TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Andrei Boitsov 201733IVSB

Personal Cyber Hygiene: Mitigating the Risks of Exposed Digital Identity Profiles

Bachelor's thesis

Supervisor: Toomas Lepikult
PhD
Co-Supervisor: Valdo Praust
Programme Director

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Andrei Boitsov 201733IVSB

Isiklik küberhügieen: digitaalisiksuse paljastuse riskide vähendamine

Bakalaureusetöö

Juhendaja: Toomas Lepikult
PhD
Juhendaja: Valdo Praust
Programmijuht

Tallinn 2023

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Andrei Boitsov

14.05.2023

Abstract

This thesis aims to outline the dangers of personal information oversharing using different methods of data collection and create a solution guide for an average user to improve their digital hygiene. The research focuses on understanding the current state of cyber hygiene, the potential risks associated with an exposed digital identity profile, and the utilisation of Open Source Intelligence (OSINT) tools for data collection.

A mixed-method approach was employed, incorporating a cyber hygiene awareness questionnaire, practical research using OSINT tools, and in-depth interviews. The questionnaire and interviews provide insights into users' knowledge, awareness, and practises related to cyber hygiene and personal information sharing. The practical research demonstrates the capabilities of OSINT tools in gathering public information to create digital profiles of individuals. The findings were used to develop targeted recommendations for improving cyber hygiene practises among users and to provide guidance on how to use these recommendations for further internet utilisation.

This thesis is written in English and is 71 pages long, including 7 chapters, and 22 tables.

Annotatsioon

Isiklik küberhügieen: digitaalisiksuse paljastuse riskide vähendamine

Käesoleva lõputöö eesmärk on kirjeldada isikuandmete liigse jagamise ohte, kasutades erinevaid andmekogumismeetodeid, ning luua keskmisele kasutajale juhend, kuidas parandada oma digitaalset hügieeni. Uurimistöö keskendub küberhügieeni hetkeseisu mõistmisele, avatud digitaalse identiteediprofiiliga seotud võimalikele riskidele ja avatud lähtekoodiga luurevahendite (OSINT) kasutamisele andmete kogumiseks. Kasutati segameetodilist lähenemisviisi, mis hõlmas küberhügieeni teadlikkuse küsimustikku, OSINT-vahendeid kasutavaid praktilisi uuringuid ja süvaintervjuusid.

Küsimustik ja intervjuud annavad ülevaate kasutajate teadmistest, teadlikkusest ja praktikatest seoses küberhügieeni ja isikliku teabe jagamisega. Praktiline uuring näitab OSINT-vahendite võimalusi avaliku teabe kogumisel, et luua üksikisikute digitaalsed profiilid. Tulemusi kasutati selleks, et töötada välja sihipärased soovitused kasutajate küberhügieeni tavade parandamiseks ja anda juhiseid, kuidas neid soovitusi kasutada Interneti edasisel kasutamisel.

Lõputöö on kirjutatud Inglise keeles ning sisaldab teksti 71 leheküljel, 7 peatükki, 22 tabelit.

List of abbreviations and terms

2FA	Two-Factor Authentication
ATO	Account takeover
GDPR	General Data Protection Regulation
MFA	Multi-Factor Authentication
OS	Operating System
OSINT	Open-Source Intelligence
SMS	Short Message Service

Table of contents

List of tables

1 Introduction

1.1 Background and Context

Cyber hygiene is a crucial component of protecting personal information and maintaining online privacy in an increasingly digital environment. Cyber hygiene refers to the practices and activities that computer and other device users take to keep their systems healthy and increase their online security. These practices are frequently part of a routine to protect identity and other information that might be stolen or modified. Users often make choices that might put them in danger because they are poorly informed on the full scope of possible hazards. The question is still relevant because people continue to disclose excessive quantities of personal information online without taking into account the opportunities provided by open source programs and their ability to gather enormous volumes of data. [1]

1.1.1 Cyber Hygiene

Cyber hygiene is a term for a collection of routines and behaviours designed to preserve the security and privacy of user data and digital identities online. In our increasingly interconnected society, where the internet plays a major role in our daily lives, adopting fundamental cyber hygiene habits is essential for keeping the risks associated with online activities as low as possible.

Making secure, unique passwords for online accounts and regularly updating them are crucial parts of good cyber hygiene. To make passwords more difficult to decipher, experts advise mixing capital and lowercase letters, numbers, and symbols. [2] Additionally, it is suggested against employing the same password across numerous accounts because doing so could expose all accounts if one is breached.

Another security method that can drastically improve online account security is two-factor authentication (2FA). Even if the password is hacked, 2FA helps guard against unwanted access by requiring a second form of identification in addition to a password.

If account security should be protected even harder, it is possible to implement multi-factor authentication (MFA). [3]

Cyber hygiene also includes exercising caution while disclosing personal information online. For instance, excessive sharing on social media sites might put users at danger for things like identity theft, financial fraud, and cyberstalking. Limiting the accessibility of personal information to trusted contacts and being aware of privacy settings on social media accounts are essential. [4]

A crucial aspect of cyber hygiene is educating oneself about the hazards and best practises related to internet security. Individuals can identify and steer clear of potential risks in the online world by having knowledge of phishing attempts, social engineering, and other threats.

In conclusion, maintaining good online hygiene is crucial for safeguarding private data and digital identities. People can greatly lower the dangers related to their online activity by developing secure habits including using strong passwords, upgrading software, enabling two-factor authentication, and being cautious when sharing personal information.

1.1.2 Digital Identity and Risks

A person's "digital identity" consists of their unique information that allow them to be recognised on the internet. A person's digital footprint consists of their usernames, emails, phone numbers, social media accounts, and overall recorded online activity. [5]

Having your identity stolen is a major concern when you have a significant digital footprint available for the criminals. Cybercriminals may impersonate an individual, get access to their accounts, and commit fraud by mining publicly accessible data of that person. [6] Attackers often collect personal data through data breaches and social engineering tactics with the intent of committing identity theft.

Another concern associated with digital identities is cyberstalking. People may unknowingly expose themselves to unwelcome attention and harassment as they post more details about their lives on social media platforms. Personal information obtained online may be used by cyberstalkers to track, control, or threaten their targets. [7]

Digital footprints, which are the traces of data left by online actions, could also be dangerous. A broad digital footprint can make it simpler for cybercriminals to put together an in-depth portrait of a person and use it for their own needs. Digital footprints can also have a lasting impact on a person's reputation because it can be challenging to completely delete material that has been shared online. [8]

Possessing a digital identity has become essential for existing in the digital age, and protecting your privacy and security requires recognition of the risks. People can substantially reduce their susceptibility to cyber attacks by being aware of possible risks and taking proactive measures to protect their digital identities.

1.2 OSINT Tools and Frameworks

The act of gathering, evaluating, and exploiting information from publicly accessible sources to serve different intelligence and security goals is referred to as open-source intelligence (OSINT). [9] OSINT allows businesses and people to obtain greater understanding of the digital environment and take the necessary actions towards protecting their digital assets and online presence.

OSINT tools and frameworks can be used to help acquire and analyse information from a variety of sources, including social media platforms, websites, blogs, forums, and public databases. [10]

Data collection tools help in gathering raw information from open sources. Examples of these tools include web tools that are available to find on OSINT Framework website, search engines such as Google, and other tools that are accessible using CLI (Command-Line Interface).

It is essential to remember that using OSINT technologies and frameworks requires a thorough awareness of ethical issues and legal restrictions. The collection and analysis of data from publicly accessible sources can cause privacy problems, and improper use of OSINT technologies may have unexpected consequences or violate the law.

Only specific, explicit and legal purposes are permitted for the collection of personal data. More data handling than is required to resolve investigative questions is prohibited by

GDPR. The data handled must be collected only for necessary purposes and processed lawfully and fairly.

Subject-specific personal data must only be kept for as long as is necessary. Additionally, personal data must be protected by IT from unauthorised or unlawful processing as well as accidental loss or destruction.

Under GDPR, the subject of your investigation has rights:

- Right to be informed of how your data is being processed.
- Right to access this data.
- Right to rectify incorrect data.
- Right to erase data.
- Right to restrict processing of personal data.
- Right to data portability – this means that as a researcher you must have in place a system that allows you to quickly and easily compile all the personal data you hold on an individual and make it securely accessible to them.
- Right to object to your data being processed.
- Rights relating to automated decision making, including processing.

In conclusion, OSINT tools and frameworks provide practical instruments for gathering, evaluating, and visualising data from open sources. Making use of these tools can help people and businesses better understand the digital environment, spot potential threats, and strengthen their overall safety measures. [11]

1.3 Objectives and Scope

This thesis will address the risks of revealing personal information, outline various data collection techniques, and put together a helpful manual that regular users can follow to improve their online safety. The focus of this thesis is exclusively on digital identity; it does not cover any aspects of physical identity. The research paper includes all the methods of data collection used. The theoretical section of the thesis is based on published articles and includes a review of the current global state of cyber hygiene and a look at the dangers of having one's digital identity exposed to social engineering and other forms of exploitation. The research method for the practical section is a survey, OSINT Tools research along with interviews to gather more in-depth data. The subjects' digital persona is created using OSINT tools, and the interview allows to gather a more personal view of respondents' awareness of cyber hygiene. The gathered data is analysed to create a clear picture of a publicly accessible digital profile, the methods employed to protect it, and ways to improve cyber hygiene. A step-by-step manual that offers users ways to solve or at least reduce the problem of cyber hygiene is based on the information that has been collected. Guide includes instructions and a manual that help users examine the available data and explain what can be done with it.

2 Literature review

2.1 Current State of Cyber Hygiene

In today's networked culture, maintaining digital security and privacy has become a significant problem for both individuals and organisations. Cyber hygiene is crucial for protecting digital assets and preventing unauthorised access to personal information. Cyber hygiene can be described as the behaviours and practices that support the safety and confidentiality of information systems, accounts, and devices. [12]

One of the major factors affecting the state of cyber hygiene at the moment is the rapid rate with which technology and the internet are developing. People are producing and storing enormous amounts of data, some of which may be very sensitive, as a result of their increasing reliance on computers, smartphones, and online services.

