

TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

Department of Software Science

Kapil Yadav 177243IVCM

**INFORMATION SECURITY MANAGEMENT FOR  
TELEWORKING IN SMALL AND MEDIUM ENTERPRISES  
DURING THE COVID-19 CRISIS**

Master Thesis

**Supervisor**

Kaie Maannel

Tallinn 2020

## **Author's declaration of originality**

Declaration: I hereby declare that this thesis, my original investigation and achievement, submitted for the Master's degree at Tallinn University of Technology, has not been submitted for any degree or examination.

Deklareerin, et käesolev diplomitöö, mis on minu iseseisva töö tulemus, on esitatud Tallinna Tehnikaülikooli magistrikraadi taotlemiseks ja selle alusel ei ole varem taotletud akadeemilist kraadi.

Author: Kapil Yadav

.....

(signature)

Date: December 21, 2020

# Annotatsioon

Käesolev lõputöö on kirjutatud COVID-19 põhjustatud eriolukorra ajal, mil üha enam inimesi asus tööle kodukontorisse. Kuigi COVID-19 mõju kaugelt töötamisele on enam-vähem mõõdetav, siis uuringuid seoses turvalisuse või turvalisuse kontrollimeetmetega väike- ja keskmise suurusega ettevõtetes on tehtud vähe. Läbiviidud uuringu põhjal võib väita, et kriisi situatsioonis kodus töötamise haldamisega ei ole ettevõtetes piisavalt arvestatud ette antud standardite ja raamistikega. Suurtel organisatsioonidel, võrreldes väike- ja keskmise suurusega ettevõtetega, on rohkem ressursse ja ajapikku väljatöötatud mudelid. Ei ole ühtset ning lihtsat viisi kaugtöö turvalisuse hindamiseks ja juhtimiseks. Täpsete suuniste või infoturbe mõõdistamise meetodi puudumine seab väike- ja keskmise suurusega ettevõtete informatsiooni turvalisuse küsimärgi alla. Käesoleva töö tulemusena on olemasolevate kaugtöö turvalisuse standardite ja raamistike baasil välja töötatud lihtne ning uudne turvalisuse hindamise mudel. Antud mudelit valideeriti pilootprojekti raames, mis hõlmas endas intervjuusid IT- ja infoturbejuhtidega ning põhjalikku küsitlust lõpp-kasutajate seas. Analüüsi tulemusel anti väike- ja keskmise suurusega ettevõtetele turvalisuse tõstmiseks juhised koos uuringu tulemustega. Lõputöö annab lähteanalüüsi üheksale organisatsioonile Eestis, pakkumaks aimdust infoturvalisuse hetkeolukorrast kodus töötamisel väike- ja keskmise suurusega ettevõtetes. Pilootprojekti märkimisväärsed leiud sisaldavad endas kaugtööst põhjustatud kommunikatsiooniprobleeme, mistõttu mõned lõpp-kasutajad ei ole teadlikud kehtestatud reeglitest; või organisatsiooni luhtunud katseid juhendamaks koduse internetivõrgu turvalisemaks muutmisest. Lisaks kasutati Pearsoni hii-ruut-testi leidmaks seoseid demograafiliste näitajate, turvalisusega seotud meetmete ja riskikäitumise vahel. Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 52 leheküljel, 8 peatükki, 18 joonist, 5 tabelit.

# Abstract

This study was conducted amid the COVID-19 pandemic, at a time where more and more individuals are teleworking. While the impact of COVID-19 on teleworking is clear, little has been done to examine associated security implications or the security control and measures used by SMEs. A background study was conducted, which found that the security standards or frameworks present are insufficient to manage and assess teleworking during this crisis. Large enterprises have abundant resources and mature security model but is not same for SMEs. There is no simple and easy approach to assess and manage the security while teleworking. The lack of clear guidance or methods to measure SMEs' security position to take appropriate action may pose a threat to organizations' information security. This study has developed a novel and simple security assessment model based on the existing security frameworks and standards for teleworking. The assessment model was validated by carrying out a pilot, which included a series of interviews conducted with security/IT managers and surveys conducted with their end-users. A list of controls based on existing frameworks and the pilot study was then proposed, which SMEs can use to tighten security during this crisis. The thesis provides benchmark data and analysis from a sample of 9 Estonian SMEs to gain insight into the current information security posture regarding teleworking in the SMEs. The pilot's significant findings included communication problems when teleworking due to some end-users not being aware of the controls, and organizations have failed to issue guidelines for aspects such as security of home networks. In addition, Pearson's chi-square was used to find associations between demographic factors and security-related measures or the practice of risky behaviors. The thesis is in English and contains 52 pages of text, 8 chapters, 18 figures, 5 tables.

# List of abbreviations

BIOS	Basic Input/Output System
BYOD	Bring Your Own Device
CIS	Critical Security Controls
COBIT	Control Objectives for Information Technologies
DDoS	Distributed Denial of Service
DNS	Domain Name Server
ENISA	The European Network and Information Security Agency
EU	European Union
FBI	Federal Bureau of Investigation
HW	Hardware
ICT	Information and Communications Technologies
IEC	International Electrotechnical Commission
IPSec	Internet Protocol Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
MAM	Mobile Application Management
MDM	Mobile Device Management
MFA	Multi Factor Authentication
NAC	Network Access Control
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OS	Operating System
PCI	Payment Card Industry
PC	Personal Computers
RDP	Remote Desktop Protocol
RQ	Research Question
SMEs	Small and Medium Enterprises
SOC1	Service Organization Controls 1
SP	Special Publication

SSID	Service Set Identifier
SSL	Secure Sockets Layer
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
USA	United States of America
UK	United Kingdom
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WHO	World Health Organisation
WPA	Wi-Fi Protected Access

# Table of Contents

<b>List of Figures</b>	<b>9</b>
<b>List of Tables</b>	<b>10</b>
<b>1 Introduction</b>	<b>11</b>
1.1 Motivation . . . . .	12
1.2 Problem Statement . . . . .	13
1.3 Research Approach . . . . .	13
1.4 Scope . . . . .	14
1.5 Contribution . . . . .	14
<b>2 Telework - Threats and Security</b>	<b>15</b>
2.1 Telework . . . . .	15
2.1.1 Factors affecting telework . . . . .	16
2.1.2 Changes during COVID-19 . . . . .	16
2.2 Security threats amid COVID-19 . . . . .	17
2.2.1 Phishing and Scam Emails . . . . .	17
2.2.2 Malware . . . . .	19
2.2.3 Malicious Domains . . . . .	19
2.2.4 Ransomware and DDoS . . . . .	19
2.3 Security frameworks/standards for telework . . . . .	20
2.3.1 ISO 27000 series . . . . .	20
2.3.2 NIST SP 800 series . . . . .	20
2.3.3 ENISA Guidelines . . . . .	21
2.3.4 PCI Guidelines . . . . .	22
2.3.5 CIS Controls . . . . .	23
<b>3 Assessing Teleworking Posture - Related Work</b>	<b>24</b>
<b>4 Methodology</b>	<b>26</b>
4.1 Limitations . . . . .	28
<b>5 Telework Security Assessment Model</b>	<b>29</b>
5.1 Developing a model . . . . .	29
5.2 Organizational and End-User Assessment . . . . .	33
<b>6 Results and Discussion from Piloting the Developed Assessment Method</b>	<b>34</b>

6.1	Results from interviews . . . . .	34
6.1.1	General overview . . . . .	34
6.1.2	Protection against major threats . . . . .	37
6.1.3	Securing remote access . . . . .	39
6.1.4	Telework client device security . . . . .	40
6.1.5	User control and guidelines . . . . .	42
6.2	Results from end-user survey . . . . .	44
6.2.1	Background of participants . . . . .	45
6.2.2	Usage of telework devices . . . . .	46
6.2.3	Securing Network and Communications . . . . .	47
6.2.4	Reminders/guidelines about phishing and scams . . . . .	48
6.3	Comparing organization and end-user perspective . . . . .	49
6.4	Company, Age, and Gender . . . . .	51
<b>7</b>	<b>Recommendations</b>	<b>57</b>
7.1	Future work . . . . .	59
<b>8</b>	<b>Summary</b>	<b>61</b>
	<b>Bibliography</b>	<b>63</b>
	<b>Appendices</b>	<b>69</b>
	<b>Appendix 1 - Interview Questionnaire</b>	<b>69</b>
	<b>Appendix 2 - Survey Questionnaire</b>	<b>72</b>



## List of Figures

1	<i>User Dispersion before and after COVID-19 pandemic declaration.[4]</i> . . .	11
2	<i>Factors of Telework. Source: Belzunegui-Eraso and Erro-Garcés[13]</i> . . .	17
3	<i>A medical phishing website trying to imitate a legitimate Canadian pharmacy. Source:Checkpoint[29]</i> . . . . .	18
4	<i>Research Approach.</i> . . . . .	26
5	<i>Enterprise controls matrix.</i> . . . . .	31
6	<i>User Guidelines matrix.</i> . . . . .	32
7	<i>Percentage of teleworkers before the coronavirus outbreak in the SMEs.</i> . .	35
8	<i>Percentage of teleworkers during the COVID-19 pandemic.</i> . . . . .	35
9	<i>Summary of responses: State of policy for teleworking.</i> . . . . .	37
10	<i>Summary of responses: Usage of remote access methods.</i> . . . . .	39
11	<i>Controls to secure data on telework devices.</i> . . . . .	42
12	<i>Release of guidelines or awareness programs for users teleworking during COVID-19.</i> . . . . .	42
13	<i>User Demographics: Age Group and Gender.</i> . . . . .	45
14	<i>Frequency of telework: before and during the pandemic.</i> . . . . .	45
15	<i>Usage of removable storage device while teleworking.</i> . . . . .	46
16	<i>Measures used by end-users to secure mobile device and communication.</i>	47
17	<i>Provision of MFA for network access to the organization.</i> . . . . .	48
18	<i>Authentication type for home networks</i> . . . . .	48

## List of Tables

1	<i>Network Security Checklist. Source:Telework and Small Office Network Security Guide[47]</i> . . . . .	23
2	<i>Summary of responses: adherence to data security standards</i> . . . . .	36
3	<i>Result of Pearson's Chi-Square : Company Affiliation</i> . . . . .	52
4	<i>Result of Pearson's Chi-Square : Age</i> . . . . .	53
5	<i>Result of Pearson's Chi-Square : Gender</i> . . . . .	54

# 1. Introduction

A pandemic is a crisis that arises from a widespread disease or plague in a vast region, for example, in multiple countries or continents. In December 2019, an outbreak of pneumonia was reported from Wuhan in China, which was later termed COVID-19. COVID-19 is the infectious disease caused by a novel coronavirus, namely severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2)[1, 2]. COVID-19 was characterized as a pandemic on 11th March 2020 by the Director-General of WHO[3]. Governments across the world are trying to contain the spread of the virus. In several countries, the government imposed a national emergency to lock-down people into their homes and shut down businesses, airports, and public places. The pandemic is compelling people to step out of their comfort zone. Organizations struggling to survive are now forced to arrange their day-to-day business by moving from office to teleworking. Figure 1 shows a graph from the report[4] by Netskope Threat Labs on the increase in teleworking due to the COVID-19 situation. The graph represents user dispersion level from August 2019 to May 2020.

