LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Job applicant's information security – Instant messaging applications as a part of virtual recruitment

Savolainen, Ville

2017 Leppävaara

LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Laurea-ammattikorkeakoulu

Job applicant's information security – Instant messaging applications as a part of virtual recruitment

Ville Savolainen
Degree Programme in Security Management Bachelor's thesis
November, 2017

Laurea University of Applied Sciences
Degree Programme in Security Management
Bachelor's Thesis

Abstract

Ville, Savolainen

Job applicant's information security – Instant messaging applications as a part of virtual recruitment

Year 2017 Pages 31

The purpose of this research-based development project is to study how job applicants could ensure their personal information security and data privacy while using three different instant messaging applications (Adobe Connect, Skype for business & Slack) during virtual recruitment processes. The objective was to gather instructions and guidelines for job applicants, and to create a short information security guidebook based on the results of this study. This thesis was conducted in co-operation with Laurea UAS as a part of project "Social media and it's equipments as a way of working-life".

The theoretical framework is based on several information security management textbooks, earlier researches and information that were gathered from the developers of the researched applications. The framework defines what information security is and the basic characteristics of information. It contains also discussion relating to theories on information security behavior of computer users, and lastly an introduction to the studied instant messaging applications.

The research methods used in the study were secondary data analysis and participant observations. Information security threats and instructions were found and analyzed during the secondary data analysis. Observations were conducted in order to find specific instructions for the safe usage of the instant messaging applications.

The study found ways to increase the information security awareness of job applicants by introducing common threats and possible consequences if they would occur. The results also included technical and non-technical instructions for preventing the threats from happening, and also instructions on how to share personal data or other content safely while using the three instant messaging applications. The guidebook was created in a way that it follows these same themes; first introducing the threats in order to raise awareness, secondly giving general instruction on how to prevent them and lastly giving applications specific instructions on how to safely share content during virtual recruitment processes.

Keywords: Information security, recruitment, virtual recruitment, privacy

Laurea University of Applied Sciences **Tiivistelmä**
Degree Programme in Security Management
Bachelor's Thesis

Savolainen, Ville

Työnhakijan tietoturva – Pikaviestintäsovellusten käyttö osana virtuaalista rekrytointia

Vuosi 2017 Sivumäärä 31

Tämän tutkimuksellisen kehittämistehtävän tarkoituksena on tutkia miten työnhakijat voisivat varmistaa oman tieoturvansa, sekä tietosuojansa koskemattomuuden virtuaalisten rekrytointiprosessien aikana, joissa käytetään kolmea pikaviestintäsovellusta (Adobe Connect, Skype for Business ja Slack). Projektin tarkoituksena oli kerätä työnhakijoille tietoturvaohjeistuksia, sekä luoda lyhyt tietoturvaopas. Tämä opinnäytetyö on tehty yhteistyössä Laurea amk:n kanssa osana ”Someta duuniin”-hanketta.

Työn teoreettinen tietoperusta pohjautuu useisiin alan oppikirjoihin, aikaisempiin tutkimuksiin, sekä tutkittujen sovellusten kehittäjiltä saatuihin tietoihin. Tietoperusta määrittelee tietoturvan ja tiedon keskeiset ominaisuudet. Myös käyttäjien tietoturvakäyttäytymiseen liittyvää teoriaa on esitetty tässä vaiheessa, sekä viimeiseksi on määritelty tutkittujen pikaviestintäsovellusten ominaisuuksia.

Tutkimusmenetelminä käytettiin kirjallisuus-/aineistokatsausta, sekä osallistuvaa havainnointia. Rekrytointiin liittyvät tietoturvauhat, sekä niiden ennaltaehkäisyyn käytetyt keinot selvitettiin ja analysoitiin aineistokatsuksen aikana. Havainnointia käytettiin, jotta voitiin muodostaa pikaviestintäsovelluksiin liittyviä ohjeistuksia.

Tutkimuksen tuloksena löydettiin keinoja, joilla voidaan nostaa työnhakijoiden tietoturvatietoisuuden tasoa, kuten yleisten uhkien esittelyä ja tiedottamista niiden seuraumuksista. Tulokset sisältävät myös sekä teknisiä, että yleisiä neuvoja, joiden avulla voidaan ennaltaehkäistä yleisimpiä uhkia. Tulosten avulla voitiin myös muodostaa sovelluskohtaisia ohjeistuksia siitä, miten niitä käyttämällä voi jakaa sisältöä turvallisesti. Tietoturvaopas luotiin siten, että sen sisältö noudatti näitä samoja teemoja; tietoturvauhat ja niiden seuraumukset esitellään aluksi tietoisuuden lisäämiseksi, tämän jälkeen esitellään yleisiä tapoja uhkien ennaltaehkäisyyn, ja viimeiseksi esitellään sovelluskohtaiset ohjeistukset.

Contents

1 Introduction

This thesis studies how job applicants could ensure their information security during virtual recruitment process while using three instant messaging applications, and how they could share files safely with these applications. The project is conducted as a functional study, and it is a part of project named; "Social media and it's equipments as a way of working-life", which is implemented by Laurea UAS in co-operation with other educational institutions. The end product of this thesis is an information security guidebook that is meant for job applicants.

Digitalization is spreading rapidly into many different aspects of our personal lives and it also has it's affects into business environment. Finnish government (2016) has lined the development of digital business environment to be one of it's five goals in the digitalization, experimentation and deregulation-project. This brings us to the fact that digitalization will reach into new aspects of our working environments, and it is also possible that virtual recruitment process might be a norm in the future.

The reason why this thesis is conducted is simply due the fact that Information security and data privacy are very important aspects of recruitment processes, especially when the whole process is done online. Recruitment is very extensive operation; there might be several persons processing our personal data and it might be restored in many different ways (Imppola 2016). We can all imagine the amount of new threats that are created when the whole process is developed into a virtual form. It would be in the best interests of both employers and job applicants that the processed data is being kept as secure and private as possible, as well as making sure that it won't get into wrong hands during the process.

If the data that is processed during the recruitment process gets breached due either the employer's or job applicant's failure of taking care of their information security, the consequences might get extensive for both of them. Since it is the applicant's personal data the gets breached, it is possible that they might later be victims of such crimes as identity theft or other misuse of the data, which can possibly lead to financial or reputational harm. The employers might also get legal consequences and sanctions as Finnish legislation sets some basic standards for information security and data privacy for them. The Finnish constitutional law states the general right for privacy which ensures that everyone has right to keep their personal data private. The more specific guidelines for ensuring information security during recruitment are mainly stated in The Act on the Protection of Privacy in Working Life (759/2004) and The Personal Data Act (523/1999). Also the soon implemented EU's General Data protection Regulation (Regulation (EU) 2016/679) gives the employers incentives to au-

dit the information security and data protection procedures, and make sure that they are set into the level that the new legislation requires.

1.1 Purpose and goals

The purpose of the thesis is to research how job applicants could ensure their personal information security and data privacy while using three different instant messaging applications (Adobe Connect, Skype for business & Slack) as a part of recruitment. More closely which factors should be taken into consideration from the point of view of information security when they attend into virtual job interviews or meetings.

Virtual recruitment is a broad topic and there are vast amounts of different applications that can be used for arranging online meetings but all of them cannot be studied within one thesis. The three applications; Adobe Connect, Skype for Business and Slack were chosen earlier to be the ones that are researched more broadly during the whole "Social media and its equipments as a way of working-life" –project, so it is only natural to narrow this thesis into them. It is also important to mention that these applications are already well known and used by many employers and job applicants; it might be more convenient for them to attend into the process if they are already familiar with the applications.

The goal is to gather instructions for job applicants on how to share all the relevant information and files without compromising their information security. The end product of this project will be an information security related guidebook for job applicants.

1.2 Background

The project "Social media and it's equipments as a way of working-life" is executed by Tampere University of applied sciences in co-operation with Laurea UAS, Lapland UAS and University of Eastern Finland. The particular Client of this thesis is Laurea University of Applied sciences, which's main responsibility in the project is to develop virtual encounters in order to bring employers and job applicants together.

The project aims to ease recruiting and employment for University and UAS students by developing career training and recruitment via social media. The purpose is to increase the share of social media in the employment and recruiting processes. The idea is to develop these topics from four different points of views:

1. The point of view of students; Developing abilities to use social media as a tool to get employed and the usage of other digital tools so that they can bring forward their skills and get visibility in the eyes of employers.
2. The point of view of educational institutions; developing abilities to use social media as a tool for career training.
3. The point of view of employers; developing the abilities to use social media as tool for recruitment.
4. The national point of view; Developing abilities and services that can be utilized in all of the third degree educational institutions.

