European Proceedings of
Multidisciplinary Sciences
EpMS

www.europeanproceedings.com
e-ISSN: 2421-826X

DOI: 10.15405/epms.2022.10.35

ICONSPADU 2021
International Conference on Sustainable Practices, Development & Urbanisation

STAYING SAFE ONLINE: ONLINE PRIVACY MANAGEMENT BEHAVIOUR AMONG DEAF COMMUNITY

Wan, Puspa Melati (a)*, Affezah Ali (b), Hamdan Mohd Salleh (c), Nor Alina Ismail (d)
*Corresponding author

(a) Taylor's University, 1 Jalan Taylors 47500, Subang Jaya, Selangor, WanMelati.WanAH@taylors.edu.my
(b) Taylor's University, 1 Jalan Taylors 47500, Subang Jaya, Selangor, Affezah.Ali@taylors.edu.my
(c) University Selangor, Bestari Jaya Main Campus, Jalan Timur Tambahan, 45600 Bestari Jaya, Selangor, Malaysia, hamdan@unisel.edu.my
(d) SEGi University, Jln Teknology, Kota Damansara 47810 Petaling Jaya, Selangor, noralinaismail@segi.edu.my

Abstract

Statistics on internet usage and reliance in Malaysia have shown staggering annual growth, especially among youths. Though advantages of technology adoption are acknowledged, the issue of cybersecurity has been a rising concern with incremental cases over the years. To ensure users' safety and devise an inclusive action plan, it is imperative to understand the usage pattern and the factors that promote or hinder certain online behaviours. This understanding can only be done by looking at different subgroups as there may be unique experiences, such as the Deaf community. Since there have been limited studies on Malaysian Deaf youths' privacy management behaviour, this study is imperative to be explored. Methodologically, 17 Malaysian Deaf youth were chosen through a multi-stage sampling method. Semi-structured interviews and face-to-face surveys were conducted in Bahasa Isyarat Malaysia (BIM) by an interpreter to examine the extent of Deaf youth engagement in online privacy management as well as to investigate the factors that contribute to or hinder their privacy management behaviour. It was found that the respondents mainly engaged in basic privacy management behaviours due to their lack of exposure to the technical aspects of privacy management as well as the negative repercussions of their behaviours. These findings point to the urgent need for further awareness and education training among the Deaf community to ensure that all users are safe amidst the further technological advancement of the nation.

Keywords: Contributing factors, cybersecurity, hindrance factors, Malaysia, youth

https://doi.org/10.15405/epms.2022.10.35
Corresponding Author: Wan, Puspa Melati
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

1. Introduction

The use of technology and social media is essential especially in this technology-centric period and among the digital natives. Users claimed that technology and social media help them to keep in touch with their loved ones (Samuel-Soma et al., 2020), especially for those who are unable to meet physically due to their tight schedules (Sponcil & Gitimu, 2013). The advancement of social media and technology also helps them create, maintain and reconnect with old friends as well as enable constant interaction with others despite being geographically distant (Sponcil & Gitimu, 2013). Social media is also used as a platform for unique expression and creative learning platforms (Ajibade et al., 2018)

A survey done by the Malaysian Communications and Multimedia Commission (2018) highlighted that the percentage of Malaysian Internet users in 2018 stood at 28.7 million (87.4%) compared to 24.5 million (76.9%) in 2016. This is mainly due to the better telecommunication structures and available services. It was also found that most of the Internet users had shared content online, particularly among younger users (61.8%), with educational content and entertainment/humorous content being the most usually shared content. Users also use the Internet to seek information (85.5%) and to connect with others (85.6%). The large population of the users (96.5%) do use the Internet to message others and 60.6% of them to communicate with others via video and voice calls (Sobers, 2021).

With the increasing trend of usage, engagement, and reliance on social media, concerns over cyber security also heightened among policymakers, authorities, parents, and even end-users. Data by Malaysia Computer Emergency Response Team (MyCERT) (2022) reveals that in January 2021 alone, there have been 10,016 reported cases that breached cyber security, and there were 10,699 reported cases throughout 2018. This can be contrasted to 2,123 cases back in 2008 (2019c). These data include cases such as intrusion, cyber harassment, spam, vulnerabilities reports, fraud, malicious codes, among others.

