LAB University of Applied Sciences

Awareness of social media privacy among the staff at Solo Sokos Hotel Lahden Seurahuone

LAB University of Applied Sciences
Bachelor of Business administration, Business Information Technology
Spring 2021
Yogesh Bhatt

Abstract

Author Bhatt, Yogesh	Publication type Bachelor's thesis	Completion year 2021
	Number of pages 40	

Title of the thesis

Awareness of social media privacy among the staff at Solo Sokos Hotel Lahden Seurahuone

Degree

Business Information Technology

Abstract

Social media has become a part of modern society and a major channel of communication and information sharing. The aim of this thesis is to know how well the staffs of Solo Sokos Hotel Lahden Seurahuone are aware of social media privacy and to provide an answer on how the awareness can be improved to stay secure on social media.

A web-form survey was done to collect primary data, and it was analyzed by thematic analysis method. The collected was compared to the literary sources.

The result of data analysis showed that the awareness of social media privacy is below average. Staffs were not aware of how their data is often used against them. Staff did not know about the available privacy settings provided by social media. A guide construction process was made, which directs the issues that were found on analysis to the solution that is mentioned on the knowledge base.

Keywords

Social media, concerns of social media privacy, employee awareness, privacy awareness, organization

Contents

Appendices

LIST OF TABLES

LIST OF IMAGES

LIST OF FIGURES

1 Introduction

1.1 Research Background

The development of social media started in the late 1990s. Some of the initial things social media asked its users were name and gender that was used to create a user profile. Currently, there are over 3.36 billion social media users (Tankovska 2021). Facebook, Instagram, Twitter, Pinterest, and LinkedIn are popular.

With such a large number of active users, these companies have collected data from each user. When social media accounts are being created, users must accept terms and conditions to use the service. Research done by ProPrivacy.com has found that only 1 percent of users read those terms and conditions. Even from that 1%, about 70% had lied, and 33% have claimed to have "read it thoroughly" (Sandle 2020).

Awareness of privacy is important so that people understand the importance of keeping personal information private and facing possible risks caused by violation of privacy. Experts of human rights are raising several privacy concerns. Social media platforms have trackers that keep an eye on users' patterns of surfing their website and collecting cookies saved by a browser, including information on other websites. Such collected data is often used against us, used in elections and advertisements. The main party who should be concerned about privacy and should care about it is users. Governments also should be concerned about their people's privacy.

1.2 Thesis Objective, Research Questions, and limitations

This section has three parts that explain the objective of this thesis, the research question, and the limitation of the thesis.

1.2.1 Objectives

The increasing privacy concerns are raising questions on users' trust in their service providers. On the surface, it might not be such a big problem with most people who are unaware of the effects of social media's acts on their data. Many people do not even know their information's worth that was provided to social media. When data is not being recorded safely, it can get into the wrong hands. These are the concerns when data is breached, but what happens when the company is trusted to do such acts. Bad things are not just any physical threat or a loss of personal information. It is found that companies have used or traded with advertisement companies. For example, Google does something called snooping and stalking. Google amasses data in user's web searches and even the routes used to take on Google Maps and what users do on devices signed into user's Google account. (Rodriguez 2018.)

The main objective of this thesis is to examine the awareness of social media privacy concerns among cleaners and housekeepers of Solo Sokos Hotel Lahden Seurahuone and help them create a guide that will help staff to improve their awareness of privacy on social media.

1.2.2 Research question

Research questions are the backbones for good research, which will help the author take examination properly without missing the track, and readers will understand the theme of the thesis.

In the thesis, the main research question is:

How well are the staffs aware of social media privacy, and how can they improve awareness with the help of the organization?

A survey of staff will be done to collect data. After analyzing collected data, it will help us to answer the research question, which will measure awareness about social media privacy concerns to staff. This survey will answer the first part of the research question. Based on this survey, groups will be formed to have members having the same level of awareness. A training plan based on a popular training framework will be provided to the organization, answering the second part of the research question.

To help answer the main research question, the thesis focuses on the following subordinate research question:

- Why do staff need to understand the privacy concerns of social media?

The primary purpose of these subordinate research questions is to examine the level of awareness of data privacy the staff at Solo Sokos Hotel Lahden Seurahuone has. Data collection is limited to cleaners and housekeepers; therefore, generalizing the results to other staff, professions, or organizations may not apply.

1.2.3 Limitations

Online privacy is a broad topic to discuss. It is not easy to cover every aspect and collect data related to every topic. To make it more specific and easier to collect data, the thesis will focus on people working as cleaners and housekeepers of the local hotel Solo Sokos Hotel Lahden Seurahuone in Lahti. The research data is collected from this specific group because such jobs do not directly relate to questions regarding social media privacy, and it is convenient for the author to collect data from them.

1.3 Theoretical framework

The theoretical framework of the thesis is discussed in three chapters, which will describe significant concepts directly related to privacy concerns of social media, employee awareness, and the importance of knowing social media privacy by the organization and its staff.

The first chapter of the theoretical part is concerned with the privacy concerns with social media. It explains the current privacy concerns raised by social media. The chapter also discusses related research.

The second chapter will discuss the benefits in the personal life of staff and organizations from awareness of privacy concerns of social media to staffs. A training model will be introduced, which can be used by an organization to conduct training to improve awareness among staff.

In the third chapter, Information that can help people stay secure and safe from social media privacy concerns will be presented. Such information is collected from the internet, and that is widely used and reliable as well.

1.4 Research methods and data collection

This step in the thesis gives an idea of which research method will be used. The research approach is a plan and procedure consisting of broad assumptions to detailed data collection methods, analysis, and interpretation (Chetty 2016). There are two types of research approaches, deductive reasoning and induction reasoning.

Deductive reasoning starts from observations to broader generalizations and theories. Deductive reasoning begins with a theory about our topic, then we narrow down the theory into more specific hypotheses that will be tested. We narrow it down even further when we collect observations to address the hypothesis. Finally, the hypotheses are tested with specific data. (Trochim 2020.)

For this research, deductive reasoning will be used. In this thesis's theoretical background, the author will recognize, collect, and familiarize training methods for a company to conduct an employee awareness program. And when data is collected and analyzed, it will be applied to the method described in the theoretical background.

Research approach	**Deductive**
Research Method	Qualitative
Data Collection	Primary source (Web-form survey).

Table 1. Research methods used in the thesis

In this step of the thesis, the research method is being decided. Additionally, it is also determined that how the data will be collected, recorded, and analyzed. There are two types of research. Those methods are the qualitative method and quantitative method.

Quantitative research is a process of collecting and analyzing numerical data. This approach is commonly used to understand patterns and medians, make predictions, test casual relationships, and generalize results to the broader population. The quantitative research approach is used in descriptive, correlational, or experimental research. (Bhandari 2021.)

Qualitative research includes collecting and analyzing non-numerical data, which can be used to understand concepts, opinions, or experiences. Qualitative research can help in examining people's experiences of the world. There are various data collection methods used under the qualitative research method. Bhandari (2020) adds that the commonly used methods are observations, interviews, focus groups, surveys, secondary research. The qualitative research method is suitable for this thesis because the aim is to understand the level of awareness among staff.

For this report, the data from staff whose work and education are not related and do not provide any information about social media privacy is collected. It is important to know the level of knowledge they have about social media privacy and ways to understand them from such staff. To collect the data, open-end questions for a web-form survey will be created to acquire the necessary information and their experiences with privacy concerns.