The goal of the whole project is to find solutions to three main themes; the employment of university and UAS students, developing competences for virtual encounters, and digitalization of the career training programs of educational institutes. This thesis is tied to Laurea's goal of developing virtual encounters.

1.3 Virtual recruitment process

The concept of virtual recruitment that is being developed during the "Social media and it's equipments as a way of working-life" –project is defined so that the whole process of hiring new personnel is done online. The idea is to organize an online recruitment event where the organizer is in charge of the online infrastructure (platforms and setting up the messaging application). Employers and applicants are the ones who are invited into the event by the organizers. The developed concept is shared into 4 different stages on which both employers and applicants has their own tasks and functions:

1. Tasks before the event/interviews
2. Logging into the virtual recruitment event and testing the microphones, webcams etc. (Adobe Connect, Skype for Business or Slack)
3. Virtual group interview
4. Logging out from the event and decision on hiring.

The four stages are introduced in figure 1 below. As the figure shows, during the first stage job applicants prepare to introduce themselves by creating e-portfolio or CV, and goes through the guidelines of attending to online recruitment events/interviews given by the organizer of the event. The employers also go through the organizer's guidelines and prepare to lead the interviews.

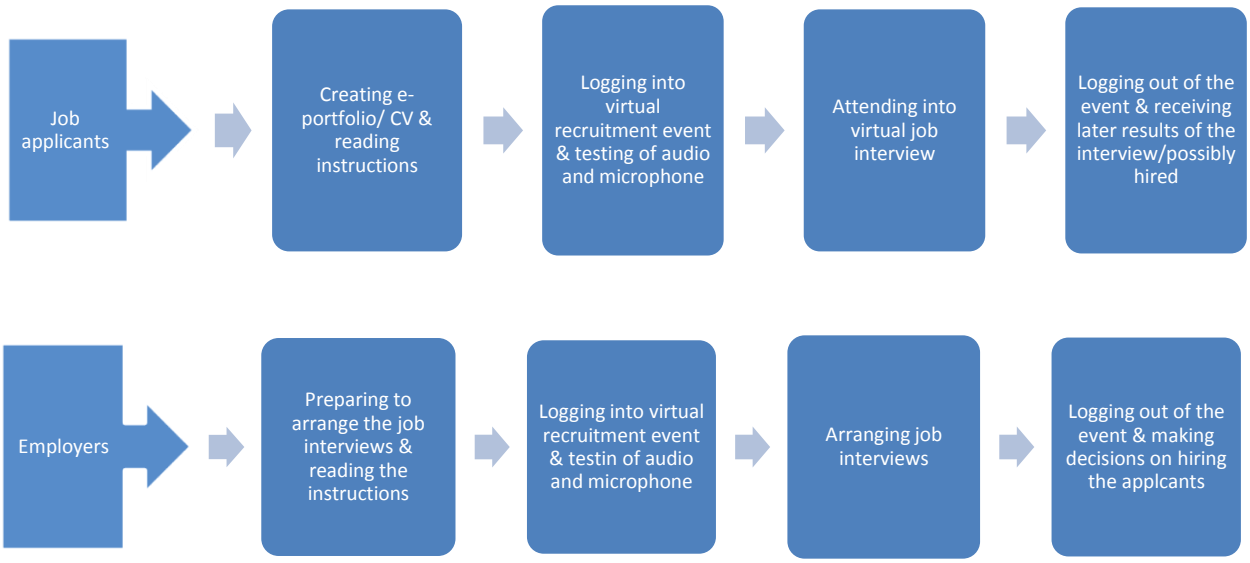

Figure 1: Virtual recruitment process

The second stage is conducted by logging into the messaging application via invitation link shared by the organizer. Both employers and applicants log in 15-30 minutes before the event begging to test that the application works (microphones, audio, etc.) and to join the meeting rooms within the application.

The third stage requires that both employers and applicants attend into virtual job interviews that are held in the earlier mentioned meeting rooms. The interviews can be either group or private implementations; this particular concept focuses on group interviews. It might also be possible that both forms of interviews, group and private, are conducted during the event, i.e. first a group interview and after that some of the applicants might receive an invitation into private interview.

The fourth stage takes place after the interviews. Both employers and job applicants leaves the event by closing the browser. After the event the employer still makes the decision on hiring and applicants are informed about the employer's decisions.

2 Theoretical framework

The theoretical framework is formed by three main sections that go through the basic concepts of information security and the chosen applications. While searching information on the basic concepts of information security I found several sources that were all used; Michael Whitman's and Herbert Mattord's textbook "The Management of Information Security", John

Vacca's textbook "Managing Information Security", and Rao's and Nayak's book "The InfoSec Handbook". These particular books state the concepts clearly and explain how they are connected to each other. Both Whitmann's and Vacca's books are also used as a textbook in several universities and UASs, including Laurea.

The second section contains discussion about information security behavior of the common computer users. It is based on Minna alasuutari's research "Prosessiteoreettinen näkökulma, joka selittää henkilökohtaisen tietokoneen käyttöön liittyvää tietoturvakäyttäytymisen muutosta", Iiro-Antti Räikkönen's research "motivations behind employee information security behavior" and Gary Jackson's book" Predicting Malicious Behavior". It is important to take human factors into consideration, so that we could understand what gives people the motivation to protect their personal information and what their point of view on information security is.

The third section contains information on Adobe Connect, Skype for Business and Slack, and it is based on the information gathered from the developers of these applications. This decision was made because the developers have very extensive information regarding their applications shared on their websites. The idea is to study the basic features and privacy policies of the applications.

2.1 Information security & the characteristics of information

According to Whitman and Mattord (2014) Information security is described to be the protection of information and it's three critical characteristics; confidentiality, integrity and availability, through the application of policy, training, awareness programs and technology. The protection also includes the systems and hardware that use, store and transmit information. In this project information security is being researched from the user's point of view so the concept of information security can be narrowed by leaving some parts of it without notice, such as technical and physical protection of infrastructure and all the other administrative aspects.

According to Whitman and Mattord confidentiality of information means that only those with proper privileges and well demonstrated need may access information. If an unauthorized person who doesn't maintain those two qualities would access information the confidentiality would be breached. Confidentiality is especially important when handling personal information about employees (or job applicants), customers, patients and other stakeholders of any organization. It is often expected that such information is protected closely and disclosure could cause big problems (Whitman & Mattord 2014).

Integrity means that the state of information is whole, complete, and uncorrupted. The integrity is threatened if information is exposed to corruption, damage, destruction or some other disruption of authentic state. This kind of a corruption might occur while information is entered, stored or transmitted (Whitman & Mattord 2014).

Availability of information occurs when it can be accessed by authorized users (person or computer system) in a usable format without interferences or obstructions (Whitman & Mattord 2014). It is important to notice that in general availability can be understood as information would be available for all of the users who want to access it, but strictly from the point of view of information security, it means that it can be only accessed easily by authorized persons, while unauthorized users are out the range of availability so that confidentiality and integrity is protected.

These three concepts are commonly known as the main characteristics of information and they should be taken into consideration when planning to ensure information security. They create the basis of information security, but they cannot ensure 100% of protection alone. As Whitman and Mattord (2014) state that present-day needs has made these characteristics inequate as their own and they cannot cover the constantly changing information technology environment entirely. Therefore it is important to introduce some other critical characteristics that can comprehend the present needs. These characteristics include privacy, identification, authentication, authorization, and accountability.

Privacy means that the information which is been collected, used and stored should be used only for the purposes that are authorized by the owner of the data (Whitman & Mattord 2014). This is one of the most important characteristics of information security from the point of view of this particular thesis, since the end product is a guide that instructs job applicants how to keep their personal information protected.

Identification is described by Whitman and Mattord to be the ability (of a system) to recognize individual users. It is usually performed in a form of a user name of user ID. Authentication is the process of defining whether the user has the identity it claims to have. The authentication process is commonly implemented by a personal identification number (PIN) or a password. Authorization is implemented after the user is authenticated. What happens during authorization is basically that the system defines whether the user has been specifically and explicitly authorized by the proper authorities to handle the data (access, modify, delete).

Accountability means that every action or all the activities done when handling data can be traced to a named user. This can be implemented i.e. by audit logs that track user activity on

an information system (Whitman & Mattord 2014). The idea is that possible misuse of the data could be traced to the user who has implemented the misuse.

According to Vacca (2013) the assurance of information is achieved when information and information systems are protected against attacks through the application of security services such as availability, integrity, authentication, confidentiality, and nonrepudiation. The application of the mentioned services should be based on protecting the information, detecting threats and reacting to threats. The idea is that in addition to just applying protective methods, users should also expect attacks and include attack detection tools, and methods for recovering from the attacks.