Numerous cyber hygiene practices have been created as a response to these problems in order to assist people and organisations in safeguarding their digital assets. Strong, unique passwords, routine software upgrades, data backups, and the usage of multi-factor authentication for online accounts are some examples of these best practices. A lot of businesses have also implemented security awareness training programs to teach staff members the value of practicing good cyber hygiene and how to spot and address online dangers.

The current condition of cyber hygiene is still in trouble despite these efforts. Many people and organisations still practice unsafe behaviours including using the same passwords for many accounts, skipping software updates, and oversharing personal information on social media. These actions increase the possibility that you may be the target of cyberattacks like phishing, ransomware, and data breaches. [13]

One of the main causes of these risky actions has been determined to be a lack of knowledge and awareness of cyber dangers and the significance of proper cyber hygiene. [14] People in particular could undervalue the negative effects of bad cyber hygiene, such as identity theft, monetary loss, or reputational harm. Additionally, people can lack the knowledge and expertise needed to put appropriate cyber hygiene practices in place,

which could cause them to rely on default security settings and have excessive faith in the protection offered by technology suppliers. [15]

To improve the current state of cyber hygiene, individuals and organisations have to emphasise digital security and privacy by setting up a proactive mitigation approach. This involves training to increase awareness of cyber threats and promote good cyber hygiene practices, in addition to implementing strict security policies and procedures to safeguard digital assets. [14]

In conclusion, the status of cyber hygiene is marked by a combination of positive developments and ongoing challenges. Despite the fact that many individuals and organisations have adopted cyber hygiene practices to safeguard their digital assets, hazardous behaviours and a lack of awareness continue to undermine these efforts. Individuals and organisations can improve their cyber hygiene and reduce their susceptibility to intrusions by prioritising digital security and privacy and investing in education and training.

2.2 Dangers of Exposed Digital Identity Profiles

Given that individuals interact in the age of digitisation, the concept of a digital identity has become ever more essential. A digital identity is a collection of records that relate to an individual, such as personal, financial, and social information. The increasing amount of sensitive data available online, along with the habit of individuals to overshare, has increased the risk of digital identity profiles being exposed. This section aims to examine the various risks associated with exposed digital identity profiles, including social engineering, privacy invasion, identity theft, and other potential threats. Understanding these risks can help protect digital identities and maintain improved cyber hygiene.

2.2.1 Social Engineering

Social engineering is a psychological manipulation technique employed by cybercriminals to deceive individuals into divulging sensitive information, such as passwords or financial data, or performing actions that compromise their security. Social engineering exploits human vulnerabilities rather than technical ones, targeting the weakest link in the security chain: people. Gathering substantial information about the

person allows the possibility to perform an excellent social engineering attack using their personal information to build trust. [16]

Phishing is an attack that attempts to steal your money or your identity by tricking you into revealing confidential information, such as credit card numbers, bank account information, or passwords, on websites that pose as legitimate. In a typical phishing email, cybercriminals pose as reputable businesses, friends, or acquaintances and include a link to a phishing website. [17]

Pretexting is a tactic employed by attackers that entails the creation of scenarios that increase the likelihood that a future social engineering attack will be successful. Pretexting may involve connecting with someone through a fake email address in order to commence the first phase of a future attempt to penetrate a network or steal data. [18]

One of the most serious risks of open digital identity profiles is that hackers could take advantage of them to gain trust from their targets, making social engineering assaults more successful. Cybercriminals, for example, may utilise personal information obtained from social media accounts or data breaches to design highly targeted and persuasive spear-phishing emails, increasing the possibility that the receiver would fall for the fraud.

Individuals should retain a high degree of suspicion when receiving unsolicited emails, check the sender's identity, and abstain from oversharing personal information online to reduce the hazards connected with social engineering. [16]

2.2.2 Financial Fraud and Identity Theft

The act of achieving financial benefit using profit-driven criminal activities, such as identity theft, ransomware attacks, email and internet fraud, and efforts to steal bank accounts, credit cards, or other payment card information, is referred to as cybercrime in finance. Financial cybercrime encompasses acts such as obtaining payment card information, getting access to financial accounts in order to conduct unlawful transactions, extortion, identity theft in order to apply for financial products. [19]

Identity theft occurs when an attacker obtains and uses a victim's personal information, such as their name, Social Security number, or credit card details, to commit fraudulent activities, such as opening new accounts, making unauthorised purchases, or even filing

false tax returns. According to the Javelin, in 2020 there were financial losses associated with identity theft accounting for 56 billion dollars. [20]

Account takeover is a kind of financial fraud in which attackers use stolen login credentials or personal information to obtain access to a victim's online accounts, such as banking. Once in command, the attacker may move money, conduct unlawful activities, or utilise the account to commit more fraud. [21]

2.2.3 Digital Footprint and Reputation Management

A digital footprint, or an electronic footprint, is the trail of data you leave when you use the internet. It includes websites visited, emails sent, and information submitted online. Internet users can actively or passively leave a digital trace. A person's digital footprint can have significant implications for their online reputation and privacy, as it can reveal personal details, preferences, and habits that may be exploited by cybercriminals or used to make judgments about their character. [22]

Online reputation management is becoming more crucial in today's digital world, as it has a significant impact on both personal and professional possibilities. A good internet reputation opens doors to new prospects, but a poor one might do the opposite. Individuals and company owners must understand the importance of keeping a positive internet reputation. [23]

In addition, a badly maintained digital footprint may raise the danger of cyberbullying, harassment, and online shaming since people may be targeted based on their online activity or personal information. In severe cases, this might result in mental anxiety, social isolation, self-harm, or suicide. [24]

2.3 OSINT Tools: Capabilities and Utilisation

Tools for OSINT are essential for gathering information that is readily accessible about people. These tools allow investigators, cybersecurity experts, and even regular users to gather information for improving cyber hygiene, spotting potential threats, and assessing the dangers of sharing too much personal information online. It is important to mention that some of the tools may not be that easily accessed and do require manual installation to make use of it from CLI or even depend upon doing manual coding.

Lookup Engines

One of the easiest methods to find information about people is search engines. Users can access a wide range of information by simply typing the name, username, or email into the search engine bar which can result in finding social media profiles, forum posts, blog posts, and more. The countless websites that such search engines crawl and index allow for the discovery of useful data regarding a person's online presence.

Social Media Websites

Social media platforms can reveal a lot of information about people, including their relationships, activities, and interests. Users can find profiles, posts, photos, and other content that can provide an insight into someone's online life. Since most of the time a person is using a big variety of different social media it can provide quite an extensive amount of data if the profile is open for public view.

Services for Reverse Email Lookup

Users of reverse email lookup services can learn more about a person by using their email address. These instruments can expose related websites, social media profiles, and other online activities. In some cases, these services might also offer extra contact details like phone numbers or addresses.

Search engines for people

Search engines for people gather data on people from a variety of sources, such as public records, social media profiles, and other databases on the internet. Users can access an extensive amount of information about a person, including contact information, social media profiles, and other personal details, by entering a name, username, phone number or email address.

Detailed OSINT Resources

OSINT resources that compile different search tools for OSINT investigations are also available for general users to use. These tools allow for searching social media, email addresses, and other resources. These tools grant users a possibility to carry out more in-depth research and compile larger amounts of data about their subjects. [9] [10]

3 Methodology

3.1 Research Design

The research design for this thesis employs a mixed-methods approach to provide a comprehensive understanding of cyber hygiene practices and digital identity management among internet users. By combining diverse data sources and employing quantitative and qualitative analysis methods, the study aims to generate characterised insights into the current state of cyber hygiene and digital identity management, allowing for the development of practical guidelines and recommendations for improving cyber hygiene practices and reducing risks associated with personal information sharing.

3.2 Practical Information Gathering

The methodology involves quantitative data collection through a cyber hygiene awareness questionnaire, qualitative data collection via in-depth interviews, and Open Source Intelligence (OSINT) tools used to assess publicly available information.

3.2.1 Cyber Hygiene Awareness Questionnaire

Quantitative data collection: A questionnaire on cyber hygiene awareness is used to collect quantitative data during the first stage of the research design. To find out more about respondents' knowledge, attitudes, and behaviours about cyber hygiene and personal information sharing practices, the survey includes both single- and multiple-choice questions as well as free text questions. To gather an extensive number of perspectives and experiences, the questionnaire is given out to a diverse sample of participants amongst the employees of Yolo Group company that focuses on IT services.

3.2.2 OSINT Data Collection

Qualitative data collection: OSINT tools are utilised to collect publicly available information on individuals that agreed to participate in the further research after submitting the questionnaire to develop a clearer understanding of the digital profiles that can be constructed using such tools. This part of the research helps to demonstrate the extent of personal information that can be collected and the potential risks associated with poor cyber hygiene practices.

Upon gathering various information about OSINT tools using Github and OSINT Framework resources it was decided that 6 tools and manual research will be used in total for the OSINT data collection part. Tools used vary from user-friendly websites to CLI tools that are used more for advanced research. Manual approach performed in a way of scraping additional information using the data found by the OSINT tools.

