices with cameras or microphones; ii) Keep personal items out of sight in public settings to avoid theft; iii) Lock your gadgets and use strong passwords; iv) Make sure the operating system on your devices is up to date; v) Download and install anti-virus software; vi) Do not root or jailbreak your phone; vii) Back up crucial personal data regularly.

Activity: Managing network connection on the personal device
Related Privacy: Personal data stored in devices such as personally identifiable information
Risks: Network intrusion, man-in-the-middle attack, and browser hijacking
Strategies: i) Connect to a VPN through a cellular network or via Wi-Fi; ii) Use Cellular data only; iii) Use Wi-Fi only.

Activity: Choosing and installing learning tools, as well as looking through the privacy policies
Related Privacy: Personal Identifiable Information (PII), biometric data, and primary data
Risks: Websites that are fake or malicious, computer viruses, malicious software, and data misuse via online learning tools
Strategies: i) Look at the URL: Websites without SSL/TLS encryption or the necessary certificates to indicate they've used that type of security protection cannot guarantee you anything; ii) Use only authentic sources to download; iii) Download software from official websites and app stores for operating systems, such as Microsoft Store, Apple App Store, and Google Play Store; iv) Look at the pricing information to see any upfront costs, such as sign-up fees or peruse fees.

Activity: Creating accounts using strong passwords
Related privacy: Personal Identifiable Information (PII) and network identity data
Risks: Password leaks
Strategies:
Passwords should contain: i) A combination of four different types of characters: upper/lower case letters, numerals, and special characters; ii) If you only have one unique character in your password, do not make it the first or final character. It should not be a name or word from any dictionary language, it should not contain any part of your name, address, or date of birth; and you should use a new password for each service or website.

Activity: Using a device that is not yours to log in
Related privacy: Personal Identifiable Information (PII) and network identity data
Risks: Leakage of user information
Strategies: i) Do not save your login credentials; ii) Always log out of websites by clicking the site's "log out" button. It is not sufficient to just shut the browser window or type in a different URL; iii) If you disable this option, no one else will be able to log in as you once you've stopped using the computer; iv) Never leave a computer with important information on the screen unattended. If you must leave the public computer, log out of all programs and close any windows that may contain sensitive data; v) Turn off the password storage functionality. Turn off the Internet Explorer function that "remembers" your passwords before you begin exploring the web; vi) Remove any temporary internet files and surfing history from your computer.

During online learning

Activity: Using search engines with caution
Related privacy: Internet browsing leaves a trail
Risks: Information such as user preferences and learning patterns are extracted and used maliciously. User data leaking as a result of a platform assault from the outside Providing illegal information to third-party platforms
Strategies:

i) Do not use words in your Google searches that disclose personal details. Do not use the internet to access your profile, addresses, card details, social security number, or other private information. These types of searches may yield a map that directs you to your front door. They may also expose you to identity theft and other privacy invasions.

ii) Do not use the search engine that your Internet service provider provides. Because your ISP knows who you are, it will link your identity to your searches. It will also be able to create a single search history from all of your searches.
iii) Do not utilize your search engine or any other tools that are associated with it. You can occasionally create a personal account and log in to search engines. However, many search engines are linked to other services, like Google's Gmail and Google Chat, MSN's Outlook, and Skype. Therefore, when you log into the search engine or one of those other services, your queries may be linked to each other and your account. So, if you have a Google Gmail or MSN Outlook account, do not use the appropriate search engine (Google or Bing Search, respectively) while logged in.
iv) The best option is to block all cookies. Allowing short-lived "session" cookies may be more convenient because cookies are necessary to view many websites (though less privacy-protecting). Because cookies only last as long as your browser is open, if you close it, reopen it, and then return to your search engine, your search provider will be unable to correlate your current searches to previous ones.

Activity: Identifying service location
Related privacy: Information about your location
Risks: Location information leaking poses a threat to personal and property safety; user information leaking occurs due to an outside attack on platforms; and illegal information provision to third-party platforms.
Strategies:
i) Turn off the cellular and Wi-Fi radios on your phone. The simplest way to execute this task is to use the "Airplane Mode" option. This disables your mobile radios and the built-in Wi-Fi radio on your phone, making it impossible for them to connect to their respective networks.
ii) Turn your GPS radio off. When you turn off location-based functions on your phone, your GPS is off, which prevents your phone from broadcasting its whereabouts. Turning on Airplane Mode also disables GPS on some phones.
iii) While Location Reporting broadcasts your location to many apps, Location History preserves your location for future searches and software like Google Now. Learners can also delete their whole location history by clicking "Delete Location History" from the Location History menu.