Rao and Nayak (2014) define information security to be the protection of information and information systems from unauthorized users accessing, using, modifying, or destroying the information (confidentiality & integrity). Other important contributors (favorable or adverse) to the field of information security are human beings, particularly employees, contractors, system providers, hackers, and crackers.

As we can see the opinions and definitions of the information security professionals are somewhat similar. By far all of the three studied sources defined information security to be more or less the protection of the key characteristics of information; confidentiality, integrity and availability. Rao and Nayak mention actions that highlight the protection of confidentiality and integrity, and they don't seem to agree with the other authors on the importance of availability. In conclusion Whitman's and Mattord's, and Vacca's definitions are broader than Rao's and Nayaks, but in general all of them have lots of similarities and they are based on same theories regarding the characteristics of information.

Whitman and Mattord extends the characteristics by adding 5 new characteristics, which is justified by appealing to constantly changing environment, or as I understood it; technological development. In my opinion it is clear that confidentiality, integrity and availability are the main characteristics of information that should be protected. The 5 other characteristics; privacy, identification, authentication, authorization and accountability should be also emphasized but in a minor role, when compared to the three main characteristics.

The sources show quite unanimous definitions for information security and it's characteristics. According to these results it should be clear that all of the 8 characteristics of information should be also noted when creating the end product; the guidebook should be created in a way that it would introduce the job applicants means to protect the characteristics of information.

2.2 Information Security behavior

According to Minna Alasuutari's (2016) process theoretical point of view people change their information security behavior based on motivational factors, current needs and feelings. Computer users constantly interact with the surrounding environment and experience information security related occurrences. These occurrences sets off different kinds of feelings and at the end create the need for security: they consider information security from their own personal point of view and seek to get rid of uncertainty by taking actions by protective matters to ensure their personal information security.

Alasuutari found out in her research that the information security behavior is always bound to the current situation/environment, even though computer users have taken the protective matters, set by the earlier feelings of uncertainty into action. Users might occasionally disable their protection, especially if they feel that some of their needs are in conflict with the protective matters. The disabling of the protection can happen i.e. when user has to hand over personal data for officials, e.g. they might send the data by using unprotected email connection because it's more convenient, and therefore risk their own data privacy. In these situation users prioritize their needs over the security, and either temporarily or permanently abandon their information security related customs. In other words users are in a constant conflict between their needs and information security behavior, which might cause occasions where information security is compromised. According to Alasuutari the occasion where user's needs override the information security can be caused by such things as the need to join a new organization/group or to ease the running of daily errands.

Gary Jackson (2014) defines also that in general people respond continuously to events and situations in the environment that precede their behavior; we continually respond to any environmental context in which we find ourselves. According to Jackson people usually form so called antecedents based on the preceding events and later modifies their behavior and predicts the possible consequences based on these antecedents. The Jackson's theory can be seen to support the fact also found by Alasuutari: earlier experiences modify the behavior of people and this same theory is also applied in his book to explain malicious behavior.

Iiro-Antti Räikkönen's research (2017) aimed to study what motivates employees to comply or not to comply with information security practices. Even though this research was conducted by studying employees of different organizations, it could still give some insight into the information security behavior of other groups of people and therefore should be observed during this thesis project. The research shows that regardless of having an overall positive attitude towards information security and believing to possess adequate understanding of information security, neglecting it still occurs from time to time.

The most common reason for neglecting information security practices according to Räikkönen was avoiding inconveniences, i.e. not changing passwords or using same passwords for several accounts. Also a false sense of security was a theme that was brought up by the employees and it could also be seen as an important contributor to neglecting information security. According to Räikkönen this false sense of security is closely related to the level of information security awareness: "if people do not understand all the ways that they can neglect information security and the possible consequences, more likely they are to neglect it".

All of the three sources introduce different theories that are related to computer user's information security behavior, but in my opinion they aren't in conflict with each other. Instead they might even support each other, especially Alasuutari's and Räikkönen's researches since both of them mention that avoiding inconveniences or easing the running of daily errands are common reasons to neglect information security practices. There is also a connection between Jackson's and Alasuutari's researches since both of them believe that the changing environment and earlier experiences determine the future information security behavior of the users.

The result of Alasuutari's research shows that people might change their point of view of information security when they have a need to join a particular group or organization; this includes also recruitment since the whole process is about joining into a new organization. Also the behavior might be influenced by convenience factors mentioned by both Alasuutari and Räikkönen, i.e. it would be more convenient for job applicants to send personal data over by non-encrypted email messages instead of encrypted ones, and therefore possibly risk their personal information security or lower their usual information security practices.

In the accordance of Alasuutari's research we can see that job applicants might have incentives to occasionally compromise their personal information security behavior if they experience, either consciously or unconsciously, that their need for applying or joining into an organization is more important than their earlier information security related protective actions; their basic information security behavior might change. According to Räikkönen this kind of neglecting of information security practices might be caused by ignorance or not being aware of information security related threats. This again in my opinion emphasizes the importance of different kinds of attempts to raise the basic information security awareness.

It is important to make the users aware of the general risks regarding information security, in this case information security risks related to the usage of messaging applications, so that they wouldn't change their general information security behavior and lower their personal protection during recruitment. As a result of researching the work of Alasuutari, Räikkönen and Jackson, I think that the guidebook should be created in a way that it would also raise

information security awareness i.e. by telling why it is important for job applicants to protect personal data and introduce the basic threats to increase the motivation of doing so.

2.3 Instant messaging applications

This section introduces basic information on the three instant messaging applications. It was necessary to study the background and basic functions of the applications before studying further into information security related themes. The following paragraphs goes through such information as the owners/developers, functionalities and privacy policies of the applications.

2.3.1 Adobe Connect

Adobe connect is a software used for web conferencing and it also offers a platform for online meetings, virtual classrooms and large scale webinars. It is commonly used to create presentations, online training materials, learning modules and desktop sharing. The software was developed by Adobe systems and it was released in 2012. It is based on Adobe Flash, which means that participants don't have to download or install anything to their computers in order to attend webinars or online meetings. The Adobe Flash works in a way that participants follow the link shared by the host of the meeting room, and they will have access into it directly through their web browser.

Currently Adobe Connect is formed by three sections: Adobe connect Meetings, Adobe Connect Webinars and Adobe Connect Learning. These three sections enable such features as audio and video conferencing, recording of online meetings, screen sharing, chat, customizable meeting rooms, Breakout sessions within a meeting and VoIP (voice over internet protocol) (Adobe Systems inc., 2017).

According to Adobe's privacy policy (2017) the North American users' information is handled according the legislation of the State of California, U.S. Other than North American users are handled by the legislation of Ireland, and they are served by the Adobe Systems Software Ireland Limited (Adobe Ireland), which operates under the North American Adobe Systems Incorporated (Adobe U.S.). Adobe also notifies that when users use Adobe applications, and accept the terms of use they also give the company a right to send user data across geographical borders to other countries, i.e. sending European user's data from Adobe Ireland to other countries where adobe and it's associates operate. The user data is retained in Adobe Servers which are located around the world, and therefore information usually has to be sent across borders.

The basic user data is given to Adobe when the user creates an adobe account, which usually contains the name of the user, email and payment information. In addition to the basic user data Adobe might also collect data such as how the adobe applications and websites are used, when they are used, and locations based on IP-address and the type of browser and devices which the user has used. Adobe claims also the right to combine this information to the data it has gathered from other sources according the legislation, this combination of data might give them i.e. information about the users employer (size, field of business and other business related information) (Adobe Systems Software Ireland Ltd, 2017).

2.3.2 Skype for Business

Skype for Business is an instant messaging application that is meant for businesses and other organizations; hence it differs by the selection of features from the actual Skype, which is meant for individual computer users. It has been developed by Microsoft and it was released in its current form in 2015.

Skype for business contains such features as instant messaging, VoIP and video conferencing up to 250 users. More advanced features are connected to other Microsoft software such as Outlook and Office, e.g. user can see if other connected users are working on the same document in office programs (Microsoft, 2017).

According to Microsoft's Privacy statement (2015) the company collects certain user data from the users of Skype for Business. The user data might be stored and processed on Microsoft's or their associates' servers that might be located in the United States or anywhere in the world where Microsoft or the associates maintain facilities. The user data might contain usage and configuration data, call quality information, types and causes of errors e.g. dropped calls, or sing on or meeting join errors. Microsoft states that the information is used to improve the features of Skype for Business and also their other services. According the privacy statement personal data is not shared with third parties without users consent, and if the data is shared with the consent they will only provide the data that the associates specifically need to do their operations, and they are prohibited from using the data to any other purpose than Microsoft have entitled them to. Commonly Microsoft provides this kind of a user data to associates that conduct some kind of limited services on behalf of Microsoft, i.e. answering customer's questions about products and services, or they might perform statistical analysis of the usage of Microsoft's products and services.