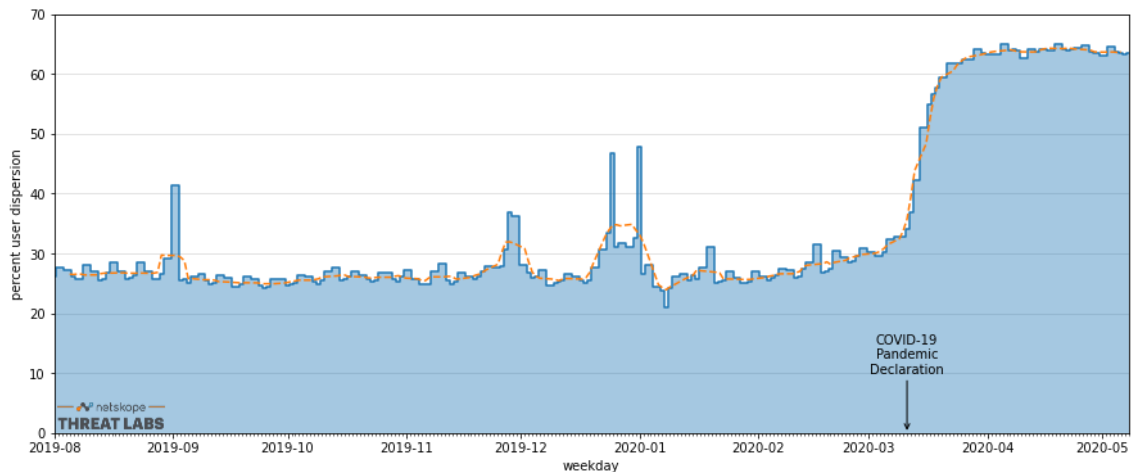


Figure 1. *User Dispersion before and after COVID-19 pandemic declaration.*[4]

Organizations have made sudden changes and challenging steps to support their business continuity. There has been an increase in the use and demand of software and solutions, which provide the ability to work, collaborate, and communicate remotely. Zoom, Slack, Microsoft Office365, and others have reported an increase in demand as companies increase their teleworking capabilities[5]. The changes in operating models of a business-such as remote work solutions, communication, and file-sharing platforms, lead to unintended growth in the threat landscape[6]. For instance, a video conferencing application, Zoom, saw a spike in the number of daily users after the coronavirus outbreak. Security vulnerabilities in the software were reported and disclosed by security professionals while the number of users climbed to 200% at the end of March 2020[7, 8]. FBI issued a warning to Zoom users after receiving multiple reports of conferences being disrupted by pornographic or hate images[9]. As a result, Zoom was banned by several companies such as NASA, Google, SpaceX, and countries, including the USA and Taiwan[10]. Such security incidents increased during the COVID-19 situation and made studies on teleworking's implications highly relevant and significant. Other factors that motivate to carry out studies in this field are discussed below section 1.1.

## **1.1 Motivation**

According to a report[11] on COVID-19 by Deloitte:

- The percentage of remote workers around the globe before the COVID-19 outbreak was 27%. As of 31st March 2020, more than 60% of users work remotely.
- Between March 13-26, 2020, there were over +400K incidents of spam emails about COVID-19. (Demography: Government, Public Sector, Banking | North America, Europe)
- Without IT's knowledge, 1,000+ insecure personal devices connect to enterprise networks every day in 30% of the US, UK, and German companies.

During the COVID-19 pandemic, all types, and sizes of organizations have implemented teleworking practices to support business continuity. Micro-firms have been using teleworking due to their informal structure, non-existent corporate hierarchies, and minimizing operational space expenditures. On the other hand, large and multinational firms provide an option to telework to address work-family issues and commute factors. Large companies also have abundant resources to fund the expertise and technology platforms needed to implement teleworking. It has been stated in a previous study that the provision of telework is more likely in micro and large, multinational firms as compared with small and medium-sized firms[12]. A recent study on teleworking during COVID-19 stated that large and multinational organizations were in a good situation to implement teleworking

on a massive scale[13].

Considering the above given statistics and points, a study on teleworking and the security implications of COVID-19 would be an interesting and timely topic to study.

## **1.2 Problem Statement**

Teleworking increased by leaps and bounds during the COVID-19 crisis, therefore understanding of information security posture is vital. However, there are not many guidelines for SMEs for easily to measure/evaluate their information security posture. As a novel approach, the thesis examines SMEs' information security posture by identifying the information security controls applied and examines user awareness compared to described and implemented controls by the company. This thesis addresses the following research questions:

- 1. What is telework and how is it different during the COVID-19 pandemic? What security threats are prevailing during the COVID-19 pandemic?*
- 2. What information security frameworks/guidelines are present in relevance to telework?*
- 3. How can existing frameworks be used to create an assessment model for telework security including enterprise and end-user perspective? How can this assessment model be validated for SMEs?*
- 4. How do demographic factors including age, gender, and company affiliation relate to knowledge of security and related measures or the practice of risky behaviors?*

## **1.3 Research Approach**

Recent and previous literature was studied and discussed to answer RQ1 and RQ2. The answer to these questions provides a strong base structure for the study and points why its significant to carry out a study on security management for telework during the pandemic. An assessment model in the form of a matrix was designed based on control and recommendations from various frameworks to answer the first part of RQ3. The second part of RQ3 was answered by a series of interview with IT/Security Managers and a survey with the end-users of the 9 SMEs. The data-set from the end-user survey was used to find interesting demographic relations that answer the RQ4. The detailed research methodology is described in chapter 4.

## 1.4 Scope

The study identifies security aspects related to teleworking during the COVID-19 situation. As mentioned previously, SMEs are less prepared for teleworking as compared to micro and large enterprises. Therefore, the author decided to carry out a study focusing on the security implications of telework during this pandemic in SMEs. Since the author is based in Estonia while carrying out this research, a series of interviews with IT/Security managers and a closed-survey of 112 end-users was done from 9 SMEs located in Estonia. The SMEs are not defined uniformly, but the general categorization is based on the number of employees and the turnover/balance sheet. The EU commission categorizes SME as an enterprise with less than 250 employees and an annual turnover of less than or equal to 50 million euros[14]. This study follows the same categorization as defined by the EU. Although BYOD's provision is an integral part of telework arrangements in many organizations, it has been excluded in this study to limit the scope. BYOD is a concept that enables employees to utilize their personally-owned technology, devices such as smartphones and laptops to stay connected to, access data from, or complete tasks for their organizations[15].

## 1.5 Contribution

The study contributes to the literature and information security management while teleworking in many ways:

- The study shows that information security is important to teleworking as it is vulnerable to various threats and cyberattacks. Various data security frameworks and guidelines have been examined to provide a matrix with a set of security controls to help manage security.
- The questionnaires were developed based on frameworks to assess security posture in SMEs when teleworking.
- A series of interviews and a survey done with 9 SMEs from different sectors were conducted to examine the matrix's security controls and their relevance to SMEs.
- The thesis provides recommendations on a set of controls for SMEs based on analysis of results from interviews, end-user surveys and existing security frameworks and guidelines.
- The examination of the associations between a company, age category, and gender and measures relating to security and risky behaviors help expand this area of literature by presenting the measures which relate to a company and the demographic measures which do not. This helps to provide insight into which company, age groups, and gender may be at higher risk in security and risky behaviors.

## 2. Telework - Threats and Security

In this chapter, we aim to answer RQ1 and RQ2 using the existing literature. The chapter will discuss the telework arrangement, various factors that affect it, changes during the COVID-19 crisis, security threats associated, and the frameworks for secure telework practices.

### 2.1 Telework

Telework is not a new working arrangement, and it was initially developed in the 1970s, where it was defined as a decentralized phenomenon based on augmented-decentralization [16]. Telework does not have any universally accepted definition stated in studies conducted in the past [17]. According to [18], most of the studies conducted are heavily based on personal experiences rather than existing theories and research. The study lists various attempts to define telework and adds to the list with a multidimensional definition. It states that telework is a multidimensional phenomenon involving ICT usage, Knowledge intensity, Intra-organisational contact, Extra-organisational contact, and location.

**Telework is a working arrangement conducted outside the employer's locations using information and communications technologies.**[19]

Telework is associated or referred to using other terms, including "telecommuting", "remote work", "distance work", and "work from home" [13]. The term 'telework' has been used to cover a diverse set of situations. The situations are based on the type of working arrangement which differs in scope and structure. Previous studies [20, 21] have classified telework based on four such arrangements:

1. *Electronic home-work*. The most common form of telework is also known as work from home. This is practiced at home by an employee using it.
2. *Satellite centers*. These refer to separate units of an enterprise geographically removed but have constant electronic communication to the organization's central premise.
3. *Neighbourhood centers*. Share space belonging to various employers or entrepreneurs. These are located near the user's home and used for other community purposes like teleservices, and tele-education.
4. *Mobile work*. Refers to work done while traveling or work that involves traveling. It

is done using electronic communication facilities to access emails and other services hosted by their headquarters.