Regarding data, the theoretical part is based on secondary sources and data. In contrast, the empirical part is based on data collected from cleaners and housekeepers working at Solo Sokos Hotel Lahden Seurahuone. The primary purpose of the research question is to find out which working group is more aware of their online data. The working group will be decided according to in which position they are working.

1.5 Data analysis

Collected data should be analyzed to help answer research questions. This thesis uses qualitative research methods. The research data here is collected through a web-form survey. The collected data is then examined to identify common and repeated topics, ideas, and patterns. This thesis uses qualitative research, and there are several methods of analysis in it. The research data is being collected via a web form survey, and a thematic method will be used to analyze the collected data. The data is closely examined in the thematic method to find common topics, ideas, and patterns of meaning that come up repeatedly.

In this research, a common approach that follows a six-step process will be used. Those six steps are as follows: (Caulfield 2019.)

1. Familiarization
2. Coding
3. Creating themes
4. Reviewing themes
5. Defining and naming themes
6. Writing up

The first step is to familiarize with the data. This step might need to read through collected data and taking notes. The second step is called coding. In this step, keywords called "codes" are created to describe specific phrases or sentences. The researcher goes through every answer gathered on the survey and highlighted everything relevant or interesting. After gathering the coded passages, patterns are identified, and themes are generated. Several codes are being often combined into a single theme. This process is called generating themes.

After generating the themes, the themes need to be reviewed. This step helps make sure that the generated themes are useful and represent the data accurately. If any errors with themes are noticed, these are being solved by splitting, combing multiple themes, discarding them, or creating new ones. The fifth step is to define and name themes. Defining themes means formulating what each theme means and figuring out how it helps the reader to understand the data.

After the actual analysis, the final step is to report the analysis. This part includes introducing the research question, research aims, and research approach. The data collection method and the analysis process are also described. (Caulfield 2019.)

1.6 Thesis structure

The thesis contains seven chapters.

Section 1: This gives a background to the report. Additionally, this chapter explains the objective, research questions, and delimitations. This chapter also has a theoretical framework of the thesis and an outline of research methods and data collection used in this thesis.

Section 2: In this section, the theoretical framework is described. This section contains three chapters, and these chapters provide a theoretical background of the research. The first chapter of this section describes the major privacy concerns with social media. At the same time, the second chapter describes employee awareness. It explains the concepts and ways of organizing employee awareness. It describes the importance of understanding social media privacy by an organization and its employee too. In the third chapter, information to keep social media data secure and private is presented.

Section 3: This section of the thesis contains the empirical part of the research. It describes the research method and the data collection process done in this research. With that, this chapter presents the collected data and its analysis with thematic analysis.

Section 4: The last section concludes the thesis and contains the necessary information for an organization to create a guide for their employee during their awareness program.

Introduction	• **Background** • **Thesis Objective, Research Questions, and limitations** • **Theoretical framework** • **Thesis structure**
Theoretical part	• Privacy concerns with social media • Employee Awareness • Things to consider to stay safe from social media privacy concerns
Empirical study	• Data collection • Data analysis • Personal guide construction
Conclusion	• Training plan • Conclusion and summary

Table 2. Structure of this thesis

2 Privacy concerns with social media

2.1 Social media

In social media, “social” means interacting with other people by sharing information with them and receiving information from them. At the same time, the term "media" can be defined as the instrument used to establish communication between two parties. Nations (2021) describes social media as internet-based communication tools that enable people to interact with each other by sharing and consuming information.

2.2 Social media privacy issues

Online privacy, also known as internet or digital privacy, refers to how much of a person’s personal, financial, and browsing information stays private when you are on the web (Sushko 2020). Currently, nearly 45% of the world's population uses social networks, in the number that becomes 3.48 billion people using social media (Cooper 2020). And if users are not concerned enough, it can leave their data vulnerable in several ways. The result can be damaging when those personal data fall into the wrong hands. About 13% of Americans have had their social media accounts taken over by some unauthorized person (Smith 2017). Unauthorized access can steal information, make the followers redirect to malware, and make other accounts easy to get hacked. The typical social media threats are Data Mining, Phishing attempts, Malware sharing, and Botnet attacks. They are explained below.

Data mining is a process used by companies to turn raw data into something useful information. Companies use software to look for patterns in large batches of data from which a business can learn more about its customer to develop effective marketing strategies, advertisements, and more (Twin 2020). Social media companies do data mining from their customers' information to understand their internet behaviors and show exact ads from their partners. It has been noticed that companies sell user's data to third-party companies without the user's permission (Lee 2018).

Phishing is a common cyber-attack that criminals perform to gain access to sensitive information. There are various ways of performing this kind of attack; email, text message, or even a phone call is common. A criminal sends messages that look like a message from a legitimate organization. These messages trick recipients into sharing private information such as banking information, username, and password of any social media. Because many people and most do not know about such attacks, social media has become an easy platform for these attacks. (Fruhlinger 2020.)

Malware simply means malicious software. It is a blanket term for viruses, worms, trojans, and several other computer programs that hackers use to harm computer systems or gain sensitive information (Fruhlinger 2019). Social media are an easy route to share these kinds of attacks. If a hacker gains access to a victim's social media account, hackers can use that account to spread malware to the victim's friends and contacts.

A botnet is a collection of web-connected devices that a hacker has compromised. Botnet helps attackers to perform an attack on a victim from multiple systems that they do not own. The main advantage is that it can take advantage of its collective computing power to spread a large amount of spam, steal credentials, or spy on someone that can be any individual or organization. (Korolov 2019.)

These botnets need a way to get into someone's computer to make it a host without its owner's consent. Social media are an easy method for attackers to deploy these botnets. URL links are shared over social media, which are connected to botnets. These URLs are later clicked or opened by someone who does not know what that could be.

2.3 Social media privacy concerns

Social media are playing a more significant role in our lives. Its popularity indicates that social media are here to stay. Because of social media's popularity, privacy has never been more important. Not only helping to establish a connection between two individuals, but these networks can also have a major impact on the user's life as well.

A user does not need high technical knowledge to stay safe from various forms of risk that came out of social media networks. Even with a little bit of knowledge and caution, it is still possible to enjoy the good parts. Some major social media privacy concerns are Account hacking and impersonation, stalking and harassment, compelled to turn over passwords, location-based services, advertisement, and marketing.

Hacking is being a major headache for the privacy and security of data. Hackers, spammers, and other cybercriminals are targeting social media accounts more and more day by day. And the reliability we have on social media such as Facebook and Twitter, if criminals get access to these accounts, they can easily impersonate the user.

The main reason why criminal is behind social media accounts is its popularity and user's blind trust. It has been a more effective way to spread viruses, malware, and scams than any other traditional way, such as email. Every user of these media must fill in their personal information. Such accounts become a treasure of wealth of personal information, allowing attackers to open credit card accounts in the user's name or otherwise misuse abuse of such personal identity. Quick login is quite popular these days. Popular news sites like CNN.com and UK's Guardian newspaper, music streaming services, and other online retailers, apps, and games allow users to make quick login using Facebook, Twitter, or Google (Stokes 2017). So, these facilities or options enable a hacker to access other user accounts via a single social media account.