2.3.3 Slack

Slack is an instant messaging application, developed by Slack Technologies in 2013. It is meant to work as a messaging platform for all kind of teams and internal communication channel for organization.

The application contains such features as direct messages to other user or group, Channels for individual topics within the group, and video calls and VOIP. It also offers plug-ins to other applications such as Dropbox and Twitter, e.g. to ease file sharing (Slack Technologies, 2017). The application is based on teams that are created by the customer. After the creation a team the customer will invite users into it. The team works as a communication channel for the users. There can be several group discussions within one team and it is also possible to individual users to chat directly with each other outside the group discussions.

Slack Technologies state in their privacy policy (2016) that they collect different kinds of user data, and they do so on behalf of their customers who creates the teams. User data contains i Messages (group and direct messages), pictures, videos, edits to a messages and deleted messages. User can also add information on their profile such as first and last name, job, phone number and photo. Slack also might collect other user data such as usage of the application, location and device information.

Slack Technologies states in the privacy policy that they may access and use customer data to provide, maintain and improve their services, and to prevent service, security and technical issues. In addition they might use other data to research and analyze trends, and to respond to service requests, i.e. if the customer has questions or problems, billing account management and marketing.

As mentioned already slack collects the data on behalf of the customer that creates a team. The customer provides the instructions on how to process the data. For example, Customer may provision or deprovision access to the Services, enable or disable third party integrations, manage permissions, retention and export settings, transfer or assign teams, share channels, or consolidate teams or channels with other teams or channels (Slack Technologies 2016).

3 Methodology

This section introduces the methods which were used for data gathering during the thesis project. The data gathering was started by conducting a secondary data analysis in order to find results on information security threats and instructions. After the analysis observations were used to gather results regarding the safe usage of the studied applications.

3.1 Secondary data analysis

Secondary data analysis is simply the analysis of already existing data found from various sources (e.g. literature, statistics, research studies etc) (Pennington n.d.). The analysis involves data gathering, studying of the data in order to find results that can be used for specific purpose, finding how the data applies to the research and drawing a conclusions.

In this case the secondary data analysis aims firstly to gather information about the common information security threats related to recruitment. Secondly the analysis is conducted to find common information security instruction that should be taken into consideration while attending into virtual job interviews.

The gathering of the information was conducted by studying literature, documents and statistics from various sources and trying to find as many as possible threats and instructions that might be relevant to recruitment processes. Also some of the ideas and data were developed/collected and analyzed during a workshop that was held with the "Social media and it's equipments as a way of working-life" –project team, which took place at Laurea Leppävaara campus at 18.8.2017.

Determining the fact that how relevant a particular threat is with a virtual recruitment process was done by reflecting the threats to the actions that are needed to be done by the applicants during the process. For an example reuse of passwords which is considered to be a major threat according the Finnish communication regulatory authority (2017) cannot be considered to be relevant if the interview is done by using adobe connect, since the logging into adobe connect events is based on invitation link and there is basically no password authentication.

After the introduction and analysis of information security threats it was time to start studying the basic instructions on how one can protect him-/herself against the common threats. This was done by gathering a list of actions that job applicants could do to increase the level of their security. In this phase the material was collected more or less from the same sources on which the common threats were gathered.

The information security instructions were analyzed by simply reflecting them on the usage of instant messaging applications and online interview situations. Determining the relevance of a particular instruction to a recruitment situation was done by analyzing whether the possible threats could be prevented by following the particular instructions.

3.2 Observations

Observations as a scientific tool and data gathering method include serving of a formulated research purpose, systematic planning, and recording and systematic checks on validity and reliability (Kothari C., 2004). Observations can be also described to involve systematic viewing, recording, description, analysis and interpretation of certain behavior (Saunders et al, 2016). While implementing observations the information is sought through by the researcher's own direct observations without asking from the possible respondents or other stakeholders of the researched phenomenon (Kothari 2004).

This study will be implemented by a form of observations called participant observations. According to Kothari (2004) participant observations occur when the observer observes by making himself a member of the group he is observing so that he can experience what the group experiences. This particular process lets the researcher to learn by directly experiencing the social situation or research setting (Saunders et al. 2016).

As there were no earlier research or literature found regarding the implementation of virtual recruitment with the researched applications, the only option was to try to experience the online interview situations as closely as the job applicants would experience them and make observations on what is actually safe behavior form the point of view of information security. The guidebook needs to contain specific instructions for the applications and they can be only gathered by using and testing the applications; seeing which the best practices are for sharing files during online interviews.

The observations were made during testing sessions where the interview situations were simulated within each of the messaging applications. As job applicants will sing into the applications as guest users and employers as host, it is important to see which would be the options for guest users to share documents and files. This particular method confirms that how the personal data of job applicant should be shared while using the instant messaging applications.

The actual function that is being observed is file sharing; how files (CVs, motivation letters etc.) can be shared during the online interviews and is it safe to share them via the sharing features of the applications. In particular it is important to find out who can see, open, delete or modify the shared files.

4 Creation of the guidebook

The content of the guidebook was created in three phases so that it begins from the basics and ends to the more detailed instructions. The phases are; studying possible threats, studying ways to prevent the threats and studying the safe usage of the instant messaging applications. The guidebook itself is also divided into three chapters that follow these three phases by the content.

The first phase gives an introduction to the common information security threats for individual computer users, and also explains why it is important to protect yourself from these threats. The reason why this kind of information is included into the first chapter is based on Minna Alasuutari's research. As said earlier the research shows that the information security behavior is bound to the computer user's environment and to the current situation where he/she operates; they might lower their personal protection e.g. due the need of joining to a new organization. The idea is to prevent this from happening by introducing the possible risks of the virtual environment, and in a way motivate the users to take protective actions into use while operating in this environment.

The second phase leads the users deeper into the virtual environment. It gives general information security instructions that should be taken into consideration during the virtual recruitment process. The instructions in the second chapter can be implemented no matter which application is in use. The third and last phase focuses on the three chosen applications and it is meant to give specific instructions on the safe usage. The chapters two and three should contain such instructions that ensure the protection of the main characteristics of information introduced in the theory section of this report.

5 Results

This section contains the results of the research stages, secondary data analysis and observations. The result were gathered and analyzed during the autumn of 2017 and they were used to create content for the guidebook.

5.1 Secondary data analysis

This section introduces the data and results that were gathered during secondary data analysis. The analysis was conducted between 1.8.-1.10.2017., and the results were analyzed during 25.9.-4.10. The results in this section were gathered from the following sources:

1. Reports and articles of Finnish Communication Regulatory Authority; Tietoturvan vuosi 2016 (2017) , palveluiden turvallinen käyttö (2017) & internetpalveluiden turvallinen käyttö (2017)
2. Thesis “Data privacy and data security in social media” by Jensen & Korpela (2011)
3. Finnish Security Committee’s guidebook “Kodin kyberopas” (2017)
4. PH National Privacy commission’s article “threats to security and privacy” (2017).
5. Social media and it’s equipments as way of working life-Workshop

These documents introduce both information security threats, and instructions for safe usage of internet, social media & other web based services. Firstly I found three critical threats that are; Threats against user’s privacy, malware and physical environment of the user. Since it was the request of the project management to keep the guidebook as summary as possible and due the fact that the main goal of the guidebook is to introduce ways to prevent information security hazards, these three threats could be considered to be enough to draw readers’ attention and raise the awareness of information security threats.

The most relevant instructions relating to the information security of virtual recruitment process were found from the same sources, and they included such factors as: What should be shared online, paying close attention to the physical environment, getting to know the terms of use, and Protect your computer and connection from malware. All of the threats and instructions are introduced more thoroughly in chapters below.

5.1.1 Privacy in social media/ virtual recruitment event

Finnish communication regulatory authority’s report “tietoturvan vuosi 2016”-report (2017) lists the most common (top 5) information security threats for individual computer users:

1. Scams and classified scams
2. Ransomware
3. Internet of things (IoT)
4. Privacy in social media
5. Reuse of passwords

The three first threats seem not to be related to recruitment very closely from the point of view of job applicants. They are considerable threats, but they relate more on general usage of internet such as web browsing and i.e. online shopping etc. All kinds of scams, ransomware and, in a minor role, IoT are mostly concerns for the employer during the recruitment process, since they have more influence to the services, applications, websites, programs, and

systems etc which are used during the process. Instead Job applicants don't commonly have possibilities to influence on them.