List of used tools is presented below:

- Analyzeid

  A website tool, simple to use by an average user. This tool is a social media username checker. The tool is gathering information on the username and getting a summary of who the person is. The full output consists of sites where this username is taken, a username summary based on the information found: full name, position, photos. [25]

- Idcrawl

  A website tool, simple to use by an average user. This tool takes a username as a parameter and provides sites where this username is used, and can find the emails connected to the username. [26]

- Whatsmyname

  A website tool, simple to use by an average user. Tool takes a username as a parameter and provides sites where this username is used, can specify the category of the account found as well as has an ability to filter the output by category. [27]

- Sherlock

  A CLI tool. Can be used on LinuxOS, MacOS and WindowsOS. Tool takes a username as an input and provides a list of websites with a link to the user's account, and has additional parameters for output formatting. [28]

- Maigret

  A CLI tool. Can be used on LinuxOS and MacOS. Tool takes username as an input and provides a list of websites using this username with an extensive report for each site if information is available and retrievable. [29]

- Holehe

  A CLI tool. Can be used on LinuxOS and MacOS. Retrieves information using the forgotten password function via email. Provides websites where the email is used, if possible retrieves additional information. Tool can also be embedded into a python application to apply filters and custom output. [30]

3.3 In-depth Interviews

Qualitative data collection: Following the analysis of the questionnaire and OSINT research results the respondents that agreed to participate in the OSINT research are selected for in-depth interviews. These interviews are conducted to gather detailed information on participants' experiences with data breaches, cyber attacks, and their online sharing habits. The interviews also explore participants' strategies for managing their digital identities and the factors that influence their decision-making processes regarding personal information sharing. The interview plan as follows:

Part 1: Cyber Hygiene Practices and Awareness

1. **Introduction**

   Introduction of the interviewer. Confidentiality and anonymity of the interview and processed data

2. **Cyber Hygiene Habits and Practices**

   Evaluation of the respondent’s internet habits and measures they take to protect their digital identities and maintain their cyber hygiene

3. **Cyber Hygiene Questionnaire**

   Review of the questionnaire answers with the respondent. Additional questions regarding the selected answers

4. **Awareness of Digital Identity Risks and Consequences**

   Discussion about potential risks related to personal cyber hygiene and cybersecurity. Additional review of attacks on the respondent

Part 2: OSINT Data Collection Results and Discussion

5. **Sharing OSINT Data Collection Results**
   Presentation of the results of the OSINT data collection to the respondents, highlighting the types of personal information that were gathered and any potential vulnerabilities or risks identified

6. **Perception of OSINT Findings**
   Respondent's thoughts about their data collection results

7. **Addressing Identified Risks and Improving Cyber Hygiene**
   Steps respondents plan to take in response to the OSINT findings
   How to improve cyber hygiene practices

8. **Conclusion**
   Additional comments

3.4 Analysis of the findings

Data Analysis: The collected data will be analysed using appropriate methods. For the questionnaire data analysis will include creating recommendation data. The OSINT data and interview will be analysed to evaluate the effectiveness of existing cyber hygiene practices and identify potential areas for improvement as well as comparing the perception on the cyber hygiene and the actual findings.

4 Practical part – gathering the information

4.1 Cyber Hygiene Awareness Questionnaire

The Cyber Hygiene Awareness Questionnaire was developed to gather information on participants' knowledge, awareness, and practices related to cyber hygiene and personal information sharing. The questionnaire was distributed via Google Forms and shared with colleagues in Yolo Group company, reaching a total of 100 responses before closing the survey. The questionnaire consisted of 18 questions, covering the following areas:

1. General Questions:

This group of questions covers broad topics related to cybersecurity and cyber hygiene. The responses to these questions provide insight into people's general knowledge and habits related to online security.

2. Data Oversharing:

This group of questions focuses specifically on the risks associated with sharing personal information online. The responses to these questions provide insight into people's awareness of the risks associated with oversharing and their attitudes towards protecting their personal information online.

3. Data Managing:

This group of questions explores people's habits and behaviours related to cybersecurity. The responses to these questions provide insight into how people prioritise cybersecurity and the measures they take to protect themselves from cyber threats.

4. Improving cyber hygiene:

This group of questions examines people's experience related to improving their cyber hygiene habits. The responses to these questions can provide information on how people are staying up to date with the current cybersecurity’s state and features.

The Cyber Hygiene Awareness Questionnaire also included additional sections that prompted the respondents to take part in the interview. By the time the questionnaire reached a total of 100 responses 28 respondents decided to take part in the further research and after the direct confirmation of OSINT data collection there were 3 respondents left that agreed for their personal data to be collected and analysed.

An overview of the questions present in the questionnaire is presented in Table 1.

Table 1 – Question Groups

Group	Questions
General questions	Q1, Q2, Q3, Q4, Q5, Q6
Data oversharing	Q7, Q8, Q9, Q10
Data Managing	Q11, Q12, Q13, Q14, Q15
Improving cyber hygiene	Q16, Q17, Q18

18 Questions from the questionnaire are presented below:

Q1: On a scale of 1-5, with 1 being the least secure and 5 being the most secure, how would you rate your personal cybersecurity?

Q2: At what point do you think it becomes necessary to change a password?

Q3: How do you typically choose passwords for your online accounts?

Q4: What one-time password method is preferred in your opinion?

Q5: Have you ever experienced a data breach or a cyber attack?

Q6: How has your experience with data breaches or cyber attacks, either directly or indirectly, influenced your approach to sharing personal information online, and do you believe your current practices are sufficient to minimise the risk of future incidents?

Q7: Have you ever shared personal information online and then regretted it afterward?

Q8: How often do you share personal information, such as your location or activities, on social media?

Q9: How do you typically handle requests for personal information from websites or apps?

Q10: How do you typically decide what personal information to share or withhold online?

Q11: How do you dispose of old devices containing personal information, such as smartphones or laptops?

Q12: How do you store and manage your personal information on your devices, such as passwords, financial information, or identification documents?

Q13: Do you have any social media accounts that you are no longer using?

Q14: Do you use a different email address for sensitive or confidential online activities, such as online banking or healthcare services?

Q15: How do you typically review and manage the privacy settings on your social media accounts?

Q16: What steps have you taken to educate yourself about online security and best practices for cyber hygiene?

Q17: How do you educate others, such as friends or family, about online security and cyber hygiene?

Q18: Have you ever conducted a security examination of your online accounts (verifying the security of the login, checking privacy settings, ensuring that best practices are followed), and if so, what did you learn?

The results of the questionnaire are presented in Appendix 2.

4.2 OSINT Data Collection

After a direct confirmation of the data being collected for the OSINT research a total of 3 respondents agreed to participate in the OSINT Data collection research. The research is attached to the Appendix 3 and includes the tools used and social media/services websites that were found using these tools. Additionally, research includes the manual part which collects the information gathered on the websites collected.

4.3 Interview with respondents

In this part the overview of the interview is presented. On average each interview took 30 minutes and was made in-person with each respondent allowing to properly show the results of the OSINT research.

Respondent 1:

Part 1: Cyber Hygiene Practices and Awareness

1. Introduction

The significance and rationale behind this research were thoroughly communicated to the respondent. They were informed that none of their personal information would be directly shared or disclosed in the study. All identifying information would be modified and presented in such a manner that it would be impossible to draw any conclusions or assumptions about the respondent's identity. The primary focus of the interview is to compare the individual's perception of their digital identity with the actual findings derived from the OSINT research, shedding light on potential discrepancies and areas for improvement in their cyber hygiene practices.

2. Cyber Hygiene Habits and Practices

Respondent mentioned that they are using social media all the time and they are free to share a lot of information online. They do use advanced techniques to secure their internal home network, regarding their gadget security - their approach is very secure and they tend to be careful and not use their working laptop for personal social media accounts. They are concerned though about their social media accounts. They do use the password manager to keep their password safe and they're pretty satisfied with their security. They do acknowledge also that some of their accounts do not have any more secure policies implemented other than a password. They only change passwords and policies when there is an enforcement from the app/website itself.

3. Cyber Hygiene Questionnaire

In the questionnaire they have selected that they do frequently change their password because on some accounts where password manager is not used they tend to forget the password.

4. Awareness of Digital Identity Risks and Consequences

The respondent is fully aware that accounts can be hacked with enough effort and that it can heavily harm someone's reputation. They have also shared that they have an incident that happened because they have used the same username on their freelance profile and personal account. The respondent was a victim of blackmail and they had serious issues with their actual job they were working on. It took weeks for the victim to regain the status in the company they have worked in. This case helped them to learn the dangers of reusing the username.

Part 2: OSINT Data Collection Results and Discussion

5. Sharing OSINT Data Collection Results

During the interview, the tools employed to gather information about the respondent were thoroughly explained, including their usage, capabilities, and the rationale behind their selection. The specific details used as input parameters for each tool were also shared, which, in this case, consisted of the respondent's full name and multiple usernames discovered through manual research. Subsequently, the findings were presented to the respondent, who reviewed some of their accounts. The interview also covered which social media platforms contained the most shared information, as well as the security risks associated with the data found on different accounts. Additionally, the manual aspect of the research was discussed, with the sources and findings being shared with the respondent, further contributing to their understanding of their digital identity and potential vulnerabilities.

6. Perception of OSINT Findings

The respondent mentioned that they do have another email that they use which potentially led to making it harder to find all the accounts and traces left. They acknowledge that using the same username in the email as a regular username can make it really easy to find most of the accounts. They were also amazed that some information in the manual research was found not from the sources they were thinking it came from.

7. Addressing Identified Risks and Improving Cyber Hygiene

They admitted that they will definitely delete some of the accounts and remove information if possible. Considering their past experience with blackmail they will also try to come up with different usernames to decrease the chances of finding information on them.

8. Conclusion

Respondent was really happy that the research was shared with them. They are considering sharing the experience and tactics learned with their close friends.

Respondent 2:

Part 1: Cyber Hygiene Practices and Awareness

1. Introduction

The significance and rationale behind this research were thoroughly communicated to the respondent. They were informed that none of their personal information would be directly shared or disclosed in the study. All identifying information would be modified and presented in such a manner that it would be impossible to draw any conclusions or assumptions about the respondent's identity. The primary focus of the interview is to compare the individual's perception of their digital identity with the actual findings derived from the OSINT research, shedding light on potential discrepancies and areas for improvement in their cyber hygiene practices.

2. Cyber Hygiene Habits and Practices

The respondent conveyed that they frequently use the internet, but they only post content on social media about once a week. They prefer to share information on platforms where privacy settings can be adjusted to limit visibility to friends only. The respondent also mentioned that they do not delete old accounts, as most platforms do not offer a straightforward option for deletion, and the only alternative is to email the company with a profile deletion request. Furthermore, the respondent shared their understanding of the benefits of using separate email addresses for different aspects of their online life, as it can enhance security. They also highlighted the usefulness of password managers in maintaining strong and unique passwords, contributing to better overall cyber hygiene.