Researchers explored the risky behaviours engaged by users that compromise their online security, such as sharing passwords. A longitudinal study done with 1,272 students found that the more engaged the children are online, the more likely they would share their passwords. The password sharing behaviour was also the norm among them (Meter & Bauman, 2015). Another risky behaviour engaged was self-disclosure. It has been argued that individuals tend to disclose more about themselves online than in person (Suler, 2004). Studies also show that people, especially children, believe that merely by having passwords they are able to protect their personal information (Choong et al., 2019). Cyber security also tends to be compromised as users tend to release personal information due to the perceived better quality of service and when a multilevel privacy control method is used (Kim & Ko, 2018). Lack of exposure and digital literacy have also been argued to contribute to risky behaviour and online privacy management (Baruh et al., 2017).

2. Problem Statement

Being safe online arguably is exacerbated for people with different abilities, including the Deaf population. The World Health Organization(WHO) (2020) has reported that 466 million people are categorised as individuals with hearing loss. Researchers have claimed that online platforms used to be the preferred avenue for people with different abilities as their stigma and discrimination can be

https://doi.org/10.15405/epms.2022.10.35
Corresponding Author: Wan, Puspa Melati
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

neutralized online hence translating into better and safer social interaction experiences (Bowker & Tuffin, 2006). Online interaction has also been an important platform for self-identity internalisation by people with different abilities as these identities can be constructed and reconstructed due to their anonymity. However, when the information about their disabilities is revealed later, ethics issues and conflict may occur (Van Gelder, 1991). Another area of research regarding people with disability is the use of social media platforms as a catalyst of change, for example, the #CripTheVote campaign (Mann, 2018).

However, based on the current literature, there has not been much discussion on the Deaf community concerning their online privacy management behaviour. Though there has been effort to educate the Deaf population via a cybersecurity curriculum in schools abroad, such initiative is non-existent in Malaysia (University of Alabama Huntsville, 2019). With the current pandemic, heavy reliance on technology also would heighten the challenge among people with disabilities who find it more challenging to adapt and have adequate access (Lazzari & Baroni, 2020).

Hence, this research is imperative to provide necessary insights on the extent that Deaf youth engage in online privacy management, contributing factors to them engaging in privacy management behaviour, and reasons for not engaging in online privacy management. This information would enable strategic planning to ensure that all members of the society are safe online.

3. Research Questions

i. This paper covers three research questions, namely:
ii. To what extent do Deaf youths engage in online privacy management behaviours?
iii. What are the contributing factors towards online privacy management behaviours among Deaf youths?
iv. What are the hindrance factors for Deaf youths to engage in online privacy management behaviour?

4. Purpose of the Study

This present study was conducted to provide an intersectional lens on privacy management behaviour as the Deaf community may have different challenges and unique experiences due to their culture and life chances. The research findings will be helpful for policymakers, application developers, educators, trainers, and other relevant stakeholders to understand the perception, experiences, and challenges among Deaf youths regarding their privacy management behaviour. This effort is also in line with the aim of the government to enhance inclusive development and provide a safe virtual environment in the effort to promote inclusive adoption of technology and its best practices.

5. Literature Review

5.1. Emails and Social Media use among Disabilities

Early studies have found that the main purpose of engaging in social networking sites is mainly to communicate and maintain relationships with others (Samuel-Soma et al., 2020). The use of technology

https://doi.org/10.15405/epms.2022.10.35
Corresponding Author: Wan, Puspa Melati
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

like SMS, email, and any other social media(s) has also been commonly used among the Deaf community since the past decade (Maiorana-Basas & Pagliaro 2014). Previous research highlighted that these technologies pave the way towards "levelling the playing field" for individuals with different abilities. Exchanging information nowadays is made easy with the technological advancement and vast social networks that individuals have. Social networks then can be defined by a group of people connected based on meaningful relationships (Tuunainen et al., 2009). These social networking sites or social media online are platforms where communities are being developed and maintained over the past years. Though these social network platforms are acknowledged as essential platforms for many, there have also been rising concerns on privacy management and cybersecurity issues. One of the concerns is due to the increased self-disclosure that people tend to engage in which they otherwise would not in the physician world (Gross & Acquisti, 2005).