The last two threats, privacy in social media and reuse of passwords are ones that job applicants can influence on, and therefore they should be emphasized when looking on to the information security of recruitment process from their point of view. During the testing sessions I noticed that reuse of passwords-threat has no relevance to this concept since the studied applications don't require password authentication, meaning that it can be excluded from further studying. This leads us to the fact that only threat from the "tietoturvan vuosi 2016"-report that is going to be introduced in the guidebook is the threats regarding privacy in social media.

The privacy in social media-threat means that people might not be aware who has access to the information which they share via the different channels of social media. For an example where is the data restored and is it sold/given for third parties to be used as marketing data, or can other users see your personal information. Users should be aware that their data might get exposed to unauthorized persons, if it is not protected.

This particular threat of privacy in social media is very close to the concept of virtual recruitment that is being developed during the "Social media and it's equipments as a way of working-life"-project. The idea of the concept is to gather employers and job applicants into virtual meeting rooms where they can interact with each other by using such features as video calls, chats and VOIP. All of these applications also reserve the right to collect user data to their servers. If you compare this to the features of Facebook groups or even to Facebook in general, you can see some similarities.

5.1.2 Malware

The second source that was found during the analysis was PH National Privacy commission's article "threats to security and privacy" (2017). The article introduces the common tools of identity thieves, hackers, marketers and other actors that might have incentives to get their hand on users' personal data. The article introduces the most common types of malware:

1. Viruses and worms: The most common malicious software that can infect a system and spread to other programs and computers without the owner noticing it.
2. Trojans: A type of malware that mislead the user to download and opening it as it is disguised as a harmless file. The Trojans let the attackers to access to the user's computer and steal personal information or download other pieces of malware.

3. Adware: Illegal versions of adware are programs which can take the form of pop-up or browser windows that cannot be closed or they can run other kinds of malware that can track the user's web habits or even keypad functions.
4. Spyware: Type of software that spies the user and then sends the information to the administrators of the software. They can get information i.e. through web cameras, microphones or going through personal files stored into the user's computer.
5. Ransomware: A type of malware that encrypts the user's computer or files to hold them ransoms. The attackers are usually requiring money to open the encrypted files.

The possible effects of these types of malware vary from small annoyance to being critically damaging for entire databases, systems and user's privacy. According to the article one of the most dangerous ways malware can threaten our data privacy is by opening a backdoor for attackers to access your passwords, IP addresses, banking information, and other personal data.

5.1.3 Physical environment

In addition to the two threats mentioned above, it is also important to emphasize general threats caused by the job applicant physical environment. This idea was generated while attending into a workshop in 18.8., where the concept of virtual recruitment was developed. We discussed the characteristics of a well organized virtual career event and one of the mentioned characteristics was actually the physical environment of the attendants. The idea is that the applicants and employers should be located in a quiet place during online interviews so that there are no distractions, but this is actually also very important aspect from the information security-perspective.

Technical solutions alone are not enough to protect information; it also requires at least some level of physical protection, i.e. being in a private location where no one can hear the interviews. If the applicant or representative of employer is in a public location during the interview, or even in semi private location, unauthorized persons could possibly hear the discussion or even spy some data from the computer screen.

5.1.4 Information security instructions

The previously mentioned documents of Finnish Communication Regulatory Authority, Finnish Security Committee and PH National Privacy Commission all gave advice on how computer users can get protected against the most common threats. Also the ideas discussed during the workshop were used to form instructions for ensuring safe physical environment. In conclusion

the instructions on how to avoid the most common information security threats during the virtual recruitment process could be presented by the following themes:

1. Think what is necessary to share during a public online career event or group interviews and what is not necessary
2. Pay close attention to your physical environment
3. Get to know the terms of use and check the privacy settings of the used applications and other services
4. Protect your computer from malware

According to the publication “Kodin Kyberopas” (2017) it would be critically important to consider beforehand which kind of information would be necessary to share publicly. The article of FCRA “internetpalveluiden turvallinen käyttö” also supports this theme by recommending considering where it is actually necessary to share personal information. These same rules could be also applied to the recruitment events and group interviews. It would be recommended to think before hand on which information you should discuss during the public parts of the possible career event or group interviews; it could help to think what kind of information is actually relevant regarding the applied position. In conclusion; don’t publicly tell anything you wouldn’t mind telling a complete stranger (date of birth, social security number, address, phone number or email), if it is needed you can provide the information privately to the employer.

The aspect of the physical environment should be considered so that there would be no possibilities for unauthorized persons to hear the job interviews, or see the screen of the applicant computer as confidential information could be exposed that way. The applicant should make sure that the location is private, at least that there wouldn’t be any other persons in the room, and ensure that the discussions could not be heard through open windows, doors etc. After all this same aspect applies when attending into traditional face to face interviews, so why wouldn’t they also apply for online interviews.

According to the article of FCRA “palveluiden turvallinen käyttö” (2017) every computer user should consider which kind of online communication services are safe to use, and how the owners of the services gather and use users’ data. The article recommends finding out at least the type of the used service and for what purposes they can use your personal data. The Kodin kyberopas (2017) also recommends that users should get to know the terms of use of the applications or services before using them. It also emphasizes paying attention to who owns the rights of published data as some applications and services might require you to give the rights for them.

The last instruction relates to the fact that by protecting your computer you will also protect your personal information (Finnish Communications Regulatory Authority, 2017). The publication “Kodin Kyberopas” recommends users to do at least the following actions:

1. Keeping your operating system, browser and plug-ins updated
2. Enabling firewall at all times
3. Using the administrator privileges only when it is absolutely necessary
4. Protecting the used local area network
5. Keeping the router updated and enabling it’s firewall
6. Enabling reliable protection software

By following these instructions the job applicants could possibly increase their level of information security, and at least decrease the possibilities of the threats to happen.

5.2 Observations

The observations were done during testing sessions that were conducted between 1.9.-5.10.2017. All of the studied applications offer at least two different methods for sharing files/content that could be used during online interviews. These options are introduces in the chapter below.

5.2.1 Adobe Connect

Files or other content, in this case CVs or other recruitment related documents, can be shared by using the three functions of Adobe Connects share pod: screen sharing, uploading a document to a content library directly from your computer, or a whiteboard (drawing and writing).

A new share pod is opened from pods-menu from the top bar of the meeting room. The opened share pod gives now the three options to share content, which can be found by clicking the dropdown arrow from the middle of the pod. In this case the whiteboard is going to be excluded from further observations, because it could not be used for file sharing in a way that is desired from the point of view of recruitment.

Uploading a document from the user's computer can be done by clicking the "share document" from the dropdown menu of the share pod and after that by clicking the "browse my computer"-button from the bottom of the opened window, which shows the upload-library. After the wanted document has been uploaded, it will appear into the library and the user can now

share it with others. If the user won’t remove the file from the history of the file sharing pod before he leaves the meeting room, it will stay visible for hosts and other presenters.

Sharing a user's screen is also an option in a way that the user can open the file to his computer screen and then share his screen via the share pod. In this way the user won't need to upload any files and it won’t leave any copies of the file into the folders of the applications. In other words instead uploading and saving a file the user can just open them on the computer screen and then share it live for other users in the meeting room.

Screen sharing is activated by clicking the "share my screen"-button from the share pod. There are three different options to choose from the screen sharing menu; Desktop, application or windows. Desktop-option will basically share everything that is visible on the user's screen. Application-option shares everything within a chosen application, i.e. all the windows and tabs of a chosen web browser. Everything done outside the chosen application will not be visible for other users. The windows-option are meant for sharing content from applications which allows users to open several windows, in a way that only a certain one window is visible for the meeting room. For an example the user can determine that he wants to share only one tab of a web browser. When the user ends the screen sharing session, there are no uploaded files to remove or other traces of the shared content saved into the history logs of the meeting room.

5.2.2 Skype for Business

The observations on this application were restricted to only using the meetings-function since it is most suitable for arranging online interviews; it can be opened from the browser and allows guest users, so that they won’t need to install any software. The users can share content during a meeting by sharing their screen, sharing attachment files or sharing notes. The sharing of notes is going to be excluded from this study, since it is actually meant for uploading and writing notes during the meeting, not sharing presentations or documents. All the sharing options can be accessed by clicking the present icon (screen icon) from the bottom of the meeting room.