3. Cyber Hygiene Questionnaire

The conversation touched upon the fact that the respondent has experienced a significant number of security breaches. They mentioned that they often receive email notifications alerting them about unauthorised attempts to access their accounts.

4. Awareness of Digital Identity Risks and Consequences

The respondent expressed awareness that their pictures and messages might be found online, indicating a level of understanding of their digital footprint. They also make an effort to minimise the sharing of banking credentials online; however, they acknowledge that this is not always successful, as some details may still be saved on certain websites. Despite this, the respondent assumes that the available information would not be sufficient for a hacker to cause significant damage.

Part 2: OSINT Data Collection Results and Discussion

5. Sharing OSINT Data Collection Results

During the interview, the tools employed to gather information about the respondent were thoroughly explained, including their usage, capabilities, and the rationale behind their selection. The specific details used as input parameters for each tool were also shared, which, in this case, consisted of the respondent's full name and multiple usernames discovered through manual research. Subsequently, the findings were presented to the respondent, who reviewed some of their accounts. The interview also covered which social media platforms contained the most shared information, as well as the security risks associated with the data found on different accounts. Additionally, the manual aspect of the research was discussed, with the sources and findings being shared with the respondent, further contributing to their understanding of their digital identity and potential vulnerabilities.

6. Perception of OSINT Findings

The respondent observed that CLI tools can be significantly more powerful than web-based tools in terms of gathering personal information. They were surprised to learn that some websites had their email hash available, and that it was possible to reverse-engineer the actual email from the hash. Even though the amount of information available about

them online is considerable, the respondent expressed relief that it had not been exploited for malicious purposes.

7. Addressing Identified Risks and Improving Cyber Hygiene

It was discussed with the respondent the potential risks associated with their current approach to cybersecurity which included the weakness of using the email username as a default username upon registration on websites. In response, the respondent shared a story about a friend who had demonstrated how easy it was to obtain information on another mutual friend using their username. This incident acted as a call to action for the responder, making them aware of the possible consequences of weak passwords, security breaches, and unknowingly disclosing information online. As a result, they decided to start utilising a password manager in their daily lives to improve their security precautions. The respondent also explained their current method of creating passwords, which involves using personal password strategies with keywords translated into another language.

8. Conclusion

The respondent expressed their intention to share the insights and knowledge gained from the interview with others. However, they acknowledged that teaching cybersecurity and cyber hygiene concepts to elderly individuals could be particularly challenging due to potential technological knowledge gaps and resistance to change.

Respondent 3:

Part 1: Cyber Hygiene Practices and Awareness

1. Introduction

The significance and rationale behind this research were thoroughly communicated to the respondent. They were informed that none of their personal information would be directly shared or disclosed in the study. All identifying information would be modified and presented in such a manner that it would be impossible to draw any conclusions or assumptions about the respondent's identity. The primary focus of the interview is to compare the individual's perception of their digital identity with the actual findings

derived from the OSINT research, shedding light on potential discrepancies and areas for improvement in their cyber hygiene practices.

2. Cyber Hygiene Habits and Practices

The respondent stated that they use the internet on a regular basis and feel comfortable sharing a lot of information online. However, they noted that they had gradually lowered the amount of personal information they post on the internet over time. They also emphasised the usage of a multiple email approach, utilising several email accounts based on the unique services they utilise. This approach allows them to classify their online activities and enhance their privacy and security in the digital realm.

3. Cyber Hygiene Questionnaire

The respondent acknowledged that they had a habit of reusing passwords for their various internet accounts. It was only after joining a company with established password manager policies that they began to pay more attention to their password security. While the respondent's personal security evaluation was assessed to be average, it was still deemed sufficient, as it was not possible to identify their email address. However, it was also noted that the respondent's preferred method for OTP — SMS-based OTP, which may not be the most secure option. This indicates that there may be room for improvement in their overall approach to cybersecurity and digital identity protection.

4. Awareness of Digital Identity Risks and Consequences

The respondent admitted to continuing the practice of reusing the same password for certain types of accounts, even though they recognise that this method is not secure. To mitigate potential risks, they ensure the use of strong and unique passwords for accounts where they share a significant amount of personal information. Moreover, the respondents expressed their awareness of the potential consequences of poor cyber hygiene, such as identity theft and financial fraud. This understanding highlights their recognition of the importance of maintaining good cyber hygiene practices to protect their digital identity and minimise risks associated with online activities.

Part 2: OSINT Data Collection Results and Discussion

5. Sharing OSINT Data Collection Results

During the interview, the tools employed to gather information about the respondent were thoroughly explained, including their usage, capabilities, and the rationale behind their selection. The specific details used as input parameters for each tool were also shared, which, in this case, consisted of the respondent's full name and multiple usernames discovered through manual research. Subsequently, the findings were presented to the respondent, who reviewed some of their accounts. The interview also covered which social media platforms contained the most shared information, as well as the security risks associated with the data found on different accounts. Additionally, the manual aspect of the research was discussed, with the sources and findings being shared with the respondent, further contributing to their understanding of their digital identity and potential vulnerabilities.

6. Perception of OSINT Findings

The respondent expressed appreciation for receiving a detailed report on their digital persona. Given that they had self-assessed their cyber hygiene as being average, they initially assumed that even more information would be found about them. They also acknowledged that using additional usernames might have led to the discovery of further information, suggesting the potential for a more extensive digital footprint.

7. Addressing Identified Risks and Improving Cyber Hygiene

Upon realising how easily searchable and accessible their personal information was, the respondent expressed their intention to delete most of the discovered accounts as a security precaution.

8. Conclusion

The respondent conveyed their intention to share the strategies and insights they gained during the interview with their relatives and close friends, emphasising the importance of spreading awareness about cybersecurity and cyber hygiene. They also noted that using the same username across multiple platforms could potentially harm an individual in the event of a cybersecurity attack. In their case, employing multiple usernames and email addresses prevented the identification of all their online accounts, demonstrating the benefits of diversifying one's digital identity as a protective measure against potential threats.

5 Analysis of the findings

5.1 Questionnaire analysis

General questions

Q1: On a scale of 1-5, with 1 being the least secure and 5 being the most secure, how would you rate your personal cybersecurity?

The majority of respondents rated their personal cybersecurity as average or above average. However, only a small number of respondents believe their personal cybersecurity is at the highest level. The results do not strictly fall into the normal distribution category but show some characteristics of a normal distribution. [31]

Q2: At what point do you think it becomes necessary to change a password?

By examining how often individuals change their passwords and the situations that prompt them to do so, we can develop recommendations for enhanced password management and overall cyber hygiene. While 29 respondents choose to change their passwords every 90 days, which can sometimes provide better security, it is not strictly necessary without evidence of a breach or cyberattack. [32] Furthermore, only 54 respondents mentioned changing their passwords following a breach or cyberattack on their accounts.

Q3: How do you typically choose passwords for your online accounts?

It is vital for the third of the respondents who use the same password across multiple accounts to understand the risks associated with this approach and adopt unique passwords for each account, thereby reducing the potential harm caused by a single account breach. The two respondents who rely on simple, easy-to-remember passwords should be made aware of the importance of using complex, hard-to-guess passwords to increase their online account security. For the eight respondents with a unique password strategy, examining their methods and assessing their alignment with password security best practices could reveal potential examples for others to follow. Company’s policy includes using a password manager for all the work-related accounts which means everyone has experience with it, but not everyone is using it for personal accounts.

Q4: What one-time password method is preferred in your opinion?

The analysis of respondents' preferred one-time password (OTP) methods reveals that while SMS and Email OTPs are popular, more secure options like hardware-based, software-based, and push OTPs have a significant following. To improve cyber hygiene and minimise security risks, it is essential to educate users about the potential vulnerabilities associated with SMS and Email OTPs and promote the adoption of more secure alternatives. By raising awareness about the advantages and disadvantages of different OTP methods and encouraging the use of hardware-based, software-based, and push OTPs, we can enhance overall security practices and contribute to better two-factor authentication measures.

Q5: Have you ever experienced a data breach or a cyber attack?

The questionnaire results reveal that almost half of respondents have personally experienced a data breach or cyber attack, and an additional third of the respondents know someone who has faced such incidents. This indicates that 81% of the respondents have either directly or indirectly been exposed to the consequences of poor cyber hygiene and security practices, emphasising the importance of proactive measures in protecting digital identities.

Q6: How has your experience with data breaches or cyber attacks, either directly or indirectly, influenced your approach to sharing personal information online, and do you believe your current practices are sufficient to minimise the risk of future incidents?

The analysis of this question shows that experiences with data breaches or cyber attacks have significantly influenced respondents' online behaviour and their perceptions of the sufficiency of their current practices in minimising future risks. A majority have made adjustments to their online habits, become more cautious, and now pay closer attention to security measures and privacy settings. These results underline the importance of learning from past experiences to improve overall cyber hygiene and can be used to inform tailored recommendations, such as continuously updating knowledge about evolving threats, emphasising strong security measures and privacy settings, and promoting cautious information sharing.

Data oversharing

Q7: Have you ever shared personal information online and then regretted it afterward?

The analysis of the responses indicates that almost half of respondents have shared personal information online and regretted it and other half of them never had such an experience. This means that 45% of the respondents most likely identified and tried removing their personal information online which may or may not resulted in successful data removal.

Q8: How often do you share personal information, such as your location or activities, on social media?

The analysis of this question highlights the varying degrees of personal information sharing on social media among respondents, the results serve as a basis for exploring further research questions and developing more targeted strategies to address the problem of oversharing and its consequences.

Q9: How do you typically handle requests for personal information from websites or apps?

Results emphasise the importance of informed decision-making when providing personal information online, informing tailored recommendations for enhancing cyber hygiene and responsible information sharing. These findings demonstrate that the vast majority of the respondents do care about not oversharing personal information when it is possible or provide false information which in some cases can be a better option than blindly give the information when requested to do so.

Q10: How do you typically decide what personal information to share or withhold online?