Past literature also reported that youths tend to score low on awareness regarding online privacy issues and available online privacy protection features provided by Facebook. It was found that most of the young generation, including the Deaf, are aware that sharing of personal information can place them at risk such as identity theft or theft and these youths also reported to have sufficient information on ways to protect their personal data. Yet, it was found that many still share their personal data and do not engage in privacy management behaviours perhaps due to the exaggerated sense of online safety (Gross & Acquisti, 2005).

5.2. Online Privacy Management among Disabilities

Based on past studies, it was found that online privacy has been acknowledged as important to most Internet users (91.9%), and about 86.0% of them do engage in proactive measures to protect their personal information online (MCMC, 2018). However, this data often does not reflect marginalised communities as they may not be among targeted or included respondents in such studies (Michella & Claudia, 2014). Thus, it is unclear the extent to which groups such as the Deaf community understand the only privacy management issues and engage in privacy management behaviour.

In fact, according to Tuunainen et al. (2009), users are aware of online privacy features and understand the functionality, but many are not equipped to protect their personal data. Privacy features and settings can also be quite technical and use terms and jargon that may not necessarily be easily understood. Hence, users may not be able to engage in profile control or safe participation online.

6. Research Methods

6.1. Sample

This paper focuses on Deaf youths in Malaysia to examine their online privacy management behaviour. Definition of youth by National Youth Development Policy (2014) was adopted, referring to individuals between 15 and 40. The choice of youth reflects the higher average hours per day by these users: Below 20 years old –6.7 hours, 20's – 8.0 hours, 30's – 7.3 hours, 40's – 5.9 hours, 50's – 4.5 hours, 60 and above – 3.7 hours. In terms of the mean age of users, the number has increased from 33.0 years in 2016 to 36.2 years in 2018 (Malaysian Communications and Multimedia Commission [MCMC], 2018).

https://doi.org/10.15405/epms.2022.10.35
Corresponding Author: Wan, Puspa Melati
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

The sample was chosen using a multi-stage sampling method and samples from Malacca, Negeri Sembilan, Perak, Penang, and Sabah states. This research is part of a larger project that includes all states in Malaysia, but only these five states were included in this paper.

To obtain the samples, researchers approached the social organisations for the Deaf community in every state in Malaysia. These state-wide social organisations serve as an important referent point to ease the identification of respondents within each state. The respondents were also recruited from each state's Bahasa Isyarat Malaysia (BIM) WhatsApp Channel [MyBIM Chl].

Within the sampling frame obtained from those social organisations, samples were selected using a simple random sampling method. A total of 17 respondents were selected for this study with the criteria of respondents who (1) are 15-40 years old, (2) owns technological gadgets, i.e., computer/laptop; smartphone; tablets (3) have social media accounts or have downloaded applications/software and (4) uses the gadget(s) at least 6 hours a day.

6.2. Data Collection Method

A qualitative approach enabled the researchers to learn about online privacy management among Deaf youths. The semi-structured interview was conducted using Bahasa Isyarat Malaysia (BIM) to ensure that the respondents could fully understand the questions posed. The survey questions cover demographic details and questions related to online privacy behaviour and strategies. All interviews were recorded for transcription process and data validation. The data was analysed by using QSR International's NVivo 12 software.

7. Findings

7.1. Privacy Management Behaviour

Based on the interview data, it was found that Deaf youths do engage in some basic privacy management behaviour. They reported trying to minimise the information that they provide on social media. The majority of them shared their real name, including family name, birthdate, marital status, sex, birthplace, hometown, and a short introduction about what they like, such as sports and food. They consider this information as safe to be shared. They, however, avoided giving their complete address, workplace, phone number, or bank details. A number of the respondents said they should avoid providing bank-related information, but they should avoid making any financial transactions, especially through arrangements made via social media. Only one of the respondents mentioned that she included check-ins as she tends to share pictures of food in her account. Interesting to note that one of the respondents said that he would try to include as minimal information as possible. If the application requires more detailed personal information to be included, he will try to fill out the bare minimum and keep on adding the information to see if he can go about with the least information. Quoting him:

> *"When I fill up a registration form online, let's say that I did not want to fill in my phone number and a few others, I would not be allowed to go through. Then I refiled the form and saw what information I can share, I just put what I can share except phone numbers. Still, if I am not*

https://doi.org/10.15405/epms.2022.10.35
Corresponding Author: Wan, Puspa Melati
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

allowed to go through and everything is reset. I will repeat the registration with more information." (Freddie)

Though a few of them said they prefer not to include email, they acknowledge that almost all of the applications would require such input before they can use it – which they would comply with using the application. All of them are not aware of how the system works, but they know from the stories shared by others not to provide their personal information to strangers, they may lose their money or steal their identities.