Activity: Back-up data
Related privacy: Personally Identifiable Information (PII)
Risks: Personal information resale, advertisements, and life safety
Strategies:
Your best defense against hardware failure, software issues (such as those caused by upgrades), and viruses, which may both ruin and damage your files, is to back up your entire system. If you do not make regular backups, you risk losing important papers, irreplaceable photographs, and custom installations that you may have spent hours creating.
i) A data backup storage option. Backup storage keeps a copy of your data, and for a successful backup, you must have it selected, provisioned, and ready to go (and recovery).
ii) Data backup to local or USB drives. Students can back up their work if they have enough capacity on their local disks or external USB devices. These backups are quick and straightforward, and they do not necessitate the use of a network. Local backups have the disadvantage of being lost if your system is damaged by fire or flood. If your backups are kept in the same area, they may be lost as well. You'll have to manage backups on a computer-by-computer basis in many cases, which can be problematic in larger systems. Local and USB disk backups are ideal for rapid backups of a few systems and are meant to recover specific data or systems in the event of software failure. Backups to local and USB disks are appropriate for quick backups of a few systems and are designed to retrieve specific data or systems in the case of software failure.
iii) Data backup via cloud storage. A recent alternative to tape backup is cloud storage. With this type of solution, you subscribe to a specific storage capacity in the cloud vendor's or service provider's data center. You do not need any hardware, like tape drives, to send backups to the cloud, but you do need an internet connection. In addition, your provider may be able to minimize the issues associated with uploading large amounts of data by supplying physical data shipment or an early seeding effort.

Activity: Using a social networking service to learn
Related privacy: Personal Identifiable Information, personal property information, and personal location information are all examples of personally identifiable information.
Risks: Live images including personally identifiable information, such as personal location, personal property, and so on.

User data leaking as a result of a platform assault from the outside
Information leakage from personal devices as a result of an outside attack

Strategies:
Follow social network etiquette

i) Avoid posting photographs of oneself that are unpleasant, revealing, or unpleasant at all costs. Keep in mind that the photographs you publish could be taken at face value and regarded as a reflection of your personality, not to mention that they will remain on the internet permanently. What may seem endearing in high school or college may not be so attractive to potential employers in the future. Never share sensitive personal information online, such as birthdates, phone numbers, addresses, schools, or hometowns, to lessen the risk of crime, vandalism, or identity theft. Never tell someone you'll be away from home for a lengthy period, such as on vacation. Avoid utilizing social media until you're entirely comfortable with the group of online friends with whom you'll be sharing your updates and have a good grasp on your privacy settings.
ii) The tone of your voice and your demeanor. Professionalism is necessary; do not say anything online, in the most public of places, that you would not say in a social or professional setting. On the other hand, politeness and respect are required: constantly consider others and treat them as you would like to be treated. Before sending any correspondence, double-check spelling, punctuation, grammar, and word choice to make sure they do not reflect poorly on the sender. Avoid using shorthand, abbreviations, or online slang if possible, and only use them in the most informal conversations.
iii) Being a responsible user. Recognize that each online forum (social networks, blogs, and digital communities) has its own set of rules, social customs, and interaction methods. Before you utilize one, take a step back and observe how people interact to choose what posting, sharing, and conduct norms to follow. Before leaving comments on other people's profiles or walls, or tagging them in your posts, think about how your actions and statements can be perceived. Use privacy settings to limit who can see your posts and shares. Send a brief message introducing yourself and explaining why you're trying to contact someone you do not know to request them to be your friend.

After online learning

Activity: Removing data traces in online learning and deactivating an account
Related privacy: Personally, Identifiable Information, personal internet history
Risks: Illegal retention of information after deleting
Strategies: Delete user-generated content and deactivate the account after usage.

BIOGRAPHIES OF AUTHORS

Client William Melchor Malinao is a Ph.D. in Commerce Candidate at Saint Mary's University of Bayombong, Nueva Vizcaya, Philippines. He is a licensed professional teacher, a Civil Service eligible under Presidential Decree 907, a certified bookkeeper, and level 1 trainer's methodology credential holder. At present, he is teaching in the business administration program at Ifugao State University – Lagawe Campus, where he is also the program chairperson for the Master of Business Administration program. Marketing Management, Business Education and Management, Entrepreneurship, and Social Sciences are the subjects of his study. He can be reached at email: clint13william@gmail.com or client13.ifsu@gmail.com.

Mark Mata Sotto is a graduate of Master in Business Administration and currently enrolled in Doctor of Philosophy in Commerce at Saint Mary's University of Bayombong, Nueva Vizcaya, Philippines. A licensed professional teacher and certified bookkeeper with level 1 trainer's methodology. At present, he is the youngest academic dean of the College of Business and Accountancy in Cagayan Valley Computer and Information Technology College - Santiago City. He is also an incumbent Sangguniang Kabataan Chairperson and SK Federation Secretary in the City of Santiago. His strong passion and leadership brought him with various local, regional and national awards. He can be reached through his email at: sottomark217@gmail.com.