Based the findings, several recommendations can be proposed for promoting responsible information sharing and improving cyber hygiene. It is crucial to emphasise the importance of understanding and utilising privacy settings on various platforms, as this allows users to manage who can view their shared content. Although most of the respondents tend to carefully decide and analyse the information shared, they still may base their decision on instincts and not on the actual necessity of providing the information.

Data Managing

Q11: How do you dispose of old devices containing personal information, such as smartphones or laptops?

The analysis of this question explores the methods respondents employ when disposing of old devices containing personal information, such as smartphones or laptops. Users should definitely erase all data from their devices before selling or disposing of them. For users who choose to keep their old devices, it is essential to securely erase or format the devices to eliminate any residual personal information. It is important to note that although different approaches can be made to dispose of old devices it is important to remember that on old devices there can be accounts saved that may be forgotten if the device is disposed of without properly going through all the data on it.

Q12: How do you store and manage your personal information on your devices, such as passwords, financial information, or identification documents?

Findings from this question suggest the need to increase awareness about the significance of secure storage and management of personal information. The use of password managers and encryption software is recommended, as well as informing users about the dangers of poorly securing their sensitive data. Quarter of the users that stated that they have not given much thought into that should look into ways of securing their personal information stored on their devices since breach of such data may backfire.

Q13: Do you have any social media accounts that you are no longer using?

Results from the question indicate a potential risk associated with inactive accounts, as they may still contain personal information of which users may have forgotten. It is recommended to encourage users to periodically review their social media accounts, deactivate or delete those they no longer use, and ensure that personal information shared on active accounts is up-to-date and protected by appropriate privacy settings. This approach would contribute to improved cyber hygiene and mitigate potential risks associated with inactive social media accounts. Even if the users would not feel like deleting the account it is still encouraged to make a note that a certain account exists, an even safer option would be to store the account credentials in the password manager, this way it will always be easy to take action with it if needed.

Q14: Do you use a different email address for sensitive or confidential online activities, such as online banking or healthcare services?

Considering that majority of the respondents do not use this security feature the findings suggest that there is a need to emphasise the importance of using separate email addresses for sensitive and non-sensitive online activities, as this can enhance privacy and security. Another possible suggestion is making use of disposable emails for services that are not used on a regular basis.

Q15: How do you typically review and manage the privacy settings on your social media accounts?

Findings highlight the importance of raising awareness about privacy settings and their impact on personal information sharing. Although the majority tend to limit the information shared online it is still important to make use of recommendations that should include promoting the removal or hiding of sensitive details to enhance overall cyber hygiene practices.

Improving cyber hygiene

Q16: What steps have you taken to educate yourself about online security and best practices for cyber hygiene?

According to the findings it is recommended to encourage respondents to explore a variety of educational materials, including online training sessions, publications, and courses. Highlight the significance of consulting experts in this field and gaining knowledge from practical experience. Additionally, initiatives should be undertaken to involve those who are not currently engaged in enhancing their cybersecurity and cyber hygiene by spreading knowledge of the possible hazards.

Q17: How do you educate others, such as friends or family, about online security and cyber hygiene?

Findings demonstrate that respondents engage in a variety of activities to promote online security and cyber hygiene for themselves and others. Providing guidance on effective cybersecurity strategies is crucial to one's own security since the breach of the accounts of their close friends and family can put their personal information in danger as well.

Q18: Have you ever conducted a security examination of your online accounts (verifying the security of the login, checking privacy settings, ensuring that best practices are followed), and if so, what did you learn?

The analysis of the last question examines whether respondents have ever conducted a security examination of their online accounts, and if so, what they learned from the process. The additional information provided by respondents includes insights on the power of the internet, the extent of personal information shared, the use of password manager tools, the realisation of weak security levels, and the discovery of overlooked security features and potential breaches. Based on the results it is possible to outline several recommendations that can help to improve the safety of users' accounts. Users should conduct a security check up regularly, which includes the verification of their credentials security, privacy settings check up, switching the shared data to the private mode and deleting accounts that are no longer used or irrelevant. Raising awareness can potentially motivate users to use password managers and 2FA which will significantly increase their accounts security.

5.2 Interview and OSINT research analysis

Since the OSINT and interview came together with the interview the analysis was combined with addition of the answers from the questionnaire that were discussed during the interview. The findings reveal insights on the personal approach of each respondent as well as outline individual recommendations based on every respondent's cyber hygiene method discussed during the interview.

Respondent 1

The analysis of the interview with the respondent and the data obtained from the OSINT research provided a lot of interesting information and personal experience examples. The respondent actively uses social media and shares considerable personal information online without withholding anything. Despite being cautious about securing their internal home network and using a password manager, they understand that some accounts lack secure policies. They only change passwords and policies when enforced by the app or website which in fact is a good security approach. During the interview, the respondent shared a past incident where reusing a username led to blackmail and professional

challenges. This experience increased their awareness and understanding of the dangers of online information oversharing. The OSINT research revealed accounts on multiple websites, including Facebook, LinkedIn, Twitter, TripAdvisor, GitHub, and Freelancer website accounts which are more than enough to get a clear picture of who this person is. Upon sharing the OSINT findings with the respondent, they expressed surprise at some of the sources and the ease with which accounts were found. They acknowledged the need to use different usernames and delete or remove information from certain accounts to decrease the chances of personal information exposure.

Based on these insights, personalised recommendations for the respondent include:

1. Regularly review and update privacy settings on all online accounts, especially social media platforms, to limit the information being shared publicly.

2. Avoid using the same usernames across multiple different accounts, as this increases the probability of finding different types of account that could potentially put at risk the reputation.

3. Utilisation of a password manager to create unique, strong passwords for all the accounts, even those that are not used on a regular basis.

4. Delete or remove personal information from accounts that are no longer in use.

5. Consider sharing the learned tactics and experiences with close friends and family to raise awareness and encourage proactive measures in maintaining cyber hygiene. This is especially important since if there is a possibility of getting the same information from the accounts of people that are close to this person then their security measures and ways to hide their personal information are getting weaker.

Respondent 2

Based on the interview and OSINT data collection results, the respondent appears to be somewhat aware of the risks associated with their digital identity, they have shared unique stories that made them learn how dangerous it can be to overshare. According to the respondent perception it was possible to find almost all of the social media accounts, those that were not found were either registered under different username, email or did not use

a real name of the respondent. There are still areas where improvements can be made to enhance their overall cyber hygiene.

The following recommendations are provided to address these issues:

1. Creating unique usernames for different platforms can help reduce the risk of personal information being linked across various accounts.

2. While the respondent has already adopted a password manager, it is important to ensure that the passwords generated are strong and unique. There are still some passwords that are not linked to the password manager, but the respondent explained that for them they have a unique strategy. It is still recommended to keep all the passwords in a password manager and only use a unique password that you can remember on the password manager itself that keep all the other credentials for them.

3. As the respondent is active on multiple social media platforms, it is essential to review and update privacy settings frequently to ensure that personal information is only accessible to intended audiences. It is common that social media can update the privacy policy and without taking that into account it can be possible that some personal information might be revealed.

4. The respondent mentioned not deleting old accounts due to the difficulty in doing so related to their home country based accounts. However, it is crucial to take the necessary steps to delete such accounts to reduce the risk of data breaches and minimise the digital footprint. Using the GDPR article 17 rights it is possible to submit a request for an erasure of the account.

5. Lastly, although teaching cybersecurity to older individuals might be challenging, it is crucial to promote digital safety awareness across all age groups since there is a high possibility that similar information about the respondent is shared by others.

Respondent 3

Respondent is an active internet user that has an account on many platforms, including social media, messaging, and coding websites. They have taken some measures to improve their cyber hygiene, such as using multiple email addresses and reducing the amount of personal information shared online. However, some of their habits, like reusing passwords and relying on SMS-based OTP, present opportunities for improvement. Respondent recognised the risks associated with their online presence and expressed a desire to take action to enhance their digital security.

Recommendations based on the respondent's approach:

1. The respondent should avoid reusing passwords across multiple accounts. Instead, they should create unique, strong passwords for each account.

2. Enhance 2FA authentication: Switch from SMS-based OTP to a more secure method such as an push OTP for two-factor authentication, if that is not an option it is also possible to add additional 2FA method on top of the SMS-based OTP.

3. Audit and clean up online presence. The respondent should review all discovered accounts and consider deleting those that are no longer in use or contain sensitive information. Regularly audit online presence to ensure no new risks have emerged.

4. Limit the amount of personal data posted online and adjust privacy settings on social media accounts to control who can access the shared content..

5. Periodically check personal information available online and request the removal of any unwanted or sensitive data, utilising GDPR rights where applicable.

5.3 Combined analysis

5.3.1 Questionnaire groups

General questions

- Educate respondents about the significance of unique, complex passwords.
- Promote the use of password managers for improved password management.
- Raise awareness about the advantages and disadvantages of different OTP methods, emphasising more secure alternatives like hardware-based, software-based, and push OTPs. Implement MFA for additional protection.
- Monitor online accounts for signs of breaches or attacks.
- Continuously update knowledge about evolving threats and cybersecurity best practices.

Data oversharing

- Encourage users to think twice before sharing personal information and to be mindful of potential risks and long-term consequences of oversharing.
- Promote the use of privacy settings on various platforms, allowing users to manage who can view their shared content.
- Emphasise informed decision-making when providing personal information online and stress the significance of understanding potential risks and best practices in online information sharing.
- Suggest the use of anonymous accounts in situations where privacy is a concern.

Data Managing

- Securely erase or format old devices before disposal.
- Encourage use of password managers and encryption software.
- Periodically review, deactivate or delete inactive social media accounts.
- Ensure appropriate privacy settings for active accounts.
- Use separate email addresses for sensitive and non-sensitive activities. Consider using disposable emails for non-regular services.
- Limit personal information shared on social media.

Improving cyber hygiene

- Explore educational materials for cyber hygiene.
- Consult experts and gain practical experience.
- Engage those not currently involved in cybersecurity and cyber hygiene.
- Provide guidance on effective communication strategies for discussing cybersecurity.
- Conduct regular security check-ups of online accounts.