According to Gordon (2021), The crime of harassment by stalking and hate crime occurs when one acts to make people annoyed, provoke, threaten, or otherwise cause another person's emotional distress. And when such acts are done by using any internet means, it is explicitly called cyberbullying. Online stalking and cyberbullying have become very popular and well-known threats nowadays, and social media have made it easy for criminals to perform such crimes. Compared to traditional bullying, the effects of cyberbullying are often more harmful and effective. Cyberbullying has allowed bullying to stay forever. Hurtful messages, words, and images are often preserved online. Even if someone deletes such bully materials, there is very much a chance to keep it with someone in the form of a screenshot or shared text message (Gordon 2021).

There are several situations where an individual may be asked to reveal a password to a person's social media account. Such activity is often happening with a new employee of an organization. In the name of ensuring an employee is not revealing any confidential information or any trade secrets, employers ask for access to their employee's social media account. And such trend is increasing. People keep adding their personal information on social media, and its pace is increasing day by day. When employers have access to their employee’s social media accounts, the risk of abuses and privacy could increase. (Miller 2015.)

People are more active on social media from their smartphones rather than computers and laptops. Many services require a user to allow an app to acquire the location of the device. When location information is collected by phone or application, several data-gathering companies collect geolocation information about users, which they sell to advertisers (Bridges 2019.). Ads are not the only place where such collected information can be used. Thieves and stalkers can use such location information collected on social media to perform their dirty activities. For example, a thief can loot someone's house if he/she knows that the house owner is out because he/she posted some traveling post or do any check-in anywhere far from home.

Companies can track and sneak at our browsing history and other online activities and understand users' purchasing habits. When a user searches something on search engines or mentions something on email, suddenly that person starts seeing ads related to searched or emailed entity. Facebook is renowned for serving ads about pregnancy and baby equipment to the newly married. (Siegel 2014.)

3 Employee awareness

In general, awareness means knowledge or perception of a situation or fact. Employers can make their workers aware of the things happening around them that might affect the organization and staff. Privacy awareness programs are more effective for new hires. They generally want to make a good initial impression and are more positive, attentive, and more easily influenced (Bilger 2014).

An external factor causes the risk with privacy, but studies also show that about 90% of data breaches are caused by human error. Phishing is a popular technique designed to deploy a low level of user privacy and data security awareness. A phishing attack caused about a third of total data breaches in 2019. (Deeney 2020.)

3.1 Benefit in Employee's personal life

When an organization conducts awareness programs, it does not only help the organization but can also make changes in an employee's personal life. When a company makes their staff learn and understand something, it is more likely that staff will have to learn and understand. There are several benefits to an employee's personal life: prevent identity theft, avoid being robbed, protect employability, and protect freedom of thought (Bridges 2021).

The common definition of social media is focused on sharing information, and if such information is personal and publicly exposed, users get affected by identity theft. Social media users are 30% more likely to be affected by identity theft than those who do not use it. Users of common social media such as Facebook, Instagram, and Snapchat are at 47% higher risk of identity theft. (Myhre 2021.)

If an employee follows these guidelines, they may secure themselves from getting robbed. When thief knows that you are not home, they may get into your home take your belongings. One easy way to find out if you are home or not would be your social media if you posted your vacation plan on social media (Bridges 2021).

Sometimes an employee may get at risk of losing the job because of their activities over social media. Employers may be keeping their eyes on their staff. Sometimes an employee may post something unprofessional, discussing politics and religion or complaining about his current job over social media. According to a Harris Poll survey, about 70% of employers utilize social media to screen candidates before hiring (Driver 2019), whereas they might keep an eye on their current employers.

Freedom of thought and speech is a fundamental right, but due to social media, people can lose it. Many popular politicians and other personalities are banned on Facebook and Twitter for their thought on the subject. When a user thinks of buying something, you are being tracked by some scripts or cookies so that social media could show ads to make money out of you. Privacy awareness programs can help staffs how to stay untracked and keep personal thoughts private on social media.

3.2 Benefits to Organizations

In this part, we discuss the multiple advantages of conducting a social media privacy awareness program.

An organization can promote good privacy practices at work: proper disposal of credit card applications and personal information. It will teach to securely transfer information and denying access to the organization's data to unauthorized personnel. (Wlosinski 2019.)

Criminals adopt new ways to use social media as a medium of performing criminal activities and violating privacy. Awareness programs provide a starting point for the ongoing improvement of awareness and practices against evolving threats. These programs also help to educate newly hired staff about security and privacy threats related to social media. Social media are convenient for sharing information. It might be dangerous if any sensitive data is posted on social media such as Facebook, Instagram, or Twitter. (Wlosinski 2019.)

Awareness can explain how an organization can enforce protective controls against the threat from malicious acts over social media and negligence via processes, procedures, and technology. Highlights the risk which poor social media usage behaviors can cause. It discourages these bad behaviors. By teaching staff to protect their work, the organization prevents malicious behavior such as publishing company secrets. (Deeney 2020.)

3.3 ADDIE training model

The ADDIE model is an instructional design methodology used to help, organize, and streamline course content production. This model was developed in the 1970s; ADDIE is the most used model for designing a training program. (Quigley 2019.)

ADDIE is a five-step training model, and it is named after five different stages included in creating training. These are Analysis, Design, Development, Implementation, and evaluation.

a) Analysis

In this first phase of the training model, an analysis of different aspects of training such as training receivers, the context of training, place of training, and objective of the training is done. Among all these, knowing trainees' knowledge and establishing the aim of the training is most important. (Apostolopoulos 2018.)

b) Design

In the design part of the model, a course is created, which fills the gaps. While creating content, the format of the course is decided. The course can be a simulation, a simple quiz, a video-based course, or paper-based courses. In this stage, the methodology and the strategy are also decided. Where time and order of to feature each section is conformed. (Apostolopoulos 2018.)

c) Development

This stage is to develop an actual course content of training which was decided in the design phase. The development phase will need a lot of testing. Testing will check with grammatical mistakes, syntax, or spelling errors, etc. (Quigley 2019.)

d) Implementation

Once everything is ready, it is time to share the course with learners. This step is mostly based on the design phase. An effective LMS (Learning Management system) software can be used to implement a course of printed or softcopy-based content.

e) Evaluation

The final step in the ADDIE model is to evaluate the learners. Evaluation can be done through the LMS, conducting interviews, or surveying learners. Based on feedback, it is possible to evaluate if the goals or objectives that were introduced in the analysis phase are achieved or not. It depends on the trainer if they want to reconduct training or result can be satisfying.