They are different forms of telework, but they share similar goals, like work flexibility, reduced business costs, increased productivity, employee retention, and the elimination of commuting time [22]. **This study is focused on regular electronic home-work or home-based telework as it is the arrangement or technique relevant to the COVID-19 crisis.**

### **2.1.1 Factors affecting telework**

Various factors affect telework, and these could either be the driving factors of telework or factors that directly or indirectly affect teleworking quality and efficiency. In 1997, Baruch and Nicholson[23] presented a framework with four elements of teleworking, as follows:

1. *Situation: Personality; Individual.* Individual factors used in previous researches, such as identifying traits, skills, and situations for the determination of individuals who qualify for telework.[21, 24]
2. *Culture: Strategy; Organization.* Organizational factors are one of the foundations of telework, comprising real estate cost reductions, skill retention, increased productivity, and fewer absenteeism [20, 22].
3. *Technology: Nature; Job.* Technology plays a vital role in the proposition and expansion of telework in organizations. Most of the past studies, including[16, 13], stated the expansion of telework would accelerate with the improvement in and development of ICTs.
4. *Home and Family.* telework has provided flexibility to perform home-family related tasks but has severe implications for the relationship between family members[25].

### **2.1.2 Changes during COVID-19**

The working condition of teleworking during COVID-19 cannot be compared to teleworking under typical circumstances. Telework during the pandemic is not seen as a free choice or alternative working arrangement but as a directive from authorities and employers. The COVID-19 crisis has given rise to new factors due to this unprecedented situation. A recent study[13] based on telework highlighted these factors and complemented Baruch and Nicholson's framework[17].



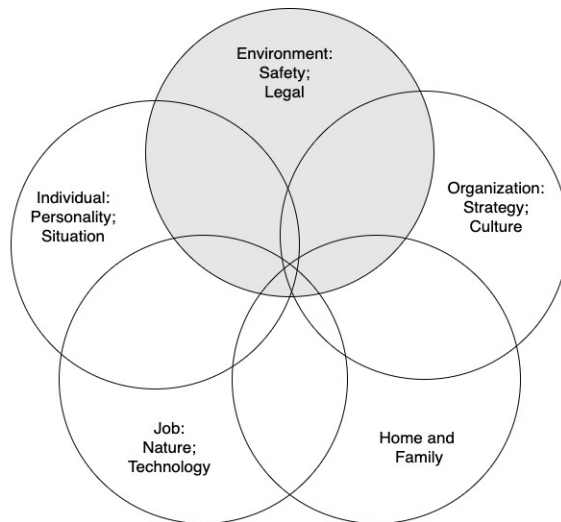


Figure 2. *Factors of Telework. Source: Belzunegui-Eraso and Erro-Garcés[13]*

The environment has always been a crucial element in the emergence of telework. In the 1970s, the focus was on reducing economic activities' environmental impact and teleworking contributed to limiting the effects.[23] Nevertheless, the safety and legal issues that have emerged during the COVID-19 have never been discussed.

The study[13] stated that telework has no significant cases in the past, where it was implemented as a result of a health crisis. A legal issue arises as people are not allowed to leave their homes, forcing them to work from home.

## 2.2 Security threats amid COVID-19

One of the major changes encountered during the COVID-19 crisis is that the largest number of employees were forced to work from home compared with any other time in recent history. Since employees around the globe are working remotely and spending most of their time on the internet, malicious actors found an opportunity to exploit this situation[26]. According to an Interpol report[27], 907,000 spam messages, 7,373 malware incidents, and 48,000 malicious URLs related to the COVID-19 pandemic were detected by one of its private-sector partners between January and 24 April 2020. This section discusses security threats and attacks that are prevalent during the COVID-19 pandemic.

### 2.2.1 Phishing and Scam Emails

Phishing attempts to lure users into providing sensitive information such as credit card details, passwords, and personal information by posing as a legitimate entity. Phishing and scam emails have been a significant threat in ordinary times as well as times of

emergency. During the COVID-19 crisis, people have been under social isolation and have experienced fear and panic, which has given the attackers an advantage. The use of COVID-19 in phishing attacks first surfaced in Japan in late January 2020[28]. The COVID-19 themed phishing emails mostly impersonate health and government authorities claiming to provide information and recommendations regarding the pandemic. Recent campaigns have been focused on coronavirus vaccine-related information and domains. Checkpoint[29] reported one such example where emails with the subject “UK coronavirus vaccine effort is progressing badly appropriate, recruiting consequence and elder adults” were used to redirect traffic to a medical phishing website shown in Figure 3.

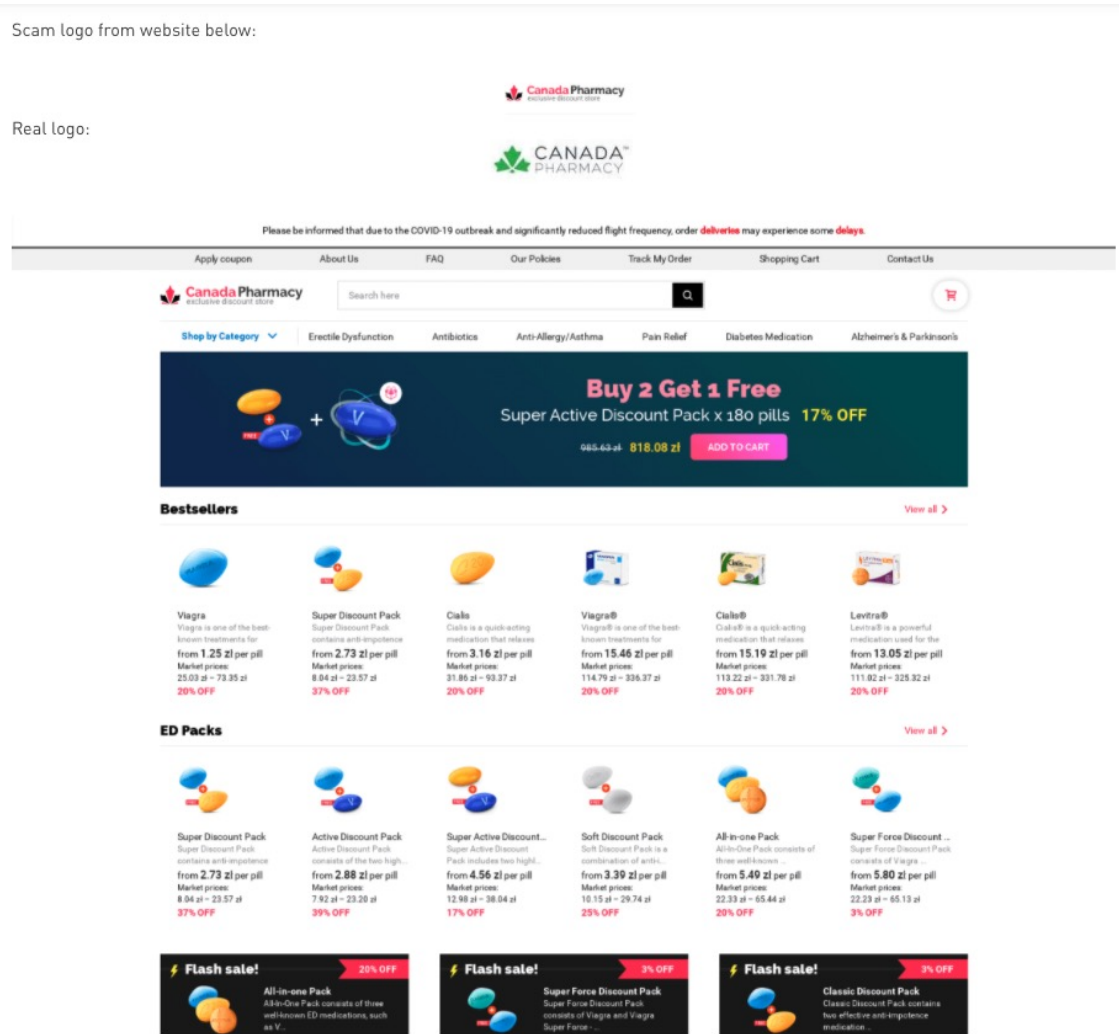


Figure 3. A medical phishing website trying to imitate a legitimate Canadian pharmacy. Source:Checkpoint[29]

### **2.2.2 Malware**

Coronavirus has been used as a lure to spread malware through embedded interactive coronavirus maps and websites. Remote Access Trojans, Spyware, and Banking trojans are being used to infiltrate systems using the COVID-19 guidelines and information as a lure to compromise networks, steal money and data, and build botnets[30]. For example, Johns Hopkins University developed an interactive map to track the number of infected cases globally, which was embedded with java-based malware by hackers[31]. The coronavirus-themed phishing campaign, which targeted Japan, included a malware called "Emotet" as an attachment pretending to be sent by a Japanese disability welfare service provider. Emotet is an old, advanced, self-propagating, and modular Trojan, originally a banking Trojan. It has been used recently to harvest user credentials and financial information and allows hackers to use the computer for malware attacks against other targets[28].

### **2.2.3 Malicious Domains**

There has been a significant increase in domains registered with words such as ‘coronavirus’, ‘corona’, and ‘COVID’ since January 2020. The deceptive internet domains are similar to COVID-19-themed phishing claiming to provide guidelines, COVID-19 updates, and statistics[28]. These domains exploit distress and panic, taking advantage of the public’s thirst for information during the COVID-19 crisis. The malicious domains are used for different scams, host data harvesting malware, honeypots for targeted users, and to obtain personally identifiable information and use it for their intended purposes[31].

### **2.2.4 Ransomware and DDoS**

Most critical and emergency response institutions, such as government organizations, hospitals, and medical centers, which are overwhelmed with the health crisis, are being targeted by DDoS and ransomware attacks[31]. The ransomware or DDoS attacks do not typically aim to steal information but prevent it from accessing critical data or disrupting the system, worsening the impact during a situation like the COVID-19 crisis. A recent example of this happened when a ransomware attack targeted The Duesseldorf University Clinic in Germany, which crippled the hospital’s IT network. Due to disruption, the hospital turned away a woman in need of emergency treatment who died while going to another city. It is reported as the world’s first healthcare cyberattack death[32].