5.3.2 OSINT and Interviews

Respondent 1 recommendations:

- Regularly review/update privacy settings on all online accounts.
- Avoid using same usernames across multiple accounts.
- Utilise password manager for unique, strong passwords.
- Delete/remove personal information from unused accounts.
- Share learned tactics/experiences with friends and family.

Respondent 2 recommendations:

- Create unique usernames for different platforms.
- Ensure strong, unique passwords with password manager.
- Review/update privacy settings frequently on social media.
- Delete old accounts using GDPR article 17 rights. [33]
- Promote digital safety awareness across all age groups.

Respondent 3 recommendations:

- Avoid reusing passwords, create unique/strong passwords for each account.
- Switch from SMS-based OTP to an authenticator app. Add additional OTP on top of the existing one.
- Audit and clean up online presence, delete unused/sensitive accounts.
- Limit personal data posted online, adjust privacy settings on social media.

6 Results based on the research

6.1 Dealing with Existing Personal Information

In today's digital era, managing existing personal information online has become increasingly important due to the potential risks and consequences related to disregarding it. As a result of the extensive use of the internet and social media, our personal information is more accessible than ever before, making it easier for criminals, potential employers, and even acquaintances to obtain sensitive information about us.

The need to protect ourselves from various threats such as identity theft, financial fraud, and harm to our personal and professional reputations highlights the importance of protecting existing personal information online. Failure to manage our digital footprints can expose us to these risks, which can have long-term implications in our lives.

Furthermore, neglecting to handle personal information online might have unanticipated consequences, such as releasing sensitive information to untrustworthy parties or losing control over how we are regarded online. It is critical to identify where your information can be accessible online in order to successfully manage your online presence and personal information. There are several tools available to assist you in searching for and gathering information about your digital identity.

This chapter will introduce to a number of open-source intelligence tools that may be used to follow one’s online presence and collect important information about the digital footprint. The tools are ordered from least capable to most powerful. However, based on the research, it is crucial to realise that all of these tools can produce a distinct outcome, and it is advised that all of the presented tools be explored. The installation guide for the CLI tools is presented at the bottom of the guide.

1. Analyzeid

Analyzeid is a simple internet tool that functions as a social network username checker. By inputting a username, the program collects data and presents a summary of the person's online presence, including sites where the username is already taken, the full name, position, and images linked with the username. This tool is a great place to start when learning about your digital identity. [25]

2. Idcrawl

Idcrawl is another simple internet tool that may help you identify websites that utilise your username as well as any email addresses associated with the username. Idcrawl assists you in identifying locations where your personal information may be susceptible by offering a comprehensive list of websites and email addresses related with your digital identity. [26]

3. Whatsmyname

Whatsmyname is a simple website tool that accepts a username as a parameter and returns a list of websites that use that identity. The application may also categorise and filter the results by category, making it easier to manage the results. [27]

4. Sherlock

Sherlock is a command-line utility that works on Linux, MacOS, and Windows. By entering a username, the program returns a list of websites with links to the user's account, as well as extra output formatting parameters. This tool provides a more detailed study of your digital footprint. [28]

5. Maigret

Maigret is yet another command-line utility for Linux and MacOS. When you enter a username, the program generates a list of websites that use that username and delivers a detailed report for each site, including available and retrievable information. This tool provides a more detailed perspective of your online presence, allowing you to understand and manage your digital identity more effectively. [29]

6. Holehe

Holehe is a command-line utility that may be used on Linux and MacOS to retrieve information via email utilising the forgotten password function. The program gathers extra information and presents a list of websites where the email is utilised. Holehe may also be integrated into Python applications to provide filters and customised output. [30]

Using these tools, it is possible create a list of information that includes one’s social media accounts, personal information, and email addresses. It is important to note that not all of

the information acquired will be relevant to one persona; there may be accounts with the same name or username that is similar to the one used to conduct the research. Manual work will be required to filter these accounts out and focus just on the accounts that are certainly belong to one person. The following phase will be advanced research on your own accounts.

Credentials Protection

To begin protecting credentials of the accounts, it is a must first outline the current strategies. It is very advised to begin utilising a password manager right away. Users can use a password manager to keep all their social media accounts' credentials in one place. The ability to save unique passwords for your accounts in one secure location is the primary feature of the password manager. This ensures that even if one of your accounts' credentials is compromised in a data breach or during a cybersecurity attack, only one of your accounts will be vulnerable. Furthermore, password manager features can assist you in creating the most unique passwords that you will not need to remember, and all passwords can be safeguarded with a single master password. To take care of the accounts you've discovered, you'll need to manually go through each one and add it to your password manager, as well as update the password.

Two-Factor Authentication

Having a safe and unique password may not be sufficient to ensure the security of your accounts. It is necessary to implement 2FA to increase security. This feature is accessible on the majority of online accounts and can be enabled with a few clicks. 2FA employs one-time passwords, which require the authentication process to consider a factor other than your password. There are various types of OTP available:

- SMS OTP.
- Email OTP.
- Hardware-based OTP.
- Software-based OTP.
- Push OTP.

Having at least one method enabled ensures that even if your password is compromised in a data breach, it will be more difficult to log into your accounts. Hardware-based, software-based, and push OTPs are the most secure since they require direct access to the device or app, whereas SMS or email OTP can be accessed by criminals via SMS attacks or accessing your email service account.

Username and Email Vulnerabilities

Now that our accounts have been secured, we can focus on the information stored on them. When we used OSINT tools to obtain information about our persona in the first stage, we saw how simple it can be to gather a significant amount of information using only our email or username. Given that this information is searchable by anyone on the internet, we must ensure that we are using numerous different emails and usernames. Dividing the emails by the category of the service used might be the easiest method to implement, however it still might help to use completely different usernames for each service. This method ensures that even if someone obtains a portion of our information, they will not be able to obtain the entire picture, perhaps saving you from stalking, digital identity theft, or social engineering attempts.

Privacy Settings

The following stage in our tutorial involves examining and adjusting the privacy settings on online accounts. It is critical for managing personal information to evaluate and update privacy settings on online accounts on a regular basis. This ensures that our data is only accessible to those with whom we wish to share it, decreasing the danger of illegal access or information misuse.

If there is no way to make the information private it is necessary to analyse the publicly shared information and decide whether it is worth keeping online. In such cases, the simplest solution would be to remove the data by hand. However, if traces of information remain after manual erasure, it is time to invoke the General Data Protection Regulation (GDPR) rights, which give individuals the right to request the deletion of their personal information in certain instances. Article 17, sometimes known as the "right to be forgotten," empowers individuals to request that organisations erase personal data about them. [33]

Device Disposal

It is important to mention that the proper device disposal methods should be used in order to make sure that none of the information we have stored on our devices is forgotten. Since in modern world we tend to change devices every few years we cannot neglect cleaning the old devices. With media data it is obvious that it should be transferred to a new device, however what usually gets ignored is the presence of various accounts that are forgotten after the device is not used anymore. Taking care of the accounts on the device and making sure that all of them are transferred on the new device or deleted is more than enough at this step.

Knowledge and Awareness

As the digital world continues to advance rapidly, users must regularly invest time and effort in educating themselves about the latest risks and effective strategies to safeguard their personal information. This can be achieved through various means, such as enrolling in online courses, subscribing to industry newsletters, and following reputable cybersecurity blogs and experts on social media. Furthermore, users should not only focus on enhancing their knowledge but also ensure that they actively share their learnings with their friends, family, and colleagues. By doing so, we can ensure that our closed ones will be able to maintain their own cyber hygiene and not expose the personal data about us that could be obtainable through accounts of others.

Remember that proper cyber hygiene entails evaluating and updating your privacy settings on a regular basis, monitoring your online accounts for indicators of breaches or assaults, and constantly updating software and devices to be secure against emerging threats. These continuing initiatives help to protect your digital identity and reduce your vulnerability to cyber threats.

6.1.1 Installation and usage guide

To make use of the mentioned CLI tools it would require installing them on your machine. It is recommended to use LinuxOS or MacOS since the installation on these systems the installation takes as little as few minutes and does not require any additional steps. Make sure that you have an updated version of Python installed. [34]

Sherlock

Clone the repository to the CLI command line

```
git clone https://github.com/sherlock-project/sherlock.git
```

Change the working directory to sherlock

```
cd sherlock
```

Install the requirements

```
python3 -m pip install -r requirements.txt
```

Usage

```
python3 sherlock username
```

Maigret

Clone the repository to the CLI command line

```
git clone https://github.com/soxoj/maigret
```

Change the working directory to maigret

```
cd maigret
```

Install the requirements

```
pip3 install -r requirements.txt
```

Usage

```
./maigret.py username
```

Holehe

Clone the repository to the CLI command line

```
git clone https://github.com/megadose/holehe.git
```

Change the working directory to maigret

```
cd holehe
```

Install the tool

```
python3 setup.py install
```

Usage

```
holehe test@gmail.com
```

6.2 Cyber Hygiene Best Practices

After taking the necessary steps discussed earlier to manage your existing personal information and improve your cyber hygiene, it's essential to maintain the security of your accounts by following best practices consistently. This guide provides a comprehensive list of cyber hygiene best practices that can help you protect your digital identity and ensure the ongoing safety of your accounts.

- Using strong, unique passwords for each account new account to prevent unauthorised access.

- Advanced step to secure the most sensitive accounts can be enabling MFA to add an extra layer of security to your accounts.

- Making sure to keep in mind that if the account of separate category is created it is better to create a new email and username. If the service or social media will not be used on a regular basis it should be considered to use disposable email addresses to protect primary emails from spam and phishing attempts.

- Regular review of the privacy settings on social media platforms to control who can access your personal information. It should be taken into account that services constantly change the privacy security settings.

- Periodical review of online accounts for signs of unauthorised access or suspicious activity. Additional check of the credit report and financial statements for signs of identity theft or fraud is also a good cyber hygiene input.