The screen sharing-function in Skype for Business is quite exactly similar as it’s equivalent in Adobe Connect; it has three options which are desktop sharing, application sharing and sharing a PowerPoint-file. Again desktop sharing means that everything happening at the users screen is shared to the meeting. Application sharing means that the user chooses an application which's content is shared, and everything else done outside the application is not going to be visible for others attendees of the meeting. PowerPoint sharing will share just the content of one chosen PowerPoint file.

Attaching files to the meeting is also quite similar to the Adobe Connect's document uploading-function. The biggest distinction between these two is that in Skype the user sharing the files is asked first to define who can actually see and download the files, as in Adobe Connect this was not possible. The user can for an example defines that everyone attending into the meeting could download his files, or he can choose a smaller group amongst the attendees. It is also important to notice that the uploaded files will be saved into the attachment folder of the meeting; they can be accessed and removed by choosing "attachment management" below the present-icon.

5.2.3 Slack

Slack gives possibilities to upload files directly from the user's computer, share file from Dropbox and Google Drive, and screen sharing which is available for paid plans (slack call) and is only available through the desktop application (doesn't work on browser versions). All the shared files will be also stored in the file storage of the slack, and they can be deleted after they are not needed. Slack calls were not enabled in the project's slack environment where I tested the application, so screen sharing will be excluded from these observations. It is also excluded from the actual interviews if they are decided to be implemented by using Slack.

Uploading a file is done simply either by dragging the file into the chat, or by clicking the plus-icon from the writing pod of the chat. The file will appear into the chat as an attachment and it can be opened or downloaded by other participants. Other option is to upload the file to Dropbox or Google Drive, and after that share the direct URL of the file into the chat. When the link is shared into the discussion the application will automatically upload the file from Dropbox or Drive.

The uploaded files can be deleted from the file archive, which is accessed via the "more items" icon from the top right corner of the browser app. The user chooses "files" from the dropdown menu of the more items-icon and after that searches the wanted file from the archive and deletes it by clicking "more actions" → Delete file.

6 Conclusions

The purpose of this thesis was to gather instruction for job applicants for ensuring their information security and gather them into a guidebook. The results shows that job applicants can and should take actions to prevent common information security threats from happening,

or at least significantly decrease the possibilities by doing so. After all the threats can lead to extensive consequences if they are not monitored or regulated.

The probability and severity of consequences of the threats were analyzed by using risk matrix introduced in figure 2. The vertical axis of the risk matrix demonstrates the level of severity that a certain happening could cause. The horizontal axis demonstrates the probability of that happening to occur. The three differently colored areas between the two axes are marked as green, yellow and red.

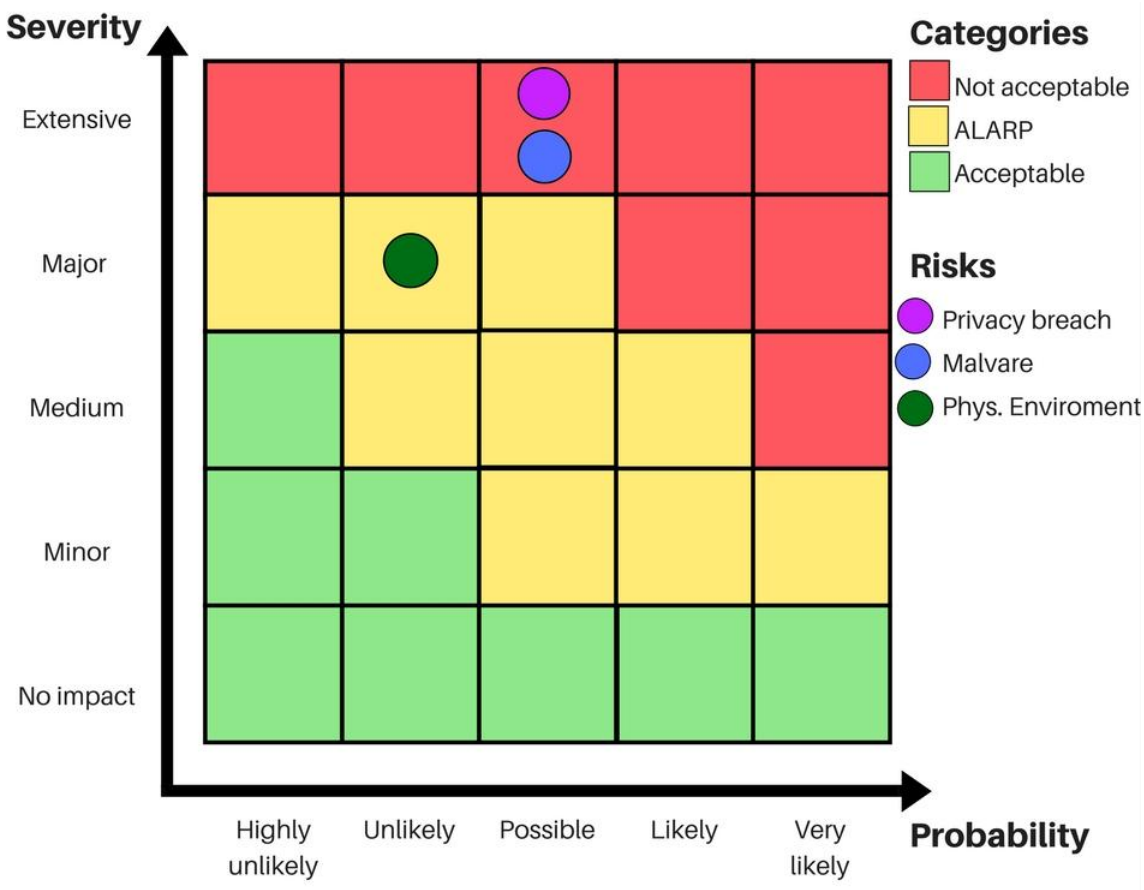

Figure 2: The risk matrix

The Green area covers combination of objects that implies that the risk is at acceptable level; there is no need to control or monitor the risks. Yellow states that the potential severity and probability of certain happening is at medium (ALARP-level) level and that these risks should be at least monitored closely, and controlled only if needed. The red area demonstrates the combination of high probability and high severity; the level of the risk is not acceptable and they should be monitored and controlled closely.

The possibility of privacy being breached sets at “possible”-level as it is mentioned in the top 5 of all the cyber security related risks of the “tietoturvan vuosi 2016”-report. The severity sets as extensive due the fact that confidentiality and integrity of the information is breached at this stage. The consequences include in worst case scenario identity thefts which can lead to financial and reputational harm. The risk sets at not acceptable-level on a risk matrix (figure 2).

The possibility of getting contaminated by some form of malware can be considered as possible on the scale of the risk matrix’s horizontal axis (they are described to be more rampant as ever). The consequences of these threats can be seen also as extensive; the confidentially, integrity, availability, privacy, authentication and authorization of processed data could be all breached. Again this risk is seen as not acceptable on the risk matrix (figure 2)

The possibility of the applicant’s physical environment causing problems can be seen to be unlikely since there are plenty of other factors that support the private locations over the public or semi public locations; i.e. assuring better audio and it can be said to be also common sense to be in private during any forms of job interviews. The severity sets at major-level since the confidentiality of personal information could get breached. These results indicate that this risk sets on level of ALARP (should be monitored as low as reasonably practicable), the yellow area of the risk matrix (figure 2).

The breach of privacy should be prevented most importantly by considering what kind of information and in which extent it is shared, also ensuring technical solutions should be noted. The protection against of malware should also be ensured by technical solutions. At last ensuring a safe physical environment should be done in a way it is done during traditional face to face interviews.

The following list introduces all of the relevant methods for preventing the three risks from happening:

1. Consider beforehand which kind of information should be shared (during both group and private interviews) and what is relevant regarding the applied position.
2. Don’t share critical personal information (phone numbers, email addresses, social security numbers etc.) publicly or during group interviews in any case
3. CVs, portfolios or other equivalents should be shared privately with the employer or the organizer of the virtual encounter before or after the online interviews
4. Use only safe and familiar local area network and protect it by keeping the router and it’s firewall updated

5. Enable virus protection and keep applications, browsers and operating system updated at all times.
6. Make sure that you are in a private and quiet location, and that there are no possibilities for unauthorized persons to hear or see the interview situation.
7. If it is necessary to share files or other content during the interviews, avoid uploading or attaching anything into the used application as they might be saved into their memory/history logs. Instead use the screen sharing function (Adobe Connect and Skype for Business), or create a public link into a Google Drive or Dropbox file (Slack).

As said earlier information security is defined to be the protection of the key characteristics of information; confidentiality, integrity and availability. This protection should be executed by technical solutions, awareness programs and common information security policies. The results of this research offer solutions for all of these aspects. Introducing the common threats raises awareness on information security related issues. The general instructions offer technical solutions for protecting the applicant's personal data, and combined with the other application specific instruction they can be used to form a common information security policy for virtual encounters.