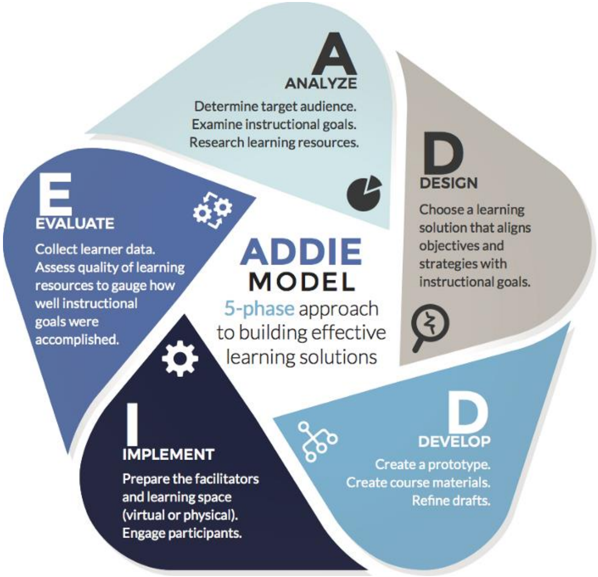
A
ANALYZE
Determine target audience.
Examine instructional goals.
Research learning resources.
D
DESIGN
Choose a learning solution that aligns objectives and strategies with instructional goals.
D
DEVELOP
Create a prototype.
Create course materials.
Refine drafts.
I
IMPLEMENT
Prepare the facilitators and learning space (virtual or physical).
Engage participants.
E
EVALUATE
Collect learner data.
Assess quality of learning resources to gauge how well instructional goals were accomplished.
ADDIE
MODEL
5-phase approach to building effective learning solutions

Figure 1. ADDIE model (Mejia 2018)

4 Social media privacy concerns

There are several things to keep in mind to stay safe on social media. While we are talking about social media, the first step toward secure privacy should start from social media itself. Sometimes user's personal information can get into the wrong hands because of the user. The reason is carelessness and not being familiar with privacy settings too. First, we will start with basic settings and notes to keep in mind.

4.1 Measures to secure social media account

Here are some basic easy-to-go tips and settings that can help stay secure over social media with no technical education.

4.1.1 Tips to consider while creating a new social media account

Staying secure starts from creating social media account Here are some tips to consider while creating a new account. (Privacy Rights Clearinghouse 2019.)

- Use a unique and strong password.
- Try to use a new or different email address to only use with social media.
- Provide the least amount of personal information and which is necessary only.
- If you are asked to set a security question, use a false or irrelevant question and a false answer to that question and save such question and answer in your note or password manager.
- Get familiar with terms and conditions and privacy policies.

4.1.2 Privacy settings

All major social media sites like Facebook, Twitter, and Instagram offer privacy protection. Users can customize accordingly. Here is a step-by-step setup guide to a secure setting for the top 3 social media. (O'Connell 2018.)

1. Facebook

   Facebook provides an easy guide to check and make the account more secure from its tool called “Privacy checkup.” To access it

   Log onto Facebook and click on "Settings.", then select "Settings & Privacy," then click Privacy checkup and make necessary changes.

2. Twitter

   To update the privacy setting on Twitter, log on and click on “Settings and privacy” in the menu below the profile picture in the top navigation bar. We can make several changes such as (O'Connell 2018.)

   - In the main “Account” setting, we can review the login method (Setup two-factor authentication), user can change the password and request a Twitter archive.
   - In “Privacy and safety settings,” users can change tweets' visibility if a user wants to keep them public or private.
   - In the “Password” section, the user can change the password of an account.
   - In Twitter “Apps” section, users can revoke access to the apps connected to Twitter.

3. Instagram

   Instagram is also another popular social media which Facebook owns. In the Instagram app, log in and go to profile. Then click the gear in the top right, where the user can make the following changes. (O'Connell 2018.)

   - Adjust settings for a user photo: Here, the user can review the pictures that friends tag before showing up on the profile.
   - Adjust Story settings: The user can hide Instagram stories from specific people and other story-related settings.
   - Edit profile or change password.
   - Set up two-factor authentication to protect others from logging into an account even they have a password.
   - Make account private: this means new people will have to request the user to follow and see Instagram photos and stories.

4.1.3 After use of social media

The effects of social media will follow its user even when they are not using social media. After use of social media or while not using it, follow these tips.

- Log off from social. It will keep the user's account and profile safe if someone gets access to the user's device. So, it better to stay logged out while not using it.

- Clear cookies and cache. Websites and applications use cookies and cache to run faster and smoothly by storing frequently used data and information. They stay on memory even after the user logs off the account, and it could be a target for data mining companies and hackers and may expose some valuable information. So, when a user has logged out, it is better to clear cookies and cache data from devices and browsers.

4.1.4 Other advice related to social media

Even after setting privacy settings and other measures, there could be a risk until a human is using. Here are some additional tips which could not make other groups.

- Multi-factor authentication is a relatively simple yet strong way to keep online accounts secure. Multi-factor authentication aims to add a layered defense that makes it more difficult for an unauthorized person to access a target, making it more difficult for an unauthorized person to access a target(account). There are different methods of use, but OTP (one-time-password) is a popular one. All social media have implemented multi-factor authentication. Multi-factor authentication sends OTP, an extra password that the system generates even after the user logins to the account with a user-defined password. OTP is sent to the registered email or phone number. To get access user must put that code. (Shacklett 2021.)

- Be aware when using third-party applications. It is always good to avoid them, but if users want to use them, review the privacy policy and terms of use. It will not harm to account, but when the user approves connection between the third-party application and social media account, asked information is shared. If it has bad intentions, the user's information might get exposed. Third-party apps can install malware on a device and cause network threats that are good enough to violate privacy. (Agarwal 2018.)

- Social media is a place to make friends, but accepting a connection request from a stranger might get users into trouble. The safest way is to reject the request, but a limit should be imposed to access personal information if the user accepts the request. Accepting a stranger's request on social media may result in being a victim of stalking or harassment.

4.2 Additional settings and advice

Sometimes it is hard for users to choose between privacy and convenience. There are several functions that social media and other apps and services use to make the user experience better, for example, collecting cookies, but on the other hand, such collected data can be used to show targeted ads or to trade the information. Here are such services that are recommended to turn off or block.

a) Block Geo-tracking

Geo-location was developed to use in maps and navigation, but recently, it has been a privacy concern. By enabling geo-location may reveal personal information as well. Geo tracking can reveal personal information such as the route user takes to work or the gym and home location. When a user goes on vacation, it records the place of stay, income level (Based on where the user lives), what does a user does for a living (Based on work location). There is no rethinking of what such information can do if it gets into the wrong hands.

We can block geolocation services on our computers and mobile phone. To turn off location services on pc, just search "Location" on the start menu. It takes directly to the location setting, where we can change it to off. Still, websites get the location of a user from the IP address of a network. For that, we can use VPN.

Not only from technical revealing but human activities also reveal location on social media. It is fun to post the visit, but not everyone needs to know they visit. Sharing such information can make users and user's homes vulnerable. Such information will let the public know that the user is far from home, making it available for break-ins. (Bridges 2019.)

b) Block cookies and clear cache

Even though cache and cookies enhance user experience, they collect information, so it is good to clear and block cookies and cache data from personal devices. It prevents user's data from getting into the wrong hands. Clearing and blocking cookies and cache does not affect the device; when required, the device automatically downloads from the server. Users must clear it frequently as it again gets stored when the device downloads. To clear unnecessary data, we can use several tools such as CCleaner. It is available for both phones and pc for any operating system.

c) Do not track requests

Prevention is better than cure. Nowadays, web browsers allow users to request services, not to track. It is a setting that requests that web applications disable their tracking of an individual user. When a user turns on DNT in a browser, the browser sends a signal to websites, analytics, ad networks, plug-in providers, and other web services that the user encounters while browsing to stop tracking user activity.

To enable it, a user must go to browser settings > privacy and security > cookies and other site data and turn on "send. "Do not track" requests with your traffic." (Kellet 2021.)