## **2.3 Security frameworks/standards for telework**

Security frameworks or standards are a series of documented processes used to define policies and procedures to ensure information security in an organization. During the COVID-19 crisis, organizations such as ENISA and PCI also released security guidelines while teleworking. This section highlights some of the frameworks and guidelines for the secure implementation and practice of teleworking.

### **2.3.1 ISO 27000 series**

The ISO 27000 series are security standards developed by the International Standards Organization. ISO/IEC 27001:2013[33] is a security specification document published in 2013 which provides requirements for an information security management system (ISMS). Teleworking is mentioned in the list of ISO 27001 controls in Annex A. Control A.6.2.2 (Teleworking) refers to developing a policy and measures to protect the information accessed, processed, and stored on teleworking sites. In addition to this, control A.6.2.1 (Mobile device policy) refers to the development of policy and supporting measures to be adopted to manage the risks posed by mobile devices[34]. ISO/IEC 27002:2013[35] is a code of practice document that provides guidelines for information security management practices, including selecting, implementing, and managing controls. The standard gives detailed guidance for implementing the controls listed in Annex A of ISO/IEC 27001:2013 document. The guidelines and arrangements discussed in section 6.2.2 (Teleworking) of the ISO/IEC 27001:2013 document include:

- Physical security of the teleworking site.
- Classification of information and services that are authorized to access and stored.
- Securing remote access methods.
- Backup procedures.
- Audit and security monitoring.
- Hardware and software support and maintenance.
- Rules and guidance on family access to equipment and information.
- Use of home networks and requirements on the configuration of wireless services.

### **2.3.2 NIST SP 800 series**

NIST SP 800 series is a catalog of guidelines, technical specifications, and reports of NIST's security activities. NIST SP 800-46 Rev.2[36] is a technical specification document published in July 2016 which provides a guide to secure telework, remote access methods,

and BYOD technologies for enterprises. The document[36] discusses security concerns and controls with relevance to telework, which includes:

- *Vulnerabilities and Threats* The threats to technologies used in telework arrangements are described, such as the lack of physical security controls, unsecured networks, infected devices in the internal network, and external access to internal resources of an organization.
- *Remote Access Methods and Security* Remote access methods such as tunneling, application portals, and remote desktop access should be used with their best implementation practices. Secure controls and implementation for remote servers is described with details on remote access authentication and communications encryption.
- *Client Device Security* Security guidelines of devices such as PCs and mobile devices used while teleworking should be controlled by organizations using MDM solutions. The information on devices should be protected using encryption techniques and backups.

NIST SP 800-114 Rev.1[37] is a guide for end-users to ensure telework and BYOD security. The document[37] focuses on end-user controls and guidelines to secure information such as:

- *Securing Information* This section includes physical security controls for the telework device and location. Encrypting information on telework devices and removable media used, backing up information, and destroying the information when no longer needed.
- *Securing Home Networks* discusses changing default credentials for network devices like the router and applying updates regularly. The use of robust authentication methods such as WPA2 is also discussed.

### **2.3.3 ENISA Guidelines**

ENISA[38] is the EU agency for cybersecurity located in Greece. Guidelines[39, 40, 41] which include recommendations for employers as well as staff on teleworking, were released to follow secure practices during the pandemic:

*For employers*

- Securing business applications via encrypted channels such as SSL VPN, IPsec VPN. Ensure that the VPN solution can sustain a large number of simultaneous connections.

- Access to application portals should be secured using multi-factor authentication.
- Prevent Internet exposure of remote system access interfaces (e.g., RDP).
- Securing the endpoints, for example, installing antivirus software.
- Mutual authentication is preferred when accessing corporate systems (e.g., client to server and server to client).

*For staff*

- Exchange of sensitive corporate information through secure connections only.
- Encrypting the data at rest, e.g., local drives (this will protect against theft/loss of the device).
- Locking the screen while not in use to avoid use or leakage of information.
- Not using the corporate computer for leisure activities and be particularly careful with any emails referencing the coronavirus.
- Being suspicious of emails could be phishing/scam, especially if they ask to connect to links or open files.

### **2.3.4 PCI Guidelines**

PCI[42] is a security standard council that developed the Payment Card Industry Data Security Standard (PCI-DSS), which is a set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. PCI released guidelines[43, 44] that should be implemented to protect remote workers and their environments. The guidelines are not part of any framework or data security standard, but they provide a good set of instructions to secure teleworking arrangements. Following is a summary of the guidelines issued by PCI:

- Use of multi-factor authentication for all network remote-accesses.
- Enforcing a strong password policy
- Ensure all telework devices have up-to-date patches, anti-malware protection, and firewall functionality.
- Use only secure, encrypted communications—e.g., a properly configured VPN.
- Automatic remote session logout after a period of inactivity.
- Implement a security awareness program to ensure that all personnel is adequately trained and knowledgeable about the business’s security policies and procedures.
- Ensure all personnel use only company-approved hardware devices- e.g., mobile phones, laptops, and systems.

### 2.3.5 CIS Controls

CIS Controls are a set of cyber defense actions recommended by the Center of Internet Security[45] that provide specific and actionable ways to stop the most pervasive and dangerous cyber attacks. The Center of Internet Security has published Telework and Small Office Network Security Guide[46]. The guide aims to assist individuals and organizations in securing the network devices as there is serious security consideration surrounding the usage of devices such as routers and modems. The guide has summarised the controls in the form of a security checklist as in the Table 1.

Table 1. *Network Security Checklist. Source:Telework and Small Office Network Security Guide[47]*

S.No	Network Security Checklist
1	Register your device with the manufacturer
2	Change the default administrative password of all routers and modems to something unique.
3	Use a unique password to access your ISP's web portal.
4	Enable two-factor authentication wherever possible. This may include accessing the ISP web portal, the router/modem, or a mobile app.
5	Change the WiFi network (e.g., SSID) password to something unique.
6	Ensure the WiFi network (e.g., SSID) name does not provide any identifying information.
7	Carefully guard who has knowledge of the WiFi network password.
8	Turn off the 2.4 GHz or 5GHz if you're not using one of them.
9	Move all routers and modems to a location not accessible by the general public or passersby.
10	Enable automatic updates for all routers and modems.
11	Turn on WPA2 or WPA3.
12	Disable WPS if possible.
13	Enable the router and modem firewall.
14	Enable NAT.
15	Enable DNS filtering on the router and/or modem.
16	Disable UPnP

CIS has also published the Implementation Guide for Small-and Medium-Sized Enterprises (SMEs)[45] which contains a small sub-set of the CIS Controls specifically selected to help protect SMEs. Since these controls are not specifically aimed for teleworking but the overall security of organization, they have not been included in this study.

### **3. Assessing Teleworking Posture - Related Work**

Studies conducted in the past on telework and information security have been discussed here, along with the recent studies on teleworking during COVID-19. The amount of research on telework during the COVID-19 crisis is abundant. However, most research done on telework in the context of COVID-19 are based on the general working environment[48], safety[13], and social and psychological issues[49, 50]. For instance, Belzunegui-Eraso and Erro-Garcés[13] conducted an empirical study based on qualitative information to analyze teleworking's implementation as a safety measure during COVID-19. The study adds an essential element - "environment" - to Baruch and Nicholson's[23] framework that describes factors affecting telework. Data from 27 companies, mostly large and multinational companies, were collected regarding the factors that led to telework implementation. The environmental factor, which includes safety and legal issues, was the prominent factor in telework implementation during the COVID-19 crisis. Self-selection bias is present in the study since SMEs are omitted, but they have been described as equally affected and less resourceful. Information control and data confidentiality as issues in the massive implementation of telework during COVID-19 have been mentioned but not applied in the study.

Looking at the studies carried out in the past, Sturgeon[51] in 1996 conducted a high-level threat and risk analysis of telework. Security threats and vulnerabilities existing in teleworking were identified and examined with risks associated with employees working on sensitive information from a remote site. A generic and simplified framework was used for the threat and risk assessment process. A broad set of solutions was suggested for telework risks. A study on small enterprises done at the University of Melbourne[52] also focused on telework risks based on Sturgeon's work and other literature. Security risks were addressed by applying security controls, including developing a telework policy, communication channels, security training, encryption, and securing devices. Risks related to cloud security management are mentioned, but controls are not discussed for the same. The controls suggested have been taken into consideration in this study.

Hatashima and Sakamoto[53] carried out a residual analysis for three user groups to manage information on personal devices while teleworking. The groups were classified based on the presence and absence of company rules and regulations and examined against storage methods and various data sensitivity levels. Employees' behavior has been discussed from the employees' viewpoint, while the company's viewpoint is suggested for



future examination.

A survey on data security practices in SMEs focusing on telework was carried out by Fintan[54] in 2007. A comparison of security practices was made between offsite and onsite employees in different firm sizes, i.e., micro and small. A list of technologies was included in the survey, but the assessment was done based on the "written security policy" and "security training and awareness." A level of discussion on security issues relating to ICT adoption in 19 studies was examined. The study concluded by encouraging more research devoted to information security issues to develop telework practice in SMEs. Although the research focuses on telework, information security, and SMEs, it is less relevant to the current scenario because significant technological advancements have taken place in the past 13 years.

Since telework was never implemented at a massive scale or as a result of a crisis, it is difficult to explain what previous research and theories have to say regarding information security handling while teleworking during a pandemic. This study focused on the security assessment method while teleworking during the pandemic, specifically for SMEs, and considered the end-users and organization's perspective.

## 4. Methodology

The research design has followed a mixed approach to solve the research problem. The mixed approach used has been referenced to the design by J.D Creswell[55]. The study collected qualitative data through interviews, and quantitative data were collected later in the form of an end-user survey. The qualitative approach was used for interviews, as open-ended questions were a better option to gain insight into security controls and measures deployed by SMEs for teleworking. However, the questionnaire was kept close-ended in end-users' case as it is easy to answer and understand. The aim was to verify knowledge and behaviors regarding the security guidelines. The emphasis given to qualitative and quantitative data was equal as they presented different perspectives i.e., enterprise and end-users. Both the qualitative and quantitative data have been analyzed separately and later combined to give final recommendations in the study.