The results of this thesis can be used in forming a short information security guidebook for job applicants as they offer clear instructions on how information should be protected, and as well as how to use Adobe Connect, Skype for Business and Slack safely during online job interviews. In addition to gathering these instructions and guidelines I also ended up publishing a blog post on the website of the "Social media and it's equipments as a way of working life"-project that is based on the results of this thesis, and also creating a summarized version of the instructions in Finnish, that was attached into a general instructions of a planned online recruitment fair.

6.1 Validity and reliability

The reliability refers to the fact that significant results of a research must be more than one-off finding and inherently repeatable (Shuttleworht 2008). In other words according to Martyn Shuttleworth other researchers must be able to perform the same results under the same conditions.

Validity encompasses the entire experimental concept and establishes whether the results obtained meet all of the requirements of the scientific research method (Shuttleworth 2008). This means that the research actually measures what is it supposed to measure and the results are genuine.

The reliability of the secondary data analysis of information security threats and instructions were verified by using several different sources and doing background checks on them in order to see that they were unbiased. It was also important to see that the analyzed data was up-to-date so that the end product would meet the present information security requirements.

The observations were made by using the latest versions of the studied applications. If the study were to be executed again with the same version of the applications the same results would be found. This can be also confirmed from the user manuals of the studied applications.

The biggest problem during the research was that there was vast amounts of secondary data and most of it was published by private companies or other publishers that were dependant on third party financing or on marketing income, and therefore they might be heavily influenced/biased towards the financier's opinions. All of these sources had to be excluded. Nevertheless at the end there were enough unbiased sources such as publicly funded government organizations and educational institutions (i.e. workshop in Laurea), so that the results could be seen as reliable.

The results can be also seen as valid, since the purpose and goals were reached. The used methods generated result which answered to the sole purpose of the thesis; how the job applicants could ensure their information security. It was also possible to form the end product, the guidebook, based on the findings of this research.

6.2 Future research

Digitalization and technological development will generate new possibilities to develop new forms of virtual encounters and it could also enable new applications and methods for arranging online job interviews. Technological development also generates constantly new threats regarding information security. In the future researchers could study this same topic in a way that it takes the new threats into consideration; in a way update the common threats and information security instructions for example to meet the requirements of the 2020's technology. It could be also possible to study new instant messaging applications or updated versions of the current ones.

The topic of information security during recruitment could be also studied from the employer's point of view. Possible research problems could be i.e. how the job applicant's data should be processed and restored, how the employees responsible on recruiting should be

trained to handle confidential data or how they could ensure a safe online recruitment environment.

References

Literature

Jackson, G. 2012. Predicting Malicious Behavior. John Wiley & Sons, Incorporated, ProQuest Ebook Central.

Kothari, C. 2004. Research Methodology: Methods and Techniques. New Age International Ldt. New Delhi, IN.

Rao, U. & Nayak, U. 2014. The InfoSec Handbook. Apress. Berkeley, CA.

Saunders, M. Et al.. 2016. Research Methods for Business Students. Pearson Education Limited. Harlow, England.

The Security Committee (FIN). 2017. Kodin kyberopas. Turvallisuuskomitean sihteeristö. Helsinki, FIN.

Vacca, J. 2013. Managing Information Security. Elsevier Science. ProQuest Ebook Central.

Whitman, M. 2014. Management of Information Security. 4th Edition. Cengage Learning. Stamford, CA.

Online

Adobe Systems Inc.. 2017. Adobe Connect. Accessed 2 August 2017. http://www.adobe.com/products/adobeconnect.html

Adobe Systems Software Ireland Ltd. 2017. Adoben tietosuojakäytäntö. Accessed 7 August 2017. http://www.adobe.com/fi/privacy/policy.html

Alasuutari, M. 2016. Prosessiteoreettinen näkökulma,joka selittää henkilökohtaisentietokoneen käyttöön liittyvää tietoturvakäyttäytymisen muutosta. Accessed 2 August 2017. https://jyx.jyu.fi/dspace/bitstream/handle/123456789/49352/978-951-39-6609-6_vaitos23042016.pdf?sequence=1

European parliament & council. 2016. General Data Protection Regulation. Accessed 23 September 2017. http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=ENG

Finnish Communications Regulatory Authority. 2017. Internetpalvelujen turvallinen käyttö. Accessed 1 October 2017.

https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvaohjeet/palveluidenturvallinenkaytto/verkkopalveluidenturvallinenkaytto.html

Finnish Communications Regulatory Authority. 2017. Palveluiden turvallinen käyttö. Accessed 1 October 2017. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvaohjeet/palveluidenturvallinenkaytto.html

Finnish Communications Regulatory Authority. 2017. Tietoturvan vuosi 2016. Accessed 12 August 2017. https://www.viestintavirasto.fi/attachments/tietoturva/Tietoturvan-vuosi_2016_ViVi_29-11-2017_L.pdf

Finnish Government. 2016. Implementation of the government programme. Accessed 25 May 2017. http://valtioneuvosto.fi/en/implementation-of-the-government-programme

Imppola, M. 2016. Työnhakijan Tietosuoja – Henkiötietojen käsittely työnhaussa. Accesse 26 May 2017. http://www.theseus.fi/bitstream/handle/10024/121596/Imppola_Minni.pdf?sequence=1&isAllowed=y

Jensen, L. & Korpela, M. 2011. Data privacy and data security in social media. accessed 26 September 2017. http://www.theseus.fi/bitstream/handle/10024/27870/Jensen_Lillian_Korpela_Maire.pdf?sequence=1&isAllowed=yhttp://www.theseus.fi/bitstream/handle/10024/27870/Jensen_Lillian_Korpela_Maire.pdf?sequence=1&isAllowed=y

Microsoft. 2017. Professional online meetings build for business. Accessed 2 August 2017. https://www.skype.com/fi/business/

Microsoft. 2015. Skype for Business privacy statement. Accessed 7 August. https://www.microsoft.com/EN-US/privacystatement/SkypeforBusiness/Default.aspx

National Privacy Commission. 2017. Threats to security and privacy. Accessed 24 September 2017. https://privacy.gov.ph/threats-security-privacy/

Official Statistics of Finland (OSF). 2017. Transition from school to further education and work [e-publication]. Accessed 25 May 2017. http://www.stat.fi/til/sijk/2015/sijk_2015_2017-01-26_tie_001_en.html

Pennington, L. n.d.. Secondary Data Analysis: Methods & Advantages. Accessed 18 october 2017. http://study.com/academy/lesson/secondary-data-analysis-methods-advantages.html

Räikkönen, I. 2017. Motivations behind Employee Information Security Behavior. Accessed 4 october 2017. https://jyx.jyu.fi/dspace/bitstream/handle/123456789/55224/URN%3aNBN%3afi%3ajyu-201708313625.pdf?sequence=1

Shuttleworth, M. 2008. Validity and reliability. Accessed 18 October 2017. https://explorable.com/validity-and-reliability

Slack Technologies. 2017. Team communication for the 21st century. Accessed 2 august 2017. https://slack.com/is

Figures

Appendices

Appendix 1: Observation sheet – File Sharing

Ville Savolainen
Laurea University of Applied Sciences
Degree Programme of Security Management

Instant messaging applications: File Sharing – Observation sheet

Application	Options for File Sharing	Notes
Adobe Connect		
Skype for Business		
Slack		

Appendix 2: Content of the guidebook

Introduction

This document contains information security instructions and guidelines for job applicants so that they would be able to ensure their personal information security during virtual recruitment processes. The first section introduces some of the possible threats and their consequences. Second section gives general instructions how to prevent the threats from happening, and the third section gives application specific instructions on how to share content safely while using Adobe Connect, Skype for Business and Slack.

Information security is described to be the protection of information and it's three critical characteristics; confidentiality, integrity and availability, but they cannot ensure 100% of protection alone; in addition also characteristics such as privacy, identification, authentication, authorization, and accountability have a role in the protection of information.

Confidentiality of information means that only those with proper privileges and well demonstrated need may access information. If an unauthorized person who doesn't maintain those two qualities could access information, the confidentiality would be breached. Integrity means that the state of information is whole, complete, and uncorrupted. The integrity is threatened if information is exposed to corruption, damage, destruction or some other disruption of authentic state. This kind of a corruption might occur while information is entered, stored or transmitted. Availability of information occurs when it can be accessed by authorized users (person or computer system) in a usable format without interferences or obstructions. Naturally it is breached when even the authorized persons with proper privileges are not able to reach the needed data.