The same kind of DNT system is recently added to iOS devices. When allowing permissions to apps, iOS asks to track users or send, do not track request, choose to "Send, do not track request" there. This kind of service is yet to come to android devices.

d) Phishing

Phishing is a way to harvest user's data such as passwords, credit card numbers, and many more by impersonating oneself as a trustworthy entity. There are various ways to find phishing emails, SMS, or links. For example, Figure 2 looks like an Instagram login page, but it is not. To find out user can see the URL of that page which is not from Instagram. The Instagram URL starts with "Instagram.com," but it is something else in this figure.

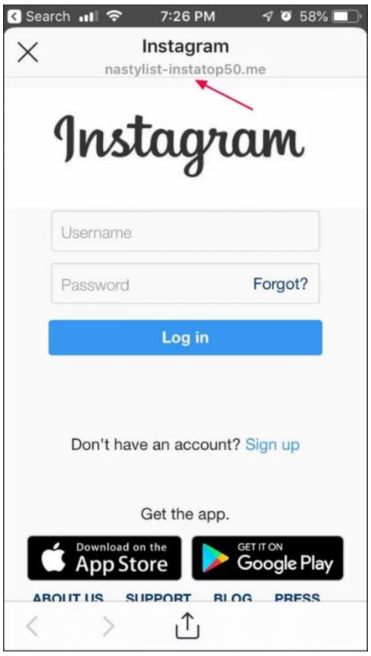

Image 1. Phishing Instagram page (Guan 2019)

Phishing can be in the form of emails and SMS as well. An easy way of noticing them is by checking the sender's address or phone number in case of SMS. It is not recommended that the user follow links from emails or SMS or send personal data without becoming sure if a person on the other side is trustworthy and authentic (Gillis 2020).

5 Data collection

The following figure shows the timetable of the thesis data collection and analysis timeline.

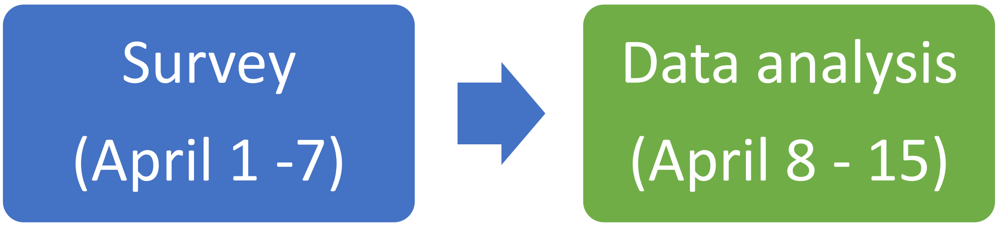

Figure 2.Data collection timetable

The primary data was collected through a web form survey. The situation created by COVID-19 had made it challenging to conduct other primary data collection methods such as interviews, so survey the web-form survey was done, which eliminated the in-person contact with participants. In the survey, 11 individuals have participated. There are six open-end questions where participants would answer the question with their views and activities. The order of questions was based on flow. 1st question would start from very basic, and it kept connecting to the next question in a simple flow.

1	According to you, what kinds of information can be shared on social media?
2	In General, what do you know about Social media privacy concerns?
3	In simple words, what kinds of activity on social media may risk your personal/organization's private information?
4	What measures have you taken to keep your information private on social media?
5	What consequence could be caused by unresponsible activity done in social media?
6	What do you know about trackers and cookies that social media websites and apps use?
7	Which tools or methods can help you to prevent websites from tracking your activity?

Table 3. Lists of survey questions.

Table 3 lists the survey questions. The motivation for each question is explained here in detail.

Question number 1 tries to understand the basic understanding of sharable content over social media. Sometimes users do not know the importance of the information they are sharing over. For example, a student gets a visa to study abroad, and in a hurry, S/he posts the decision to make show off on Facebook. Still, such a document includes personal information such as passport number and social security number.

Whereas question 2 helps to an understanding about privacy concerns that a particular individual knows. People might be suffering or may be causing a problem to other people on social media unknowingly. Such acts might be punishable by law as well.

3rd question is essential because it helps to understand if a person does or does not know about activities that might risk personal or organizations' private information. Question number 4 helps to see the kind of security activities participants practice to keep themselves safe from social media privacy concerns.

Question number 5 is used to understand if participants know about consequences caused by harmful activities over social media. Where question number 6 takes the participant's technical knowledge into account. The last question is also related to technical aspects and tries to know if participants have been using any tools to stay secure. Names of tools and methods are expected from participants.

6 Data analysis

The purpose of the data analysis is to find answers to the research question. Thus, the purpose of the survey was to find out how aware staff are of social media's privacy concerns and how they have coped with social media privacy concerns. As per the report's plan, the collected qualitative data from the survey is analyzed in thematic analysis. The analysis will go through several steps to finally generate a group of similar ideas. The analysis starts with the first step of familiarization.

6.1 Familiarization

Familiarization helps to get to know the collected data. While presenting the data in this step, main points will also be highlighted to create a common code in the following analysis step. The following is the presentation of the collected answer to each question. Answer in each row of the table is a response of a different responder.

a) According to you, what kinds of information can be shared on social media?

Name, country, gender, age
Fun activities, information,
personal information, educational information
Things with real content
News
That information can improve you and your friends.
social awareness
Health awareness
Awareness and motivational things.
Any kind of
Informative information which can be useful to everyone

b) In General, what do you know about Social media privacy concerns?

In my opinion, there are many privacy concerns we should know about, like data mining, malware sharing, Phishing, etc.
Little I know, a hacker can fetch your data from social media
Always chance of leaking personal information.
Don't know
Privacy about the personal information
No nothing
it's about keeping personal or organizational data or information's safely
The subset of data privacy
Somehow
Nothing
We can't blindly trust social media platform; therefore, it is necessary to make your security strong on social media and update your privacy setting from time to time

c) In simple words, what kinds of activity on social media may risk your personal/organization's private information?

Spam mail or text, exploring phishing websites.
Going through an unknown link
Visiting unsecured site
Don't know
Adding unnecessary app &games
Criminal activities
weak password
When it posted on social media, it may end up falling in the wrong hand
Password hacking
Illegal
Sharing our location every time and as well sharing our passwords with multiple people can have risk on social media

d) What measures have you taken to keep your information private on social media?

No
Yeah, I have taken like two ways authentication.
VPN
I have changed my personal information setting to only me. So, that other has no longer access to it.
Till not
Well, I have private my information in settings
Yes, I have applied a two-factor Authentication system and connected my social media account with my registered mobile and email account to get notified if any unusual things occur

e) What consequence could be caused by unresponsible activity done in social media?

Data leak and account hacking
Waste of time
Hack
We might get into legal problems.
I do not know what. (4 similar response)
Interfere with work
People may know our private information
Our account might get hacked; our personal information could be exposed

f) What do you know about trackers and cookies that social media websites and apps use?

No (9 response with an exact word)
Trackers and cookies help in better web surfing.
No, I do not know
No, I do not have any idea about this

g) Which tools or methods can help you to prevent websites from tracking your activity?

No (9 responses with an exact word)
I used to block the third-party cookies in chrome
Well, you can add your mobile number to track your activities.
Yes, we can disable our GPS location, and better not to open any unusual link if it seems suspicious to any extent.

6.2 Coding

All the highlighted text is copied down in this step, and a code representing the actual data is assigned.