The various steps taken in the research method have been shown in the figure 4.

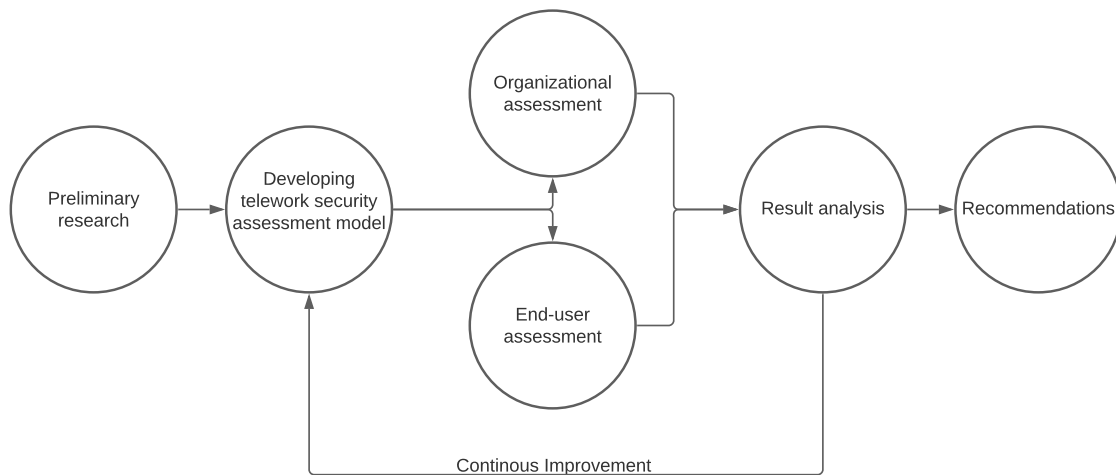


Figure 4. *Research Approach.*

The specific method used to answers the research questions have been described below.  
**RQ1:** *What is telework and how is it different during COVID-19 pandemic? What are the security threats prevailing during the COVID-19 pandemic?*

The study's first step was to conduct preliminary research on telework, telework during COVID-19, and security threats amid COVID-19. This step aimed to understand the concept of telework, to determine how telework during COVID-19 is different from traditional

telework and identify the prevalent security threats during COVID-19. This step was already mentioned in the sections 2.1 and 2.2, and it answers research question 1.

**RQ2:** *What information security frameworks/guidelines are present in relevance to telework?*

The second step involved finding and describing the security standard, framework, and guidelines relevant to telework. The step included a description of telework practices included in the ISO 27000 series, the NIST SP 800 series, and the ENISA guidelines, which was done in the section 2.3 and answered research question 2. This study's second research question consisted of the following:

**RQ3(a):** *How can existing frameworks be used to create an assessment model for telework security including enterprise and end-user perspective?*

The frameworks described in the section 2.3 were used to create a matrix and further two questionnaires to answer the first part of RQ3. The matrix and the questionnaires have been discussed in the chapter 5.

**RQ3(b):** *How can this assessment model be validated for SMEs?*

The second part of Research Question 3 lent itself to descriptive statistics and could be answered solely through descriptive analysis. The analyses conducted to examine these research questions consisted of constructed pie charts for single responses, line charts for multiple responses with the associated percentages being reported, and relevant percentages also reported directly within the chapter 6 text.

**RQ4:** *Does knowledge of security and related measures or the practice of risky behaviors relate to demographic and related measures?*

**a:** *Is knowledge of security and related measures or the practice of risky behaviors associated with the company the respondent is affiliated with?*

**b:** *Is knowledge of security and related measures or the practice of risky behaviors associated with respondent age category?*

**c:** *Does knowledge of security and related measures or the practice of risky behaviors associated with respondent gender?*

Research question 4 and its associated sub-questions were answered using Pearson's chi-square, a bivariate method of statistical analysis. Pearson's chi-square was used to answer this study's third research question, which inquired about the relationship between the demographic and related measures of the company, age group, and gender, and the survey items relating to security and related measures as well as risky behaviors. All bivariate statistics were conducted using Pearson's chi-square as all measures included in this study were categorical, with the majority having a nominal level of measurement. Pearson's chi-square is used in order to determine whether two categorical measures, which can be measured either on the ordinal or nominal level of measurement, are significantly associated[56]. While Pearson's chi-square can be used to determine the association between two ordinal variables[56], a non-parametric correlation such as Spearman's rho can also be

used here[56] and may be considered more typical.

Pearson's chi-square compares actual and expected cell sizes between two measures and calculates, statistically, whether the deviation of the actual cell sizes from the expected cell sizes are large enough to achieve statistical significance[56]. Cell sizes refer to the total sample size associated with each combination, or intersection, of response categories associated with each of the two measures analyzed[56]. Suppose the calculated chi-square value is above a specific threshold, with the threshold depending upon freedom's associated degrees. In that case, the significance will have been achieved at the .05 alpha level, and the result can be said to have achieved statistical significance[56]. Pearson's chi-square is also an omnibus test, referring to the fact that if one or both of the variables included for analysis have more than two categories of response, additional analysis would be required in order to determine between which specific comparisons the significance lies[56].

The results of Pearson's chi-square have been discussed later in section 6.4.

## **4.1 Limitations**

The study has some limitations that have been listed below:

- Although the literature was collected through worldwide research, the interviews with security managers and the survey for users have been restricted to SMEs in Estonia. By examining only this specific area of the world and its focus on SMEs, this study cannot generalize any of the results found beyond this specific population or geographic area.
- The bivariate analyses conducted served to examine the potential for any significant associations between specific measures included in this study. However, as these data were cross-sectional, causality cannot be determined. Instead, these analysis can only be said to examine whether or not a significant association exists between the pairs of measures examined, and if a significant association was found to be present, the nature of that relationship.
- The control and guidelines suggested in the thesis is valid for SMEs as they have been formulated and validated based on similar businesses' know-how.
- The study majorly contributes to SMEs which do not have any provision of BYOD. The control and guidelines regarding BYOD are not studied and discussed in this research.

## 5. Telework Security Assessment Model

### 5.1 Developing a model

This section presents a security assessment model for telework arrangement, developed based on the various controls and practices recommended by frameworks discussed in the section 2.3. This section will answer our **RQ3**: *How can SMEs assess their telework security posture following the requirements from frameworks for enterprise and end-user perspective?*

Although the frameworks defined security management and controls for teleworking, they do not cover all the aspects which are relevant during the pandemic, as discussed below:

- **NIST SP 800 series.** The NIST framework consists of most of the controls and security practices for teleworking. The NIST has two detailed documents focusing on enterprise and user controls. Although it covers most aspects, it does not consider mass teleworking as a pandemic because it was released in 2016.
- **ISO 27000 series.** The ISO does not have a dedicated document for telework practices; the security controls for telework have been mentioned and described briefly in ISO 27001 and ISO 27002. It discusses the matter to be considered when designing a security policy for teleworking. It mostly comprises of organizational aspects and lacks end-user controls.
- **ENISA guidelines.** ENISA[38] has not published any document regarding the security practices or controls for teleworking. However, it released guidelines for SMEs and other entities for secure telework practices for both employers and employees during the pandemic.
- **CIS guide.** The Center for Information Security[45] has a security guide for telework, but it focuses on network setup and configuration.
- **PCI guidelines.** The PCI[42] does not have any specification document but provide some guidelines to secure telework practices during the COVID-19 crisis.

It is clear from the above points that a specific security framework or guideline cannot be used in its entirety to create an assessment model for telework. Therefore, control and recommendations from various frameworks and standards were used to develop a teleworking assessment model. Since the SMEs have limited resources, the constraint

for the developed assessment model includes the ease to implement without significant resources. So they can use the model for conducting regular assessments to implement appropriate controls and plan communication to end-users based on the outcomes.

During the analysis of telework security frameworks/standards, it was discovered that it relies upon the following two aspects:

- *Employer*. This includes the security of enterprise technologies used for telework, such as remote access servers, telework client devices, and remote access communications.
- *Employee*. It refers to users' awareness and recommendations for securing telework computers' OS and applications, as well as home networks.

Based on the above categories, two matrices were developed focusing on enterprise and user controls, respectively. Figure 5 shows the first matrix for enterprise controls of which most have been imported from the NIST guide to Guide to Enterprise Telework[36] as it has detailed descriptions of various aspects and related control for teleworking.

STANDARDS/Frameworks /GUIDELINES FOR TELEWORK	NIST	ISO	ENISA	CIS	PCI
<b>ENTERPRISE CONTROLS</b>					
A policy and supporting security measures to protect information accessed, processed or stored while teleworking.					
<b>Security Against Major Threats</b>					
Physical security controls					
Securing networks					
Restricting external access to internal resources					
User awareness and training					
Audit and security monitoring					
<b>Remote Access Security</b>					
Use of remote access methods such as tunneling					
Remote access server security					
<b>Telework Client Device Security</b>					
Securing telework PCs					
Securing telework mobile devices					
Protecting data on telework client devices					
<b>User Guidelines</b>					
Phishing and scam emails					
Use of network and technologies					
Securing home networks					
Defining the use of devices by family and friends.					

- Control is imported from this framework/standard/guideline
- Control is also mentioned in this framework/standard/guidelines
- Author couldn't find the control listed in framework/standard/guidelines

Figure 5. Enterprise controls matrix.

The second matrix as below in Figure 6 is based on user guidelines for teleworking which contains control, guidelines and recommendations from NIST, ISO and ENISA.

STANDARDS/Frameworks /GUIDELINES FOR TELEWORK	NIST	ISO	ENISA	CIS	PCI
<b>USER GUIDELINES</b>					
<b>High Level Controls</b>					
Segregation of devices					
Physical security controls					
Encrypting files stored on telework devices and removable media					
Ensuring that information stored on telework devices is backed up.					
Avoid exchange of sensitive corporate information through possibly insecure connections.					
<b>Home Networks</b>					
Change default passwords					
Updates and Patching					
Use a WPA2, WPA, or WEP key					
<b>Phishing and Scam Emails</b>					
Be very suspicious of mails if they ask to connect to links or open files.					
Mails sent from people/company you know, but asking for unusual things are also suspect.					