- Follow credible sources, attend webinars, and participate in forums to stay up to date on the newest cybersecurity risks, trends, and best practices. Share your information and experiences with friends and family to assist them in improving their own cyber hygiene.

By following these cyber hygiene best practices, one can keep their accounts secure, preserve digital identity, and reduce chances of becoming a victim of cyber threats. Users must keep in mind that cyber hygiene is an ongoing activity, and remaining knowledgeable and vigilant is critical to protecting personal information in the ever-changing digital world.

7 Summary

This thesis aimed to address cyber hygiene in the digital society, focusing on the dangers of personal information oversharing and offering a solution guide for users. The research provided valuable insights and achieved the initial goals.

The literature review covered the current state of cyber hygiene, exposed digital identity profile dangers, and open-source intelligence (OSINT) tools. This foundation highlighted the relevance and importance of improving personal cyber hygiene to mitigate potential risks.

The practical part implemented a cyber hygiene awareness questionnaire, interviews, and OSINT data collection, allowing for an in-depth analysis of user behaviour, perceptions, and awareness regarding their digital presence and associated risks.

The findings revealed a general lack of knowledge among users about their online exposure and potential risks. Many users have implemented basic cyber hygiene measures, but there is room for improvement. OSINT data collection demonstrated the ease of obtaining personal information and potential hazards. Based on these findings, recommendations and best practices were developed. The thesis also emphasised understanding and exercising GDPR rights to manage existing online personal information.

In conclusion, this thesis provided significant insights on personal cyber hygiene and practical actions for users to improve digital security. It raises awareness of the problems related to personal information oversharing and offers effective solutions while laying the foundation for future research in cyber hygiene and digital identity protection.

This thesis has certain limitations, such as the small sample size for questionnaires and interviews, which may impact the generalisability of the findings. Future research should expand the sample size and explore the interplay between personal and professional digital identities. While this thesis focused on OSINT tools for data collection and analysis, future research could explore integrating various data collection methods to provide a more comprehensive understanding of users' online behaviour and potential risks. Addressing these limitations will contribute to developing more effective strategies for ensuring a secure online environment and fostering a safer digital landscape.

References

[1] C. Brook, “What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More,” 21 12 2022. [Online]. Available: https://www.digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more#:~:text=Cyber%20hygiene%20is%20a%20reference,could%20be%20stolen%20or%20corrupted. [Accessed 13 April 2023].

[2] Webroot, “How Do I Create a Strong and Unique Password?,” [Online]. Available: https://www.webroot.com/us/en/resources/tips-articles/how-do-i-create-a-strong-password. [Accessed 5 April 2023].

[3] Microsoft, "What is two-factor authentication?," [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-two-factor-authentication-2fa. [Accessed 11 April 2023].

[4] M. E. Velasquez, "How Oversharing on Social Media Affects Your Privacy," 23 December 2022. [Online]. Available: https://www.keepersecurity.com/blog/2022/12/23/how-oversharing-on-social-media-affects-your-privacy/. [Accessed 5 April 2023].

[5] M. Rouse, "Digital Identity," 4 June 2012. [Online]. Available: https://www.techopedia.com/definition/23915/digital-identity. [Accessed 3 April 2023].

[6] Federal Trade Commission Consumer Advice, "Identity Theft," [Online]. Available: https://consumer.ftc.gov/features/identity-theft. [Accessed 04 April 2023].

[7] R. Awati, "Cyberstaling," August 2021. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/cyberstalking. [Accessed 4 April 2023].

[8] L. Rainie, S. Kiesler, R. Kang and M. Madden, "Anonymity, Privacy, and Security Online," 5 September 2013. [Online]. Available: https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/. [Accessed 4 April 2023].

[9] European Commission, "Open-source intelligence," 2 May 2022. [Online]. Available: https://data.europa.eu/en/publications/datastories/open-source-intelligence. [Accessed 2 2023 April].

[10] J. Nordine, "OSINT Framework," [Online]. Available: https://osintframework.com/. [Accessed 10 April 2023].

[11] OSINT Central, "How is OSINT affected by GDPR?," [Online]. Available: https://osint-central.com/osint-gdpr/. [Accessed 12 April 2023].

[12] H. Asker and A. Tamtam, "Knowledge of Information Security Awareness and Practices for Home Users: Case Study in Libya," 8 February 2023. [Online]. Available: https://eujournal.org/index.php/esj/article/download/16424/16285. [Accessed 5 April 2023].

[13] A. A. Cain, M. E. Edwards and J. D. Still, "An exploratory study of cyber hygiene behaviors and knowledge," 2018. [Online]. Available: https://par.nsf.gov/servlets/purl/10083310. [Accessed 10 April 2023].

[14] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," June 2010. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167404809001436?via%3Dihub. [Accessed 7 April 2023].

[15] M. Zwilling, D. Lesjak, Ł. Wiechetek and G. Klien, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," January 2022. [Online]. Available: https://www.researchgate.net/publication/339273589_Cyber_Security_Awareness_Knowledge_and_Behavior_A_Comparative_Study. [Accessed 10 April 2023].

[16] C. Hadnagy, Social Engineering, John Wiley &Sons , 2010 .

[17] Microsoft, "Protect yourself from phishing," [Online]. Available: https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44. [Accessed 10 April 2023].

[18] Fortinet, "What Is Pretexting?," [Online]. Available: https://www.fortinet.com/resources/cyberglossary/pretexting. [Accessed 10 April 2023].

[19] Global South Dialogue on Economic Crime, "CYBERSECURITY AND FINANCIAL CRIMES," [Online]. Available: https://gsdec.network/8374/cybersecurity-and-financial-crimes/. [Accessed 10 April 2023].

[20] Javelin, "Pandemic Ushers in Identity Fraud Scams," 21 March 2021. [Online]. Available: https://javelinstrategy.com/press-release/total-identity-fraud-losses-soar-56-billion-2020. [Accessed 10 April 2023].

[21] Javelin, "Identity Fraud Losses Total $52 Billion in 2021, Impacting 42 Million U.S. Adults," 29 March 2022. [Online]. Available: https://javelinstrategy.com/press-release/identity-fraud-losses-total-52-billion-2021-impacting-42-million-us-adults. [Accessed 10 April 2023].

[22] Kaspersky, "What is a digital footprint? And how to protect it from hackers," [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint. [Accessed 10 April 2023].

[23] netreputation, " What is Personal Online Reputation Management?," [Online]. Available: https://www.netreputation.com/what-is-personal-online-reputation-management/. [Accessed 11 April 2023].

[24] S. Hinduja and J. W. Patchin, "Bullying, Cyberbullying, and Suicide," July 2010. [Online]. Available: https://www.researchgate.net/publication/45289246_Bullying_Cyberbullying_and_Suicide. [Accessed 10 April 2023].

[25] Analyzeid, “Username Checker,” 14 June 2020. [Online]. Available: https://analyzeid.com/username/. [Accessed 16 April 2023].

[26] IdCrawl, “Username Search,” [Online]. Available: https://www.idcrawl.com/username. [Accessed 16 April 2023].

[27] OSINT Combine, “WhatsMyName Web,” [Online]. Available: https://whatsmyname.app/. [Accessed 16 April 2023].

[28] S. Dushantha, “sherlock-project / sherlock,” [Online]. Available: https://github.com/sherlock-project/sherlock. [Accessed 16 April 2023].

[29] S. Dushantha, “soxoj / maigret,” [Online]. Available: https://github.com/soxoj/maigret. [Accessed 17 April 2023].

[30] Palenath, "megadose / holehe," [Online]. Available: https://github.com/megadose/holehe. [Accessed 17 April 2023].

[31] S. M. Ross, Introductory Statistics, Academic Press, 2017.

[32] J. S, "What is Personal Online Reputation Management?," 1 April 2023. [Online]. Available: https://www.netreputation.com/what-is-personal-online-reputation-management/. [Accessed 10 April 2023].

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Andrei Boitsov

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Personal Cyber Hygiene: Mitigating the Risks of Exposed Digital Identity Profiles", supervised by Toomas Lepikult and co-supervised by Valdo Praust.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

14.05.2023

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Questionnaire results

An overview of the 18-question questionnaire is presented in Tables 2 - 19.

Q1: On a scale of 1-5, with 1 being the least secure and 5 being the most secure, how would you rate your personal cybersecurity?

Table 2 – Security scale

Response - single choice	Number of Respondents
1	0
2	8
3	49
4	39
5	4

Q2: At what point do you think it becomes necessary to change a password?

Table 3 – Password change

Response - multiple choice with “Other”	Number of Respondents
Every 90 days - as a precaution	29
After a breach/cyberattack	54
When suspicious activity is noticed	83
After using a public computer	36
Responses added by respondents	
After request given by a system	2
Never with 2FA	2

Q3: How do you typically choose passwords for your online accounts?

Table 4 – Password choise

Response - single choice with “Other”	Number of Respondents
I use the same password for multiple accounts	38
I use simple passwords that are easy to remember	2
I use complex passwords that are difficult to guess	22
I use a password manager to store unique passwords	30
Responses added by respondents	
I have a unique strategy that I use	8

Q4: What one-time password method is preferred in your opinion?

Table 5 – OTP method

Response - multiple choice with “Other”	Number of Respondents
SMS OTP	51
Email OTP	32
Hardware-based OTP	19
Software-based OTP	41
Push OTP	22
Responses added by respondents	
I do not know what it means	1

Q5: Have you ever experienced a data breach or a cyber attack?

Table 6 – Data breach experience

Response - single choice	Number of Respondents
Yes, multiple times	15
Yes, once	31
No, but I know someone who has	35
No, I have never experienced a data breach or a cyber attack	19

Q6: How has your experience with data breaches or cyber attacks, either directly or indirectly, influenced your approach to sharing personal information online, and do you believe your current practices are sufficient to minimise the risk of future incidents?