Survey extract	Codes
Any kind of, No, I do not have any idea about this, Nothing, till not, do not know.	Uncertainty
Personal information, Trackers help in better web surfing.	Misinformation
Privacy about personal information. It is about keeping personal or organizational data or information safely, a Subset of data privacy, Adding unnecessary apps &games, Illegal activities.	Misunderstanding of question.
We can't blindly trust social media platform; therefore, it is necessary to make your security strong on social media and update your privacy setting from time to time; going through unknown link, weak password, I used to block the third-party cookies in chrome; well, you can add your mobile number to track your activities. VPN	Acknowledgment of risk
Like data mining, malware sharing, Phishing, leaking personal information, exploring phishing links got via social media, when it posted in social media, it may end up falling in the wrong hand, sharing our personal social media passwords shared with multiple people, two ways authentication, personal information setting to only me, our account might get hacked, our personal information could be exposed, People may know our private information, We might get into legal problems, data leak	Correct information.

Table 4. Coding survey data

6.3 Creating themes

In this part, the common theme is created for codes that have a similar pattern. In this analysis, the collected idea was straightforward and more like common practices that most people would do, even if that is current or wrong. Five codes are being created from the collected information, and here these codes will be assigned to a specific theme.

Codes	Theme
Uncertainty Misinformation	Lack of basic information.
Acknowledgment of risk Misunderstanding of question	Unclear
Correct information	Aware

Table 5. Generating themes

6.4 Reviewing themes

In this reviewing part, generated themes are checked with the actual survey extract. It is important to make sure that themes are a useful and accurate representation of the data.

Theme	Survey extract data
Lack of basic information	any kind of, No, I do not have any idea about this, Nothing, till not, do not know. Personal information, VPN, Trackers help in better web surfing.
Unclear	Privacy about personal information. It is about keeping personal or organizational data or information safely, Sub-set of data privacy, Adding unnecessary apps &games, Illegal activities. We cannot blindly trust social media platform; therefore, it is necessary to make your security strong on social media and update your privacy setting from time to time, going through unknown link, weak password, I used to block the third-party cookies in

	chrome, you can add your mobile number to track your activities.
Aware	Like data mining, malware sharing, Phishing, leaking personal information, exploring phishing links got via social media, when it posted in social media, it may end up falling in the wrong hand, sharing our personal social media passwords shared with multiple people, two ways authentication, personal information setting to only me, our account might get hacked, our confidential information could be exposed, People may know our private information, we might get into legal problems, data leak

Table 6. Checking accuracy of themes with actual data

While cross-checking the themes and the extract data from the survey, it is confirmed that each theme is representing the correct data. The themes represent data, but it is enough to understand why those themes are assigned to that specific data. Overall, it is hard to understand the meaning of the theme. So, themes are defined in the next step.

6.5 Defining and naming themes

It is time to define the themes. Defining themes means formulating what each theme means in this analysis and figuring out how it helps understand the data.

Theme	Definition of the theme.
Lack of basic information	In this analysis, lack of information means not having proper awareness about the risks of privacy concerns of social media or prevention methods for privacy concerns of social media. With It, some answers have no connection with the question, i.e., wrong answer. There is no specific authority that could define whether it is right or wrong. So, it is assumed that the wrong answer was caused by a lack of basic information about social media privacy concerns.
Unclear	This theme represents such data, which is incomplete and not properly clear. Such vague and unclear answers could have been clearly explained. Information could not help to know whether participants can understand social media privacy concerns totally and their knowledge to use tools and methods to prevent issues caused by privacy concerns.
Aware	In this analysis aware means having proper awareness of social media privacy concerns and related aspects. The answer is clear, and the answer provider knows what it means.

Table 7. Defining the themes

6.6 Writing up

The result of the analysis is presented in this section. This section will have four subsections. Those subsections will help understand the aims and approach of the research, the methodology used to collect the data, and how thematic analysis was conducted. Finally, the result explains the findings, and the conclusion will explain the takeaways and answer the research question.

a) Introduction

This research aimed to measure the awareness of privacy concerns of social media among the staff of a hotel who are working as cleaners and housekeepers. The research question focused on understanding how aware these staffs are, who had no direct connection regarding social media privacy.

b) Methodology

Data was collected through a web form survey. Because of the Covid-19 situation, the author couldn't have face-to-face interaction to have interviews. The questions in the survey were open-ended. These types of questions allow participants to answer more detailed explanations.

The whole process of the thematic approach is done in this thesis. Thematic analysis is often done in physical form, so it was tricky to analyze soft copy form. Throughout the analysis process, several answers could not make through Familiarization. Such responses were mainly irrelevant to the asked questions, whereas some answers were common. For example, even questions were open-ended, participants just answered "No."

Codes and themes were generated to explain the relevancy of the answer with the question and the research concept rather than giving synonyms meaning.

c) Results

The result of the research is quite unexpected for the author. As a simple hypothesis, it was expected that participants would have a fair knowledge of the privacy concerns of social media. Even though the collected data was qualitative, if we compare the amount of information in themes other than "*aware,*" it is significantly more. Where theme "aware" was supporting the hypothesis

Lack of basic information has often come up in data. Most participants do not have any acknowledgment of risks that can cause harm.

Similarly, we can see participant's "*unclear"* understanding of many terms. For example, *"Sub-set of data privacy, Adding unnecessary app &games, Illegal activities."* These answers hint that participants know what they meant, but they do not have enough understanding terms that they want to answer.

Meanwhile, the theme "*Aware*" represents the understanding and awareness of social media privacy concerns among participants. The collected data lacks this insignificant theme amount. This theme shows that participants have little knowledge and awareness of the risks that privacy concerns can cause. Still, in terms of prevention, participants lack a good amount of knowledge and information.

d) Conclusion

This research shows the awareness of privacy concerns among working staff is low. Participants might have known about some terms of privacy through some sources, but overall, everyone needs more training to improve their awareness. As the data was collected and analyzed in qualitative, it can not specify to someone individually that their understanding is low or vice-versa. But when we talk about the data overall, everyone needs more knowledge to improve their awareness. Here are some common problems found on staffs' awareness: -

1) They do not know about available privacy settings on social media websites.

2) They do not know how their personal information is tracked and used against them.

3) They do not know enough about data-stealing attacks like Phishing, malware, and botnet attacks.

4) They do not know about the possible drawbacks of services that were developed for good.

5) Lack of enough technical and non-technical knowledge to prevent an individual from social media privacy concerns among staff.

By this point, research focused on the staff of an organization. The importance of staff being aware of social media's privacy concerns is well explained in the theoretical part. So, we can say that organizations can play an essential role in making their staff aware of the privacy concerns of social media. A practical training framework is introduced in the theoretical chapter. An effective training plan can be formed, answering the second part of the research question related to the organization's help to staff to improve awareness.

Detailed answers to the research question and subordinate questions are given in the conclusion and summary of the thesis.

7 Creating a social media privacy guide

To increase awareness among staff, it is necessary to teach the staff about social media privacy concerns and possible solutions. The data analysis found five critical issues. These problems can lead an employee to privacy concerns that social media have increased. A guide should consist of answers to existing problems and possible future problems.

Here the answer to the problem found by data analysis is presented.

Problem 1: - They do not know about available privacy settings on social media websites. Here “they” represent the participants of a survey done in this report. It is found that some of the participants do not know that every social media allows their user to keep their data private through settings that users can easily change. The user does not need any technical knowledge to make such changes. Users need to know about such privacy-related settings because by doing this, they can limit access to their friends or other users from their such personal information that they do not want to share.