Another common way for the respondents to protect themselves was to ignore and/or block any suspicious messages and/or persons. Some respondents said they would quickly block someone if they received messages to indicate that they won something or some money. Three of them said that they would block some messages when they are unclear about the offer provided or if the messages seemed too good to be true. Some quotes from them are as illustrated below:

"I ignored them. I told them that they are cheaters and I said goodbye to them. Then I blocked them immediately. I blocked them on Mudah.com and WhatsApp." (Cassie)

"Somebody tried to cheat me, I blocked him immediately. He told me that I won some money, I did not believe him. I just ignored and blocked him." (Nina)

Only two of the respondents said that they use the privacy settings in order for them to keep them safe online. This includes setting the videos that they share online in private mode so that others cannot pry and stalk on them and disable the feature that would allow strangers to message them directly. However, one of them said that she did not know the technicality to set the privacy but managed to get a friend to help.

Only a few respondents mentioned other behaviours that they engage in to maintain their privacy and keep them safe online. One of the respondents said that she would always log out after using any applications. She mentioned that that is important as she will receive a notification when someone is trying to log in; hence, she can change the password or take any other measures necessary. Two of them said that they would clear caches, especially after using the bank applications.

7.2. Contributing Factors to Engaging in Online Privacy Behaviour

Most of the respondents have mentioned that the main reason they engage in privacy management behaviour is to protect themselves from being a victim of a scam, blackmail, and identity theft. This idea of protecting oneself may be heavily attributed to the personal experiences that they faced as well as learned from the 'mistakes' of others. They have either personally experienced being scammed or know of someone who was scammed. A few of them were scammed by fake sellers who ran away with their money or engaged in delayed tactics, which the product never came. Quoting one of them:

"It was on Facebook. I asked them how much it was. They said it was RM650 per box (masks).

https://doi.org/10.15405/epms.2022.10.35
Corresponding Author: Wan, Puspa Melati
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

I could not remember how many were inside the box. Anyway, after I transferred the money to their bank. I kept the receipt. I asked them to take a snapshot of the package tracking number so that I can follow. However, they did not reply to me after one day. Then I realised that they blocked me so that I could not contact them. I reported this case to the police. The police could not help me. I just have to accept it. It was just a small matter." (Christina)

A few also received messages that they had won something or were selected to participate in an online game with a lucrative reward. These individuals were then asked to provide some crucial information to partake in this activity, such as their GrabPay details or to transfer a sum of money and the balance will be reimbursed later. Nina's experience is as shared below:

"My friend shared her experience with me. She told me her money was gone. I was shocked. She lost about RM800. She said something that through some vote, she would get money back. My friend gave her Grab account to that person. In order to allow that person to use the Grab app, a code would be required. She gave the code and realised she was cheated and lost her money." (Nina)

Another contributing factor found in this research was the role of significant others in providing the necessary advice to the respondents. Most of the Deaf youths said that they often turn to their siblings, spouse/partners, and friends whenever they are unsure of something - for example when they do not understand the wordings used in the terms and references, what information is safe to be included in the registration forms, or when they received suspicious messages.

7.3. Hindrance Factors to Engaging in Online Privacy Behaviour

The data shows that most respondents did not read the terms and references required before registering for certain applications. Some cited that they were lazy to do so as the terms and references were too long. As a result, most merely hit the next screen button and accept the terms. One of them even said that the companies should consider summarising the write up and keep them shorter so that it is easier for users to read and understand them. Another respondent said that he tends to get excited when he downloads any new application, and hence he is often in a rush. His friends would recommend applications that are considered "great," so he would just skip the terms and references – going straight into the app to evaluate them himself.