Control is imported from this framework/standard/guideline

Control is also mentioned in this framework/standard/guidelines

Author couldn't find the control listed in framework/standard/guidelines

Figure 6. *User Guidelines matrix.*

The two matrices discussed above are a reference for telework assessment for enterprises and end-users. The first matrix as in Figure 5 is used to develop a open interview whose target audience was IT/security managers or professionals responsible for the security of enterprise technologies. The interview questions were devised based on a matrix shown in Figure 5, which focused on enterprise controls divided into the following categories:

- *Security Against Major Threats*
- *Remote Access Security*



- *Telework Client Device Security*
- *User Guidelines*

The second matrix as shown in Figure 6 was used to develop a questionnaire with mixed questions. The target audience for the questionnaire is the end-user of an enterprise. The questions assessed user knowledge about controls and guidelines issued by their organization.

## **5.2 Organizational and End-User Assessment**

To validate the assessment method developed above in section 5.1, a pilot was carried out for the model, which included a series of interviews with IT/Security managers and a survey of total 112 end-users from 9 SMEs. The data collection was conducted using the survey method. The responses to both the questionnaire as well as the interview were recorded using Google Forms[57]. Initially, the questionnaire and interview were developed and piloted with Company A to understand the challenges and limitations. To overcome the challenges and limitations, the questionnaire was further improved using the recommendations and feedback received. The significant improvements include the addition of the Estonian language to the questionnaire for a wider reach and to restructure the questions to avoid the apparent nature of the questions.

### **Ethical and Privacy Considerations**

- The link to forms to record the survey and the interview was distributed directly to the responsible person via email. None of the links to the survey were posted on the internet or social media platforms.
- Separate links to the user survey were generated for each company to ensure the data's integrity.
- A disclaimer was provided in both the survey and the interview form about using the data collected. It was conveyed that the data collected would be treated confidentially and that the information provided would not allow them to be identified in any research outputs/publications.
- The collected data, which were always anonymous, has been securely kept by the researcher. All relevant data and datasets will be securely destroyed seven years following the completion of this study.

## **6. Results and Discussion from Piloting the Developed Assessment Method**

The results discussed in this chapter are based on the analysis of data collected from the interviews and the survey. The section 6.1 includes descriptions from the resultant interviews. The results include control mentioned by IT/Security professionals in the interview, which has been discussed and compared with the controls present in security standards and frameworks for teleworking. Section 6.2 contains a descriptive analysis of results from the end-user survey. Section 6.3 compares some interesting findings concerning the company and end-user perspective. Therefore, the section 6.1, 6.2 and 6.3 validates the security assessment model for teleworking SMEs answering the RQ3(b).

The author acknowledges that the sample is not sufficient to conclude for all Estonian SME population; however, the below analysis of pilot study results provides a starting point/benchmark for other small SMEs to compare their posture with other companies. This analysis has been used to develop recommendations in Chapter 7.

### **6.1 Results from interviews**

An interview with IT/Security Managers was conducted with a semi-structured questionnaire, as previously mentioned in methodology. A total of 9 responses were recorded from professionals belonging to different companies, 7 are medium enterprises, and 2 are small enterprises. The participants' work in enterprises belonging to different sectors, including computer software, financial services, broadcast media, telecommunications, manufacturing, machinery, and aviation. Although the participants come from different sectors, they all have a common aspect concerning the use of ICT technologies while teleworking. This study focuses on information security while teleworking and will not consider the different sectors of SMEs while concluding the responses.

#### **6.1.1 General overview**

The first section of the questionnaire included closed-ended questions regarding the state of telework in their organization.

How would you define the percentage of people working remotely from home before the outbreak of coronavirus?  
9 responses

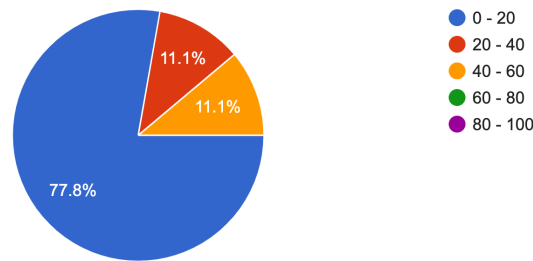


Figure 7. *Percentage of teleworkers before the coronavirus outbreak in the SMEs.*

Firstly, the interviewee was asked to describe the working arrangement in their company before the coronavirus outbreak. The motive here was to see if teleworking already existed in the SMEs before the COVID-19 pandemic. Figure 7 shows that a small percentage of people had the provision of teleworking before the coronavirus outbreak.

Coronavirus outbreak as a pandemic urged governments worldwide to prepare for health emergency with several drastic measures, including the nationwide lockdowns in many countries. As the lockdowns were introduced, a large proportion of the workforce was instructed to stay home and work remotely - if their functions make it possible. As figure 8 shows, SMEs in Estonia also adopted the telework arrangement to ensure business continuity during the COVID-19 pandemic.

How would you define the percentage of teleworkers during the COVID-19 situation in your organization?  
9 responses

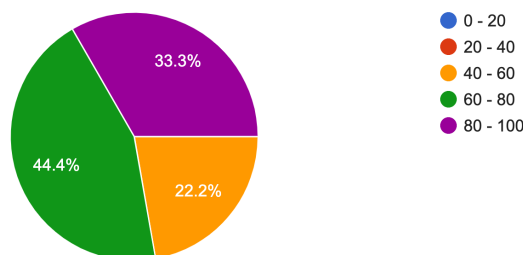


Figure 8. *Percentage of teleworkers during the COVID-19 pandemic.*

The motive behind the above questions was to determine that the interviewee's organization was effected by the coronavirus pandemic and adopted teleworking as a counter-measure. Since the interview and the end-user survey are both made based on controls and recommendations from security standards and frameworks, it is essential to know if the SMEs who participated in the study follow any security standards or frameworks.

Table 2 shows the summary of response from the companies when asked about adherence to data security standards:

Table 2. *Summary of responses: adherence to data security standards*

Information Security Framework/Standards	Number of Responses
NIST	2
ISO 27001	1
PCI	1
ISO 27001 and PCI	2
SOC1	1
Not aware	2

Most of the participant organizations directly or indirectly adhere to NIST/ISO/PCI standards. This does not mean that the enterprise is NIST/ISO 27001/PCI compliant, but they use data security standards to maintain and develop its information security management system.

Moving on, the professionals were asked about the existence of technologies to support teleworking in their organization.

- *Already had enough resources and remote solutions to deal with such situation.* 4 out of 9 interviewees said that their organization had enough resources to deal with the teleworking situation originating from the coronavirus pandemic.
- *Existing technologies and remote solutions were upgraded.* Some companies were already acquainted with the teleworking arrangement but did not have enough resources for a massive increase in the number of teleworkers during the pandemic. 4 participants said that they had to upgrade their existing technologies for teleworking to support their business functions. For instance, an interviewee told the company already had a VPN solution, but it was upgraded as the number of users and bandwidth increased.
- *New remote solutions were bought to tackle the crisis.* 1 out of 9 interviewees said that the company had to buy new solutions for teleworking during the pandemic.

Having technology is not enough; the acceptable use of these computing and telecommunications resources is vital for an organization. The rules and guidelines for all individuals accessing and using an organization's IT assets and resources are defined in an IT or Security Policy. The design of an Information Security Policy is evaluated based on a framework or standard[58]. ISO/IEC 27001:2013 mentions implementing a telework policy through which an organization can develop the rules for the implementation of safeguards to protect information accessed, processed, or stored outside its premise[34]. The NIST Guide to Enterprise Telework[36] also recommends developing a telework

security policy defining forms of remote accesses, device, permissions permitted by an organization for teleworking. A telework policy or telework security policy is essential to secure the information being accessed while teleworking. The next question is based on the existence of telework policy in organizations.

Does your organization have a policy for telework?  
9 responses

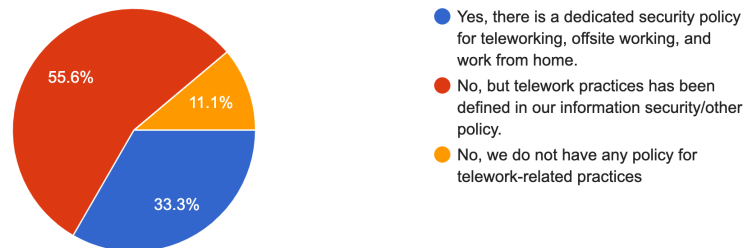


Figure 9. *Summary of responses: State of policy for teleworking.*

As shown in figure 9, most of the firms already have a defined telework practice as the offsite functions have been described in a policy. Nevertheless, it is defined in information security or other policies. However, certain participants state that their company has a dedicated security policy for teleworking and offsite work. Only 1 out of 9 participants said that telework and offsite functions are not defined in their policy.

### 6.1.2 Protection against major threats

This section contained open-ended questions regarding the controls based on major security concerns for telework. The NIST Guide to Enterprise Telework[36] refers to threat modeling for telework to identify the security requirements in teleworking arrangement and technologies. Four major security concerns that have been listed in the guide are very likely to be present in a telework threat model[36]:

1. Lack of physical controls
2. Unsecured networks
3. Infected devices on internal networks
4. External access to internal resources

Firstly, respondents were asked about modifications that have been implemented to access internal resources and how their organizations ensure security over external and unsecured networks while teleworking during the COVID-19 crises. The majority of the organizations ensured that their employees working on the critical data could not access resources outside of their premises, even before the COVID-19 pandemic. However, these employees were

allowed to access the resources through the VPN over multi-factor authentication. Also, businesses strictly ensured that users were logged out from their access module if there was any idle time. Some firms never made any changes as there had advanced telecommuting services. Others made sure that only the company's authorized PC were able to access the company data.

The next question was regarding the telework devices' physical security since these devices' mobile nature makes them more likely to be lost or stolen, resulting in data compromise. Responses to the question were quite common and mutual in regards to physical security controls deployed in the organizations:

- MFA protected logins to their laptops and network. Ensuring BIOS security.
- Full volume encryption using a solution such as BitLocker and FileVault(only for devices with critical data).
- Other common security controls such as passwords, lockscreen, session-logout, Face-ID, and biometric authentication.