Problem 2: - They do not know how their personal information is tracked and used against them. Participants have no idea about how they are being followed and used against them. This can be tricky because there is no label on the information presented to the user other than ads. Users should try to block trackers as they can be harmful to privacy. There are several tools and extensions freely found on the internet.

Problem 3: - They do not know enough about data-stealing attacks like Phishing, malware, and botnet attacks. Many people are suffered from phishing attacks. Phishing is an easy way to harvest someone’s private information, such as passwords and credit card numbers. To find that participants of the survey do not know about phishing was shocking. Malware and botnet are often hidden and hard to find. These get into devices through some applications that the user downloads from the internet. A survey should include information about how such attacks can be blocked.

Problem 4: - They do not know about the possible drawbacks of services that were developed for good. Here we are talking about services such as cookies and caches. This is more like a technical term. Cookies and caches store personal information on the web browser. These kinds of memory make the task easy for data miners. It is essential to clear such cookies and cache, and if possible, it is good to block.

Problem 5: - Lack of enough technical and non-technical knowledge to prevent individuals from social media privacy concerns among staff. Technical knowledge represents information about several apps and tools which are easy to use and freely available on the internet. Meanwhile, non-technical means information about several developments, such as a multi-factor authentication system that create an extra layer to the security and privacy of an individual's online avatar. Many users openly share their location over social media, in the usual case, it might be fun, but if a criminal finds out such information, it may lead to problems. It is crucial to let users know about the possible trouble caused by simple mistakes over social media.

This report was focused on a particular organization, but the above-explained issue can be considered common. Even if this report focuses on one organization, other organizations can still organize similar research as it is done in this thesis.

To improve the awareness of staff, an organization can organize training. Such a training program should include all the problems their staff face due to social media privacy concerns. ADDIE model can be used to manage an effective training program. In the next chapter, an instructional plan based on the ADDIE model is presented.

Creating and implementing guide with the help of ADDIE model.

An organization can help staff to improve awareness by organizing training based on the ADDIE training model. The following training plan is constructed based on collected data.

- Analysis

  An organization must analyze its staff, place of training, and objective of training. This thesis examined staffs and found out that almost all staffs need training of the same level. The exercise aims to improve the awareness of privacy concerns of social media. A company can book a meeting room with the capacity of 11 people and a coach to conduct the program.

- Design

  The next step is to design a course and its format. It is noticed that the understanding label of hotel staff is basic, so an easy-to-understand guide needs to be created as report analysis has found about five significant problems that need to be solved. So, a guide mainly focused on those questions needs to be constructed in this stage of the ADDIE model. A coach can form a PowerPoint presentation based on a guide to present and explain the guide itself. A coach should be from a related field of online privacy, who can make clear explanations without any mistakes.

- Development

Guide creators should check grammatical mistakes, syntax, and spelling errors in the guide as data analysis found that the understanding label of staff is basic. Using too many technical words might make them confused. In this step of constructing the guide, it is necessary to make sure that basic and easy-to-understand words and terms are used.

- Implementation

  It is time to call all the participants to a decided place of training. A printed copy can be provided to participants, and a coach will start presenting and explaining. At the same time, participants can read the guide as well for a deeper explanation. With a bit of break, the program can be finished within 30 minutes.

- Evaluation

  After training is finished, the evaluation of participants is done. For evaluation, a survey can be conducted to check whether the training was successful or not. The same survey questions which were created for data collection published in Appendix 1 can be used. Based on feedback, it is possible to evaluate if the goals and objectives of the training were achieved or not. A trainer can conduct training again if they feel that it is necessary.

8 Conclusion and summary

The research was done to determine social media's privacy concerns among staff working as cleaners and housekeepers of Solo Sokos Hotel Lahden Seurahuone. The main aim of this thesis was to find out the awareness level of privacy concerns of social media among staff.

Privacy concerns are increasing. Threats are not coming only from strangers but from our beloved and trusted companies as well in the name of personalized services. And still, such personalized ads do not help users. Users know what they need, and they search for it. It may be challenging to come out of personalized services, but we will be keeping our personal information to ourselves. It is not a problem to share information within the limit, but when such little information gets into the wrong hands, it can cause chaos.

Privacy concerns of social media are popular these days. However, from a survey, we learned that still many people are not aware of privacy concerns, and it is apparent that users do not see any prevention methods. Effective programs from the government and users themselves should show interest in keeping information private and stay safe.

8.1 Answers to research questions

The research questions will be answered to determine the level of awareness and how it can be improved.

Research question:

How well are the staffs aware of social media privacy, and how can they improve awareness with the help of the organization?

From the collected data and its analysis, we can say that awareness among staff was between poor and moderate. It was found that some of the staff do not have any idea about the asked question, and some of them had little information, but they had no idea of how to make their information safe on social media. From the data analysis, we can say that the staffs' awareness level was poor, and a guide was necessary to improve it.

For the second part of the question, an organization can conduct a training program that can help improve the awareness among staff. An effective training plan and guide are provided in a thesis that can make it easier for an organization.

Why do staff need to understand the privacy concerns of social media?

Staffs are not just members of an organization but part of society as well. Their knowledge and awareness affect a particular organization and many people near them as well. They can change and spread awareness within the community as well.

8.2 Recommendation for further study

Online privacy is a broad subject. In this thesis author just tried to cover the privacy concerns of social media. For further researcher, it is recommended to try to cover other aspects of online privacy such as tracking over the internet, spying and snooping, information mishandling, data harvesting. People need to know the back draws of the internet and its usage, and its effect on privacy.

References

Agarwal, H. 2018. The Hidden Dangers of Using Third Party Apps. appknox. Retrieved on May 10, 2021. Available at https://www.appknox.com/blog/the-hidden-dangers-of-using-a-third-party-mobile-app

Apostolopoulos, A. 2018. ADDIE Training Model: What Is It and How Can You Use It?. Talentlms Retrieved on March 10, 2021. Available at https://www.talentlms.com/blog/addie-training-model-definition-stages/

Bhandari, P. 2020. An introduction to qualitative research. Scribbr. Retrieved on February 8, 2021. Available at https://www.scribbr.com/methodology/qualitative-research/

Bhandari, P. 2021. An introduction to quantitative research. Scribbr. Retrieved on February 8, 2021. Available at https://www.scribbr.com/methodology/quantitative-research/

Bilger, K. 2014. Raising Awareness in Your Organization. Ohsonline. Retrieved on March 12, 2021. Available at ohsonline: https://ohsonline.com/Articles/2014/10/01/Raising-Awareness-in-Your-Organization.aspx

Bridges, J. 2019. Why geotracking is a growing threat to online privacy. Reputation Defender. Retrieved on March 15, 2021. Available at https://www.reputationdefender.com/blog/privacy/why-geotracking-is-a-growing-threat-to-online-privacy

Bridges, J. 2021. Top 10 reasons to keep your personal information private. Retrieved on March 15, 2021. Available at https://www.reputationdefender.com/blog/privacy/top-ten-reasons-keep-your-personal-information-private

Caulfield, J. 2019. How to do thematic analysis. Scribbr. Retrieved on February 7 2021. Available at https://www.scribbr.com/methodology/thematic-analysis/