Though the above mentioned reasoning is not uncommon even among the hearing community and can even be linked to individual preferences, the following responses are important hindrance factors that should be understood so better protection can be curated to assist the Deaf community. One of the highlighted factors was language proficiency. Most of them confessed that they are not proficient in English language and/or the English used was too "complicated" for them. Below are some of their quotes:

https://doi.org/10.15405/epms.2022.10.35
Corresponding Author: Wan, Puspa Melati
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

"I do not read the terms and references because I do not understand English well. So, I simply skip
to hit the button to accept." (Rina)

"The English word is long, complicated and high for me. If the English were short and simple, I would be able to understand." (Candy)

"It would be good if I am good at English. I will be able to agree with their terms and references." (Chistle)

In addition to language proficiency, some also mentioned that their low literacy level also hinders them from engaging in online privacy management. Many are not exposed or trained in computer literacy as well as other academic training that would have indirectly enhanced their general knowledge and would help them manoeuvre in the virtual world. Instead, they possessed various hands-on vocational skills and wished they could have the opportunity to enhance further other skills that are seldom extended to the Deaf community. Some of their quotes are included below:

"What they offer is just vocational courses, but we never learn how to use the computer. It is because many of us are poorly educated. Many of us are illiterate. We are unable to understand English and also Malay. Vocational courses are all they offer, for example, hair cutting, makeup, repair things. Many of us know how to do these because we learned them. But we are poorly educated." (Fret)

"Yes, I want to learn how to protect myself. But how can I access the learning? I am not good at these yet. I wanted to learn more and more. What I learned is from my experience. So, I really want to know how I can protect ourselves while I am online to make sure my bank account and others are safe. I am very curious. The reason is that many Deaf are not well educated. Most of them do not know what "online" means. They only know what Facebook and Instagram are. iPad, Chat, Upload photos - these are common things they know about. They also know how to shop using Shopee and Lazada. But the fact is that they do not really know what is happening on the Internet. We do not have anyone who is an IT expert that can help to explain to us. It is happening to us. Many of us are not good at IT. I wish to learn more from hearing people. If they can, I want to learn. Deaf people could not help me because they have no IT knowledge. So, it would be good if hearing people can help us to understand the Internet." (Nina)

8. Conclusion

This research was conducted to learn the experiences and challenges faced by Deaf youths regarding online privacy management. The findings supported earlier literature where their cyber security has been compromised due to information sharing, lack of exposure, and digital literacy. This research findings also concur with Gross and Acquiti's (2005) work which found that though the respondents are

aware of the potential risk, most of them provide their personal information on various social networking platforms and applications. However, they try to limit their detailed information wherever possible (Snider et al., 2021).

In addition, this research shows that the Deaf do not take the issue of personal management lightly online, perhaps due to cases that they have personally experienced or learned through their acquaintances. Thus, they carry out some form of privacy management measures, but basic ones. This is due to their limited access and opportunities to understand further and learn how to protect themselves better. It is hoped that these research findings would raise the necessary concern and be taken into consideration for future strategic plans to educate the Deaf community on the workings of online platforms and provide training for more sophisticated ways of keeping them safe online.

Acknowledgments

This research is part of the Fundamental Research Grant entitled: Developing a framework that links online privacy literacy, privacy management behaviour typology, and managing strategies for Deaf youth (FRGS/1/2019/SS06/SEGI/02/1). We would also like to acknowledge other research members of this grant, namely Safuwan Samah (Public Service Department, Putrajaya), Siti Norbaya Daud (SEGi University, Selangor), and Sharifah Syahirah Syed Sheikh (Kolej Universiti Poly-Tech MARA (KUPTM), Kuala Lumpur) as well as Anthony Chong and Late Esther Wong who have helped substantially throughout the data collection process.