Table 7 – Data breach influence

Response - single choice with “Other”	Number of Respondents
I am more aware of the risks, and I've made some adjustments to my online habits	27
I now pay more attention to security measures and privacy settings on the platforms I use	16
I understand evolving threats and I am thinking of improving my practices	14
I've become much more cautious and selective about the information I share online	23
No, I continue to share information online as before, but I'm aware of the potential risks	16
Responses added by respondents	
I am pretty confident that with my security the attack is not possible	4

Q7: Have you ever shared personal information online and then regretted it afterward?

Table 8 – Personal information oversharing

Response - single choice	Number of Respondents
Yes, this happened multiple times	20
Yes, just once	25
No, this never happened to me	55

Q8: How often do you share personal information, such as your location or activities, on social media?

Table 9 – Personal information sharing frequency

Response - single choice	Number of Respondents
Every day, I am not afraid of sharing my personal information	6
A couple times a week, I like to be active online	7
A couple times a month	18
A few times a year, might make a post somewhere	37
Never, I avoid sharing personal information when it is not strictly required	32

Q9: How do you typically handle requests for personal information from websites or apps?

Table 10 – Requests handling

Response - multiple choise	Number of Respondents
I provide all requested information	5
I provide only the information that is required	67
I provide false information to protect my privacy	18
I avoid providing personal information whenever possible	55
I check the website's or app's privacy policy before providing personal information	10

Q10: How do you typically decide what personal information to share or withhold online?

Table 11 – Sharing preferences

Response - multiple choice with “Other”	Number of Respondents
I review the privacy settings on each platform to manage who can view my shared content	17
I evaluate the risks of sharing sensitive information	49
I consider future consequences before sharing	47
I use anonymous accounts when needed for privacy	31
I trust my instincts and comfort level when sharing	45

Q11: How do you dispose of old devices containing personal information, such as smartphones or laptops?

Table 12 – Device disposal

Response - single choice with "Other"	Number of Respondents
I sell the device after erasing all the data from it	41
I physically destroy the device	9
I just keep the device around me without disposing the data or the device itself	37
I am not sure how to dispose of old devices containing personal information	7
Responses added by respondents	
I keep device after formatting	6

Q12: How do you store and manage your personal information on your devices, such as passwords, financial information, or identification documents?

Table 13 – Storing and managing personal information

Response - single choice	Number of Respondents
I use programs that have their own password protection such as a password manager	47
I keep all my personal information in an encrypted folder or file on my device	17
I prefer to keep it all in a physical folder or file that I keep in a secure location	11
I have not given much thought to that	25

Q13: Do you have any social media accounts that you are no longer using?

Table 14 – Old social media accounts

Response - single choice	Number of Respondents
Yes, a couple	52
No, I do not register an account in a social media if I am not using it often	32
I had an account but I took action and deleted it	16

Q14: Do you use a different email address for sensitive or confidential online activities, such as online banking or healthcare services?

Table 15 – Different email

Response - single choice	Number of Respondents
Yes, I use a separate email address that is dedicated only to sensitive activities	46
I use the same email address for all my online activities, I find it easier to manage	29
I have not considered using a different email address for sensitive activities	25

Q15: How do you typically review and manage the privacy settings on your social media accounts?

Table 16 – Privacy settings review

Response - multiple choice with “Other”	Number of Respondents
I regularly update my privacy settings to ensure I'm comfortable with the info being shared	22
I limit the personal info I share by providing only basic information	75
I remove or hide certain details, such as my birthdate or home address	55
I don't use social media, so I don't have any privacy settings to manage	8

Q16: What steps have you taken to educate yourself about online security and best practices for cyber hygiene?

Table 17 – Cyber hygiene education

Response - multiple choice with "Other"	Number of Respondents
I have attended online security training sessions	28
I regularly read about online security	33
I have taken online courses or certifications related to cybersecurity	11
I am taking advice from professionals in the field	50
I am actively learning from my own mistakes	52
I am not trying to improve my cybersecurity and -hygiene	14

Q17: How do you educate others, such as friends or family, about online security and cyber hygiene?

Table 18 – Education of others

Response - multiple choice	Number of Respondents
I share articles on social media that educate about online security	19
I have helped friends or family to make their accounts secure	48
Provided guidance on best practices for password management and data protection	31
I have recommended specific cybersecurity apps to others	29
I explained to my friends and family dangers of data oversharing online	50
I have not yet educated others about online security, but I am interested in doing so	16
I do not think it is needed	2

Q18: Have you ever conducted a security examination of your online accounts (verifying the security of the login, checking privacy settings, ensuring that best practices are followed), and if so, what did you learn?

Table 19 – Security examination

Response - single choice with “Other”	Number of Respondents
No	74
Yes, with no additional information provided	6
Yes, with additional information provided below	20
Internet is a powerful tool and any information that was shared can be found online	
I was sharing more information that I was comfortable with	
I have used password manager tools to run a security check	
My security level appeared to be weak	
Found potential breaches from online resources	
I have not learned new information	
There are a lot of options that are overlooked by me	
Learned that there are a lot of security features I can configure	
I googled myself	
I have used a password manager to check my security	
There are a lot of options to configure	
I have learned that my data was leaked several times	
I have fixed potential problems	
Learned that there are mechanisms that can be enabled	
I only do it if the system prompts me to do so	
Learned that I am using a lot of similar passwords	
I noticed that enabling 2FA can benefit my cybersecurity	
Learned that it is best to be on the safe side, but not drive yourself insane with it	
I use a lot of similar passwords	
Learned that I only properly secure my financial accounts	

Appendix 3 – OSINT research results

Table 20 – Respondent #1 findings

Website tools	CLI tools
Analyzeid	Sherlock
Blogspot.com	https://blogspot.com https://hub.docker.com https://www.fiverr.com https://www.freelancer.com https://freesound.org https://www.g2g.com https://www.github.com https://gitlab.com https://www.instagram.com https://medium.com https://t.me https://tiktok.com https://www.tradingview.com https://twitter.com
Idcrawl	Maigret
https://tripadvisor.com https://github.com https://twitter.com https://facebook.com https://tiktok.com https://linkedin.com	https://www.shutterstock.com https://t.me fullname https://github.com https://www.tradingview.com https://www.freelancer.com company role location https://www.tiktok.com https://www.pinterest.com https://twitter.com https://www.fiverr.com

Website tools	CLI tools
	https://blogspot.com https://www.strava.com https://tripadvisor.com https://www.picuki.com https://imginn.com https://hub.docker.com https://gitlab.com https://freesound.org Interests: coding, photo, sharing, music, messaging, stock, trading, freelance, video, art, shopping, blog, forum, travel
Whatsmyname	Holehe
https://hub.docker.com https://github.com https://t.me https://freesound.org https://www.tiktok.com https://www.tradingview.com https://www.tripadvisor.com https://twitter.com https://gitlab.com https://giters.com	Amazon.com ebay.com evernote.com freelancer.com spotify.com
Manual	
Travel history Brother Origin country Full education and working background Skype	

Table 21 – Respondent #2 findings

Website tools	CLI tools
Analyzeid	Sherlock
https://www.deviantart.com https://www.linkedin.com https://www.scribd.com https://slack.com/ https://www.myfitnesspal.com https://www.periscope.tv https://www.pinterest.com https://weheartit.com	https://ask.fm https://www.cgtrader.com https://community.eintracht.de https://www.gumroad.com https://hackerrank.com https://www.openstreetmap.org https://www.strava.com https://tsevincek.deviantart.com https://www.fiverr.com http://en.gravatar.com https://www.periscope.tv https://sketchfab.com https://open.spotify.com https://t.me https://twitter.com https://www.wattpad.com https://osu.ppy.sh
Idcrawl	Maigret
https://www.facebook.com https://www.pinterest.com https://spotify.com	https://www.pinterest.com https://www.strava.com https://ask.fm https://jsfiddle.net https://t.me https://www.fiverr.com https://www.pinterest.com https://www.wattpad.com http://en.gravatar.com gravatar_email_md5_hash https://osu.ppy.sh https://www.gog.com

Website tools	CLI tools
	https://picsart.com https://vsco.co Interests: photo, messaging, shopping, art, sharing, forum, gaming, reading, writing
Whatsmyname	Holehe
http://en.gravatar.com https://www.myinstants.com https://omlet.gg https://www.pinterest.com https://www.periscope.tv https://picsart.com https://t.me https://www.wattpad.com	https://pinterest.com https://lastpass.com https://discord.com https://pinterest.com https://twitter.com https://spotify.com
Manual	
Family picture Email was found using md5 hash Profile picture with face Languages spoken Part of them phone number Archived Google Plus account 9 data leaks Gaming account	

Table 22 – Respondent #3 findings

Website tools	CLI tools
Analyzeid	Sherlock
https://www.paypal.com https://www.reddit.com	https://kik.me https://www.snapchat.com https://t.me https://archive.org https://ask.fm https://www.codecademy.com https://www.g2g.com https://www.github.com https://www.grailed.com https://www.instagram.com https://www.reddit.com https://apps.runescape.com https://tiktok.com https://www.twitch.tv https://twitter.com https://www.mercadolivre.com
Idcrawl	Maigret
https://github.com https://www.instagram.com https://twitter.com https://www.facebook.com https://www.reddit.com https://www.tiktok.com https://www.twitch.tv https://www.snapchat.com	https://gist.github.com https://www.twitch.tv https://www.reddit.com https://github.com https://www.tiktok.com https://www.pinterest.com https://www.freelancer.com https://www.strava.com https://nitter.kavin.rocks https://www.picuki.com https://www.facebook.com https://www.codecademy.com https://imginn.com

Website tools	CLI tools
	https://steemit.com https://ask.fm https://t.me http://.weebly.com https://lan.op.gg https://www.pixwox.com Interests: photo, messaging, art, sharing, business, forum, coding, news, streaming, discussion, video, art, freelance, education, networking
Whatsmyname	Holehe
https://ask.fm https://www.depop.com https://giters.com https://github.com https://ws2.kik.com https://www.reddit.com https://steemit.com https://www.tiktok.com https://www.palnet.ioz https://twitter.com https://t.me	No data found
Manual	
Facebook account Personal relationships from the past were found on one of the websites 2 usernames Middle name Origin country Sister Companion	