Chapman, R. (2019). What Is Data Analysis In Research And How To Do It?. Retrieved on February 8, 2021. Limeproxies. Available at https://limeproxies.netlify.app/blog/what-is-data-analysis-in-research-and-how-to-do-it/

Chetty, P. 2016. Importance of research approach in a research. ProjectGuru. Retrieved on February 5, 2021. Available at https://www.projectguru.in/selecting-research-approach-business-studies/

Cooper, P. 2020. 140+ Social Media Statistics that Matter to Marketers in 2020. Retrieved on March 18, 2021. Hootsuite. Available at https://blog.hootsuite.com/social-media-statistics-for-social-media-managers/#general

Deeney, N. 2020. Why Is Security Awareness Training Important? Metacompliance. Retrieved on March 12, 2021. Available at https://www.metacompliance.com/blog/why-is-security-awareness-training-important/

Dimitrov, I. 2021. invasive apps. Pcloud. Retrieved on March 13, 2021. Available at https://blog.pcloud.com/invasive-apps/

Driver, S. 2019. Don't Let These Social Media Mistakes Ruin Your Career. Retrieved on March 12, 2021. Businessnewsdaily. Available at https://www.businessnewsdaily.com/6758-social-media-mistakes.html

Mejia, M.E. 2019. How Instructional Design Impacts Every Organization Including Yours. Medium. Retrieved on March 4, 2021. Available at https://medium.com/dice-group/how-instructional-design-impacts-every-organization-including-yours-14fe1a4c511b

Fruhlinger, J. 2019. Malware explained: How to prevent, detect and recover from it. Csoonline. Retrieved on March 12, 2021. Available at https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html

Fruhlinger, J. 2020. Malware explained: What is phishing? How this cyber-attack works and how to prevent it. Csoonline. Retrieved on March 12, 2021. Available at https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

Gillis, A.S. 2020. Phishing . Techtarget. Retrieved on March 18, 2021. Available at https://searchsecurity.techtarget.com/definition/phishing

Gordon, S. 2021. What Is Cyberbullying?. Verywellfamily. Retrieved on March 18, 2021. Available at https://www.verywellfamily.com/types-of-cyberbullying-460549

Guan, H. 2019. Instagram 'Nasty List' Phishing Attack. University of guelph. Retrieved on May 10, 2021. Available at https://www.uoguelph.ca/ccs/infosec/instagram_phishing

Herold, R. 2018. 12 Reasons Why Data Privacy Protection Brings Business Value. Cpomagazine. Retrieved on March 20, 2021. Available at https://www.cpomagazine.com/blogs/privacy-intelligence/12-reasons-why-data-privacy-protection-brings-business-value/

Kellett, S. 2021. What Is "Do Not Track" (DNT) and Does It Work?. Avast.com. Retrieved on May 10, 2021. Available at https://www.avast.com/c-what-is-do-not-track

Korolov, M. 2019. What is a botnet? When armies of infected IoT devices attack. Csoonline. Retrieved on March 12, 2021. Available at https://www.csoonline.com/article/3240364/what-is-a-botnet.html

Lee, D. 2018. Facebook's data-sharing deals exposed. BBC. Retrieved on March 13, 2021. Available at https://www.bbc.com/news/technology-46618582

Miller, B. 2015. Can an Employer Ask to See an Employee's Social Media Account?. HR Daily Advisor. Retrieved on March 15, 2021. Available at https://hrdailyadvisor.blr.com/2015/03/12/can-an-employer-ask-to-see-an-employees-social-media-account/

Myhre, J. 2021. Privacy on Social Media Guards Against Identity Theft. BusinessNewsDaily. Retrieved on March 15, 2021. Available at https://www.businessnewsdaily.com/4194-social-media-security-tips.html

Nations, D. 2021. What Is Social Media?. Lifewire. Retrieved on March 11, 2021. Available at https://www.lifewire.com/what-is-social-media-explaining-the-big-trend-3486616'

O'Connell, B. 2018. How to Manage Your Privacy Settings on Social Media. Experian.com. Retrieved on May 10, 2021. Available at https://www.experian.com/blogs/ask-experian/how-to-manage-your-privacy-settings-on-social-media/

Privacy Rights Clearinghouse. 2019. Social Networking Privacy: How to be Safe, Secure and Social. Privacy Rights Clearinghouse. Retrieved on May 10, 2021. Available at https://privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and-social

Quigley, E. 2019. ADDIE: 5 Steps To Effective Training. Learnupon. Retrieved on March 12, 2021. Available at https://www.learnupon.com/blog/addie-5-steps/

Rodriguez, C. 2018. 3 Ways Your Data is Being Used Against You — And What to Do About It. Myamberlife. Retrieved on March 12, 2021. Available at https://www.myamberlife.com/learn/3-ways-your-data-is-being-used-against-you-and-what-to-do-about-it/

Sandle, T. 2020. Report finds only 1 percent reads 'Terms & Conditions'. Digital Journal. Retrieved on March 17, 2021. Available at http://www.digitaljournal.com/business/report-finds-only-1-percent-reads-terms-conditions/article/566127#:~:text=The%20group%20found%20that%20only,have%20%E2%80%9Cread%20it%20thoroughly.%E2%80%9D

Shacklett, M. 2021. multifactor authentication. SearchSecurity. Retrieved on May 10, 2021. Available at https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA

Siegel, R. 2014. Targeted Marketing and Online Privacy. TriplePundit. Retrieved on March 7, 2021. Available at https://www.triplepundit.com/story/2014/targeted-marketing-and-online-privacy/58336

Smith, A. 2017. Americans and Cybersecurity. Pewresearch. Retrieved on March 15, 2021. Available at https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

Stokes, N. 2017. Should You Use Facebook or Google to Log In to Other Sites? . Techlicious. Retrieved on March 20, 2021. Available at https://www.techlicious.com/blog/should-you-use-facebook-or-google-to-log-in-to-other-sites/

Sushko, O. 2020. What Is Online Privacy? This Is Your Human Right. Clario. Retrieved on March 10, 2021. Available at https://clario.co/blog/what-is-online-privacy/

Trochim, W. M. 2020. Deduction & Induction. Conjointly. Retrieved on February 6, 2021. Available at https://conjointly.com/kb/deduction-and-induction/

Twin, A. 2020. Data Mining. Investopedia. Retrieved on April 20, 2021. Available at https://www.investopedia.com/terms/d/datamining.asp

Vinz, S. 2015. Developing your theoretical framework. Scribbr. Retrieved on February 5, 2021. Available at https://www.scribbr.com/dissertation/theoretical-framework/

Wlosinski, L. G. 2019. The Benefits of Information Security and Privacy Awareness Training Programs. isaca, 5.

Writer, S. 2018. Top five social media privacy concerns. Reputation defender. Retrieved on 12, March 2021. Available at https://www.reputationdefender.com/blog/privacy/top-five-social-media-privacy-concerns

Appendices

Appendix 1. Survey questions

According to you, what kinds of information can be shared on social media?

In General, what do you know about Social media privacy concerns?

In simple words, what kinds of activity on social media may risk your personal/organization's private information?

What measures have you taken to keep your information private on social media?

What consequence could be caused by unresponsible activity done in social media?

What do you know about trackers and cookies that social media websites and apps use?

Which tools or methods can help you to prevent websites to track your activity?