References

Ajibade, S. S. M., Ahmad, N. B., & Shamsuddin, S. M. (2018). A Study of Online and Face to Face Tutors and Learners'. *Innovations in Computing Technology and Applications (ICTA), 3*, 1-5.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26-53. https://onlinelibrary.wiley.com/doi/full/10.1111/jcom.12276

Bowker, N., & Tuffin, K. (2006). Dicing with Deception: People with Disabilities' Strategies for Managing Safety and Identity Online. *Journal of Computer-Mediated Communication, 8*(2). https://doi.org/10.1111/j.1083-6101.2003.tb00209.x

Choong, Y. Y., Theofanos, M. F., Renaud, K., & Prior, S. (2019). Passwords protect my stuff—a study of children's password practices. *Journal of Cybersecurity, 5*(1). https://doi.org/10.1093/cybsec/tyz015

Gross, R., & Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks (The Facebook Case). *ACM Workshop on Privacy in the Electronic Society*, Virginia. https://doi.org/10.1145/1102199.1102214

Kim, S., & Ko, I. (2018). How do multilevel privacy controls affect utility-privacy trade-offs when used in mobile applications? *Etri Journal, 40*(6). https://doi.org/10.4218/etrij.2017-0259

Lazzari, M., & Baroni, F. (2020). Remote teaching for deaf pupils during the Covid-19emergency. *14th International Conference on E-Learning 2020*. IADIS Press.

Maiorana-Basas, M., & Pagliaro, C. M. (2014). Technology use among adults who are Deaf and Hard of Hearing: A national survey. *Journal of Deaf Studies and Deaf Education 19*(3), 400–410. https://doi.org/10.1093/deafed/enu005

Malaysia Computer Emergency Response Team (MyCERT). (2021). *MyCERT Incident Statistics 2020.* https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=2650ed29-88be-4cec-86cc-13f8e07ae228

Malaysia Computer Emergency Response Team (MyCERT). (2022). *MyCERT Incident Statistics 2021.* https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=77be547e-7a17-444b-9698-8c267427936c

Malaysian Communications and Multimedia Commission (MCMC). (2018). Internet users survey 2018: Statistical brief number twenty-three. WP: *Malaysian Communications and Multimedia Commission*.

Mann, B. W. (2018). Rhetoric of Online Disability Activism: #CripTheVote and Civic Participation. *Communication, Culture and Critique, 11*(4), 604-621. https://doi.org/10.1093/ccc/tcy030

Meter, D. J., & Bauman, S. (2015). When sharing is a bad idea: The effected of online social network engagement and sharing passwords with friends on cyberbullying involvement. *CyberPsychology, Behaviour, and Social Networking, 18*(8), 437-42. https://doi.org/10.1089/cyber.2015.0081

Samuel-Soma M. Ajibade, Opeoluwa Adetola, Siti Mariyam Shamsuddin & Ruth Chweya. (2020). Social Communication of Students on Social Media Network Platform: A Statistical Analysis. *Journal of Science, Engineering*, *Technology and management, 2*(2), 11-20. https://doi.org/10.46820/JSETM.2020.1101

Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity, 7*(1). https://doi.org/10.1093/cybsec/tyab019

Sobers, R. (March 16, 2021). *134 Cybersecurity Statistics and Trends for 2021*. https://www.varonis.com/blog/cybersecurity-statistics/

Sponcil, M., & Gitimu, P. (2013). Use of social media by college students: Relationship to communication and self-concept. *Journal of Technology Research, 4*, 9-13. http://www.aabri.com/manuscripts/121214.pdf

Suler, J. R. (2004). The Online Disinhibition Effect. *CyberPsychology & Behaviour, 7*(3), 321-326. https://doi.org/10.1089/1094931041291295

Tuunainen, V. K., Pitkanen, O., & Hovi, M. (2009). Users' Awareness of Privacy on Online Social Networking Sites – Case Facebook. *BLED 2009 Proceedings. 42*. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1000&context=bled2009

University of Alabama Huntsville. (2019). *UAH Center for Cybersecurity and Education developing high school curriculum for students who are deaf*. https://www.newswise.com/articles/uah-center-for-cybersecurity-and-education-developing-high-school-curriculum-for-students-who-are-deaf

Van Gelder, L. (1991). The strange case of the electronic lover. In C. Dunlop & R. Kling (Eds.), Computerization and controversy: *Value conflicts and social choices* (2nd ed., pp. 364–375). Academic Press.

World Health Organization. (2020). *Deafness and Hearing Loss*. https://www.who.int/news-room/fact-sheets/detail/deafness-and-hearing-loss