Privacy means that the information which is been collected, used and stored should be used only for the purposes that are authorized by the owner of the data. If data is used for other purposes than recruitment or i.e. it gets into unauthorized hands, privacy is breached. Identification is described to be the ability (of a system) to recognize individual users. It is usually performed in a form of a user name of user ID. Authentication is the process of defining whether the user has the identity it claims to have. The authentication process is commonly implemented by a personal identification number (PIN) or a password. Authorization is implemented after the user is authenticated. What happens during this stage is basically that the system defines whether the user has been specifically and explicitly authorized by the proper authorities to handle the data. Accountability means that every action and all the activities done when handling data can be traced to a named user. Accountability can be ensured for an example using audit logs or other means of documentation.

Information security threats

According to the Finnish Communications Regulatory Authority's report "tietoturvan vuosi 2016" (2017), the breach of privacy was one of the most common threats for computer users. Privacy is also a notable factor during recruitment and therefore it should be protected with due diligence. The breach of job applicant's privacy could be caused by the negligence while sending personal data to the employer. As a consequences of the possible data breach the confidentially of processed data could be lost. In the case of recruitment the data usually contains confidential personal information and could cause major harm if it's in the possession of unauthorized persons. Also the integrity of the data is in danger since it could get damaged or even corrupted. The breach of the confidentiality and integrity of personal data could also allow identity thefts or other means of misuse.

The second threat, malware or malicious software, are types of software that can open a backdoor for attackers to access your passwords, IP addresses, banking information, and other personal data. The possible effects of these types of malware vary from small annoyance to being critically damaging for entire databases, systems and user's privacy.

At last it is important to emphasize the physical protection of data. If we look recruitment from the point of view of job applicant, the physical environment where he/she is during a virtual meeting plays an important role on behalf of information security and data privacy. In a worst case scenario the environment would be a public place where unauthorized persons can hear or see something confidential, in a other scenario the environment could be private but confidentiality could be breached by negligence i.e. open door or window. As we can see at least the confidentiality and also privacy of the job applicant's personal data might get breached.

Threat	**Risk**	**consequences**
Breach of privacy/data leak	possible	Extensive -loss of confidentiality -loss of integrity -loss of privacy - enables identity thefts
Malware	Possible	Extensive

		-loss of integrity -loss of identification -loss of authentication -loss of authorization -loss of accountability -possibly loss of availability
Physical environment	Unlikely	Major -loss of confidentiality -possibly loss of privacy

Table 1: Threats

General instructions

The breach of privacy should be prevented most importantly by considering what kind of information and in which extent it is shared, also ensuring technical solutions should be noted. The protection against of malware should be ensured by technical solutions. At last ensuring a safe physical environment should be done in a way it is done during traditional face to face interviews.

The following list introduces all of the relevant methods for preventing the three risks from happening:

Consider beforehand which kind of information should be shared (during both group and private interviews) and what is relevant regarding the applied position.
Don't share critical personal information (phone numbers, email addresses, social security numbers etc.) publicly or during group interviews in any case
CVs, portfolios or other equivalents should be shared privately with the employer or the organizer of the virtual encounter before or after the online interviews
Use only safe and familiar local area network and protect it by keeping the router and it's firewall updated
Enable virus protection and keep applications, browsers and operating system updated at all times.
Make sure that you are in a private and quiet location, and that there are no possibilities for unauthorized persons to hear or see the interview situation.
If it is necessary to share files or other content during the interviews, avoid uploading or attaching anything into the used application as they might be saved into their memory/history

logs. Instead use the screen sharing function (Adobe Connect and Skype for Business), or create a public link into a Google Drive or Dropbox file (Slack).

Application specific instructions

While using Adobe Connect files can be shared by using the three functions of applications share pod: screen sharing, uploading a document to a content library directly from your computer, or a whiteboard (drawing and writing). In more detail a new share pod is opened from pods-menu from the top bar of the meeting room, and content sharing options can be found by clicking the dropdown arrow from the middle of the pod. Screen sharing is the only recommended option to be used during the online interviews, as the other options will leave the file saved into the memory of the share pod where it might be visible for unwanted users.

The recommendations for using Skype for Business' content sharing option are quite similar. There are three options; Screen Sharing, uploading/attaching files or sharing noted. The sharing options can be accessed by clicking the present icon (screen icon) from the bottom of the meeting room. Again only screen sharing would be recommended option during online job interviews, since the two other methods leaves the shared content into the memory of the meeting where it might be exposed to other users.

The browser version of Slack offers two methods for content sharing: Uploading/attaching files directly from user's computer or sharing a public link into Google Drive or Dropbox files. Uploading files directly from your computer will lead to the situation where the file is going to be restored into the sharing folder of the Slack meeting, so this option should be avoided. Instead it is recommended to share the needed files via Google Drive or Dropbox.

appendix 3: Content published in a blog

Be aware on information security of virtual encounters – tips for attendees

Be aware on information security of virtual encounters – tips for attendees
Digitalization and rapid technological development creates constantly new possibilities for developing virtual encounters. While developing new concepts for these virtual encounters it should be essential that also the aspect of information security is taken into consideration.

Such writers as Michael Whitman & Herbert Mattord (2014), and John Vacca (2013) all define information security to be the protection of three critical characteristics of information; confidentiality (in Finnish luottamuksellisuus), integrity (eheys) and availability (saatavuus). Meaning only those with proper privileges and well demonstrated need may access the protected information, the state of it is whole, complete, and uncorrupted, and it should be accessible for authorized users without interferences.

The three characteristics mentioned above should be protected by application of common information security policy, technological solutions, training and awareness programs. These actions should prepare us to protect information, detect threats and react to threats.

What are the threats?

Information security is an important aspect of any recruitment process, and it is in the best interests of both employers and job applicants that the applicants' personal data is kept as private as possible. Nevertheless if the data would get breached for some reason, the consequences might be extensive. In a worst case scenario breach could enable identity thefts and other forms of misuse of personal data, and hence lead to either financial or reputational harm, if not both.

The job applicants should at least be aware of such threats as breach of privacy (who has access to their information, where it is stored and to whom it could be distributed), common types of malware and the physical environment during online job interviews.

How can the data be protected?

At the end the extent of the consequences of data breach depends on the extent of the shared data. Therefore it would be critically important to consider beforehand which kind of

information should be shared; what is relevant regarding the applied position, and what should be said during group or private interviews. As the developed concept is concentrated into group interviews, it would be recommended to go through which kind of personal information should be told during them. Most importantly it would not be advisable to share critical personal information (phone numbers, email addresses, social security numbers etc.) publicly or during group interviews in any case.

Personal information such as CVs, portfolios or other equivalents should be shared privately with the employer or the organizer of the virtual encounter before or after the online interviews. If it's absolutely necessary to share files while attending to Adobe Connect, Skype for Business or Slack meeting, it would be recommended to use the screen sharing function (AC & Skype) or to create a public link into Dropbox or Google drive file (Slack). Uploading or attaching files directly from the user's computer might save the files into the memory/history logs of the used application so it should be avoided.

The aspect of physical environment should be considered so that there would be no possibilities for unauthorized persons to hear the job interviews, or see the screen of the applicant's computer. It is critical to make sure that the location is private meaning no other/unauthorized persons in the room, and any open windows or doors. The environment should be ensured at least the same way it is done while implementing traditional face to face or group interviews, as the developed concept is focusing on group encounters.

Are there any technical solutions for data protection?

The last instruction relates to the fact that by protecting your computer you will also protect your personal information. According to The Finnish Security Committee (2017) at least following technical solutions should be executed to ensure malware free computer:

1. Keep operating systems, browsers and plug-ins updated
2. Enable firewall at all times
3. Use the administrator privileges only when it is absolutely necessary
4. Protect the used local area network and use only safe networks that you are familiar with
5. Keep the router updated and enable it's firewall
6. Enable reliable protection software

Conclusions

Job applicants can and should take actions to prevent common information security threats from happening, or at least significantly decrease the possibilities by doing so. It is important

to be aware of the threats and then apply the above instruction so that the online recruitment environment is kept as safe as possible.

The author Ville Savolainen is a student of security management from Laurea University of Applied Sciences, working on a thesis which studies the information security of virtual encounters.

References:

Turvallisuuskomitea. 2017. Kodin kyberopas. Turvallisuuskomitean sihteeristö. Helsinki

Vacca, J. 2013. Managing Information Security. ProQuest Ebook Central. Elsevier Science.

Whitman, M. 2014. Management of Information Security. 4th Edition. Stamford. Cengage Learning.