However, 22.2% participant stated that there was not any kind of controls for physical security. According to NIST Guide to Enterprise Telework[36] primary mitigation strategies for lack of security controls include device storage encryption at-least for sensitive data and using strong authentication, preferably multi-factor authentication. The ISO/IEC 27002:2013[35] also includes physical security control while teleworking. Although the ISO document stresses the physical security of teleworking sites rather than teleworking devices. Choosing a telework site is not an option during the COVID-19 crisis as the people are restricted to their homes. The standard also recommends physical locks or special locks for devices with sensitive or critical information. Nevertheless, none of the participant organizations had deployed laptop locks or security locks to control physical security while teleworking.

Moving forward in the interview, the participants were asked whether their company had any procedures for securing their company's internal networks from compromised and infected devices. 77.8% of the participants said they had a malware detection or an antivirus solution to deal with telework devices' infections. Additionally, 55.5% also stated that their organization has network monitoring and intrusion detection solutions to counter any compromised and infected devices on the network. The NIST guide[36] recommend the use of anti-malware technologies, such as Antivirus on devices along with NAC solutions to verify the security posture of telework devices before allowing it access to the internal network. The recommendations or security mitigation closely resemble the controls observed in the responses from the interviews.

### 6.1.3 Securing remote access

There are various options for an organization to provide remote access to its computing resources. This section includes questions about the use of different remote access methods and securing them.

Firstly, the participants were asked about the methods used for remote access in their organization. The choices included the remote access methods most commonly used for teleworkers: tunneling, portals, remote desktop access, and direct application access.

What all remote access methods are enabled for users to access the internal resources of your company? (Select all that apply)

9 responses

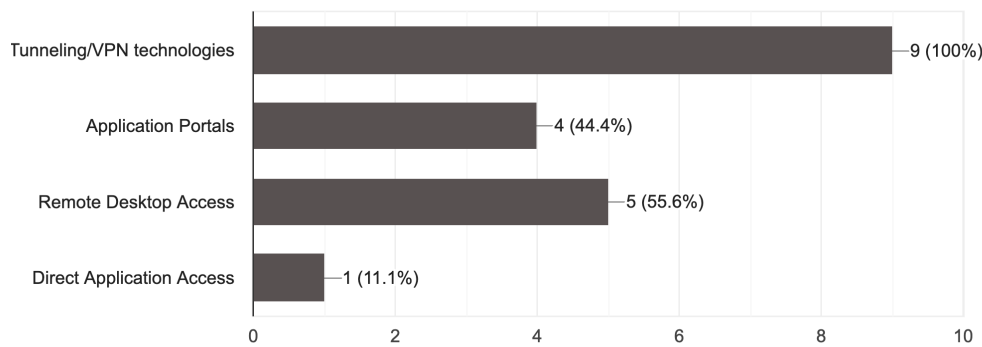


Figure 10. Summary of responses: Usage of remote access methods.

As shown in above figure 10, most SME's use the VPN solution to remotely access their resources. Although application portals and remote desktop access also have a fair amount of usage.

Next, the participants were asked if the remote access method existed before the COVID-19 crisis or were introduced/changed due to teleworking during the pandemic. 44.4% of participants said that there were no changes in remote access methods; they were already being used before the coronavirus outbreak. 33.3% accepted that minor changes were done, such as other VPN access. 11.1% told that direct application access was given by IT to users to support the business functions during the pandemic.

When asked about securing the remote access methods being used, 55.5% said VPN itself is a security control for access to company resources. 44.4% said that the VPN was bundled with strong MFA to ensure security. The interviewees said they were either using third party VPN solutions such as JunosVPN or an in-premise OpenVPN solution. The remote server placement was not discussed as there is little advantage to set up a tunneling server at the edge of a sub-network instead of the network perimeter. In the case of RDP access, it does not involve remote access servers, so there is no issue with the remote access server's placement. Regarding the application portal and direct application access, better

to run those on the organization's perimeter so that the firewall can control access to these servers[36].

The pandemic changes include increased monitoring level and security awareness/training for the remote access of resources. 66.6% interviewees said that they did not encounter any major challenges to main security regarding remote servers. The other reported issues such as decreased visibility on machines and devices security and deployment of security policies on remote access in a small amount of time.

#### **6.1.4 Telework client device security**

In this section, the security of devices such as PC or mobile devices used by a teleworking user is discussed. As told before in scope, this study does not include BYOD device security. A list of controls recommended in the NIST guide[36] was suggested for the questions in this section, but the participants were free to add their controls. The first question was regarding the controls to secure the telework PCs. The choices of answers given to participants are as follows:

- *A properly configured firewall installed and enabled to stop network-based threats.* All the participants agreed with the existence of this control in their organization. Although a firewall is a basic security feature essential in every organization. A single policy firewall for all environments may be too restrictive. The NIST guide[36] suggests firewalls be configured to auto-sense the network devices are connected to and choose security based on that information.
- *A centralized patch management system is applying OS and application security updates.* 88.9% participants told the centralized patch management system provides OS and application security updates to PCs while teleworking.
- *Use their limited privilege accounts for regular work and use a separate administrative account only for tasks that require administrator-level access, such as some software updates.* 44.4% interviewees said that telework users have a different account with limited privileges on their telework PCs. The administrative account is only used for administrator-level access. This security measure reduces the possibility of an attacker to gain administrator access to telework PCs.
- *Enforce session locking, which prevents access to the PC after it has been idle for a period of time.* 55.6% said that session login policy is enforced in their organization. The security measure prevents access to the PC after it has been idle for some time (such as 15 minutes). After a session is locked, access to the PC can only be restored through authentication.
- *Physically security by using cable locks for telework PCs in unsafe external environments.* None of the interviewees choose this control as the provision of using cable



locks by users did not exist in their organization. The option was provided for the question as the NIST guide[36] recommends using cable locks or other deterrents to theft.

The interviewees' above responses demonstrate that most security measures recommended by the NIST guide[36] are present in the organizations. However, control such as cable locks of physical security does not exist in any organization. The NIST guide's security measures are recommendations, and it might not be essential or necessary for an organization. Since none of the organizations have or plan to have this control, it might be excluded from the framework.

The next question was regarding the controls to secure the telework mobile devices in the organization. Following are the responses :

- *Require a password/passcode and/or other authentication before accessing the organization's resources.* 66.7% respondents said that they have some authentication mechanism on their mobile phones.
- *Determine if the device manufacturer provides updates and patches; if so, ensure that they are applied.* 22.2% told that mobile device provided to the user by the organization is from a manufacturer which offers regular updates and patches.
- *Restrict which applications may be installed through white-listing or black-listing.* 33.3% told they control the application being installed on the mobile devices by the user. This implies that the organization is administering the device, and the user has fewer privileges.
- 22.2% said they neither provide mobile devices nor any access to company resources from the mobile devices.

Some participants said that the controls applied are recommended to users, but there is no organization's enforcement. This implies that the organization does not administer the devices. The NIST guide [36]however, recommends the use of MDM and MAM solutions to control and administer the use of mobile devices.

Further in the interview, the participants were asked about controls to protect data on telework devices. The above questions talked about the security of devices; to ensure the overall security; it should also protect the data stored, sent to, or from telework devices.

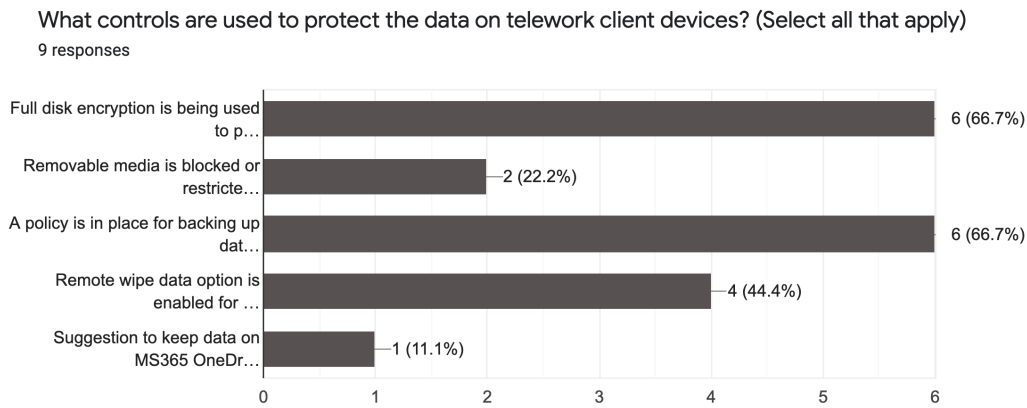


Figure 11. *Controls to secure data on telework devices.*

As shown in the figure 11, 66.67% of interviewees said encryption and backup are used to protect the data on telework devices. Other controls included blocking removable media and remote wipe options for telework devices in case of theft or loss. A participant also mentioned that they encourage their users to store data on cloud applications (such as One Drive by Microsoft) instead of local machines. When asked about the challenges faced regarding the security of telework devices and data on the devices, a participant mentioned asset management, which is being addressed. One participant also mentioned a sharp rise in accidents (such as a liquid spill on devices) due to change in the environment.

### 6.1.5 User control and guidelines

This section includes questions regarding controls and guidelines issued by an organization for end-users while teleworking.

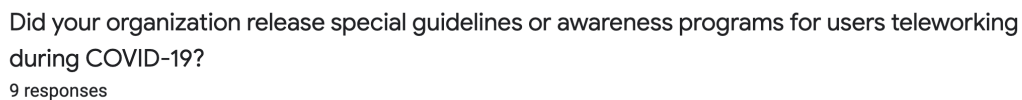


Figure 12. *Release of guidelines or awareness programs for users teleworking during COVID-19.*

As shown in the figure 12, all the companies issued guidelines and training to users while teleworking. The control is crucial as users are not physically present in the company; the IT/security administrators have low visibility on the telework devices. The control is also important as it has been recommended in the NIST guide[36], ISO 27001[34], ENISA[39] and PCI guidelines[43]. The next question was regarding the aspects communicated in the organization's training or guidelines to end-users. A list of controls was provided as a choice, but the interviewees were free to add their controls. Following is a summary of the responses received:

- *Detecting and avoiding elevated phishing threats, including COVID-19 scams and fraudulent websites.* All the respondents said that they issued training or guidelines to detect scams and phishing emails. Phishing emails and scam are a significant threat during the pandemic, as discussed before in section 2.2.1. The security in this regard also depends on user knowledge and behavior.
- *Use of multi-factor authentication wherever possible.* 88.9% made sure that they implemented MFA and communicated users to use it all the potential applications such as VPN and web application portals.
- *Not permitting family members or others to use company-provided equipment, including laptops and phones.* 100% denied the use of machines by kids or other family members. However, during the pandemic, everyone is working or learning from home. The enforcement of this control might be questionable, and end-user behavior is essential.
- *Not copying work files or information to personal devices, including home network drives and personal online storage.* 66.7% encouraged users to use the company provided cloud storage instead of local storage, including removable media and personal cloud storage.
- *Not using company computers for personal email, file sharing sites, or social media without approval.* 44.4% prohibited using company-owned equipment for personal use such as file sharing, social media, and personal emails. However, the control is recommended to end-users; user behavior is a deciding factor in this control.
- *Use of WPA2, WPA or WEP key for home WiFi networks.* 33.3% told that they advised users to use WiFi networks with a strong authentication while teleworking and avoid using open/public networks.
- Other responses included guidelines related to communication applications such as Teams and remote access solutions such as VPN, which was introduced due to telework in the pandemic.

Most of the controls above are recommendations provided to employees by the organization. However, it is not determined if the user follows these recommendations. User behavior

and activity were accessed based on the survey, which is discussed later in section 6.3 of this study.

The next question is regarding user control and activity, where interviewees were asked how they monitor users' activity remotely. 33.3% said they have a security monitoring solution that monitors network traffic and system logs collected through tools such as Suricata, LogCollector, and Graylog. 44.4% told that they audit system and access logs to see if any sensitive information was accessed or modified. One respondent said they use existing solutions such as the Gsuite security center to monitor whether large data is accessed or stored outside the network. Another interesting response was that email and content filtering are in place, but mostly they rely on user goodwill.

The challenges mentioned by interviewees regarding user control and guidelines include monitoring the network 100%, applying changes quickly and effectively. One participant also mentioned the risk of ransomware and other threats to which employees might not be educated properly, especially newly hired who might not be very good at detecting scam and phishing attacks.

## **6.2 Results from end-user survey**

The survey was carried out for the SMEs' end-users to understand their knowledge and behavior regarding the security of organization information and assets while teleworking. A total of 112 responses were recorded from end-users of the 9 SMEs in Estonia.

The participants belong to the nine companies whose IT/Security Manager was interviewed. The survey was forwarded to the users via email by the same. The participants of the survey do not need prerequisites regarding the knowledge of telework and cybersecurity. The users are employees from different departments of the organizations.

The survey(appendix 8) comprised a total of 22 questions divided into four major sections. Participants were made aware of the topic and purpose of the survey. The participation in the survey was not mandatory. The survey was anonymous as it didn't require any identifiable information such as name and email. The survey was kept anonymous to ensure privacy, get better response rates and honest responses. Illustrations as in appendix 8 defining the important terms such as teleworking and telework devices in the survey context were presented before the questionnaire.

## 6.2.1 Background of participants

The first two questions are regarding the demographic factors, including age and gender.

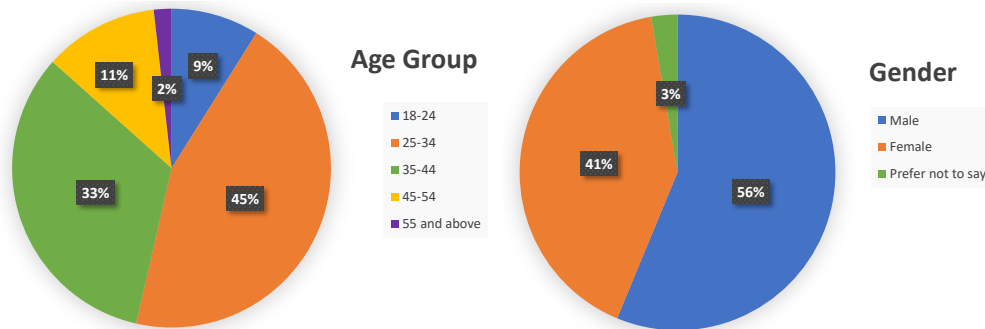


Figure 13. *User Demographics: Age Group and Gender.*

As illustrated in pie chart of figure 13, the age group of the participants is quite varied and dispersed. The gender factor is also distributed quite uniformly for the number of participants. The above factors are important as they could help determine the knowledge and behaviors of different age classes and gender in security while teleworking. The relations between participants' demographics and behavior are discussed later in section 6.4 of this chapter.

Next, the users were asked about the frequency of working remotely before the coronavirus outbreak, followed by the changes that occurred during the pandemic. It is crucial to know if users have experienced a change in the working arrangement that may have led to implications and adversities.

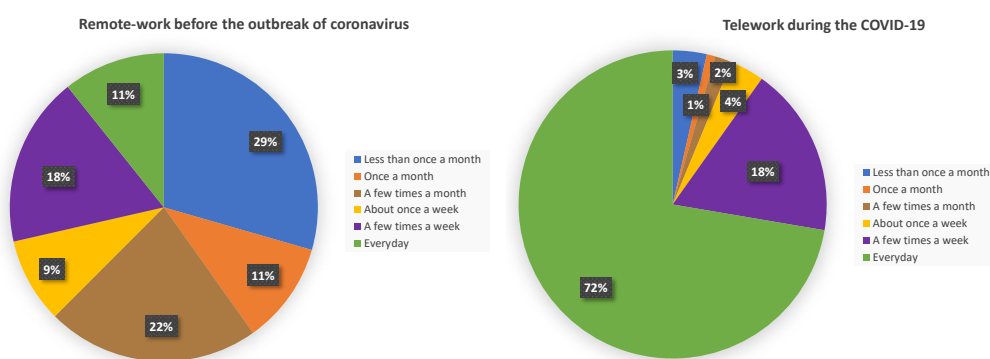


Figure 14. *Frequency of telework: before and during the pandemic.*

The above graphs in figure 14 confirm that users were subjected to change in the work environment, and a large percentage was teleworking during the COVID-19. There is a sharp increase in the number of teleworkers; a similar pattern was observed in the organizations' interview results by IT/Security counterparts.

## 6.2.2 Usage of telework devices

The section includes questions regarding the use and segregation of telework devices and securing information accessed and stored. When asked if the company allowed corporate device such as a laptop for personal use, 59% of the users out of 112 choose yes. 21.4% of the users did not know if the company had allowed corporate devices for personal use. The remaining users, i.e., 19.6%, said that their company did not allow telework devices for personal use. In the interview with IT/Security managers, 100% accepted that their company allows corporate laptops for personal use. However, 41% of the users are either not aware or have misinformation regarding the usage.

Next, the users were asked if the company allowed corporate laptops by kids and other family members. 61.6% said that their company denied the use of company-owned equipment by family and kids. 34.8% users were doubtful about the company's policy regarding the usage of corporate laptops by family and kids. A small percentage, i.e., 3.5%, said that the company had allowed corporate laptops by family and kids during the pandemic. However, all the IT/Security managers had denied using company-owned equipment by friends and family members during the interview. The above responses imply that the users are not aware of the device usage policy as it is not communicated clearly. The ISO 27002[35] states that the organization should issue rules and guidance users regarding family and visitor access to equipment and information while teleworking. In the COVID-19 situation, it gets more important because the user is teleworking daily and surrounded by kids and other family members. During the pandemic, distance learning became a mandatory component of educational institutions such as schools, colleges, and universities around the world[59]. Therefore it is likely that corporate devices being used by family members.

The next question was regarding the use of a removable storage device to store information.

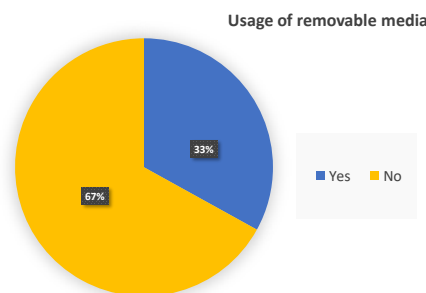


Figure 15. *Usage of removable storage device while teleworking.*

In section 6.1.5, 66.7% interviewees said they encouraged their users to use company-provided cloud storage instead of local storage, including removable media. The result from interviews is equal to the results obtained in the survey in the context of removable

storage use. As shown in figure 15, 33% of users are using local storage devices, which might be subjected to information leakage. However, the use of removable devices is subjected to the nature of the job, but the company should ensure security in such matters. The NIST guide[36] also recommends that an organization should control the use of removable storage devices by either providing the equipment with a strong encryption solution or prohibiting the use.

The interview results regarding mobile device security were noticed; most organizations did not have an MDM solution for teleworking devices such as mobile phones. Therefore, users were asked how they ensure the security and communication of mobile phones.

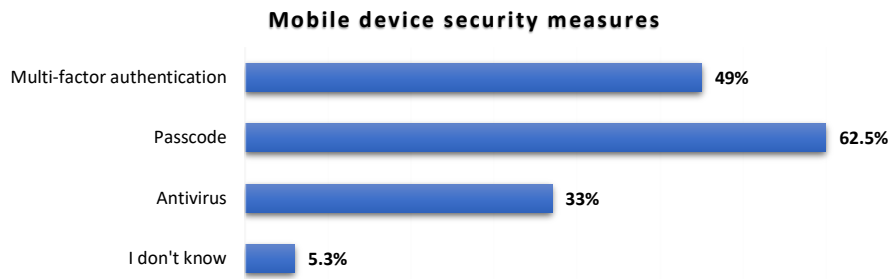


Figure 16. Measures used by end-users to secure mobile device and communication.

A list of choices was given, and users could select multiple answers and add additional measures if they wanted. The graph in figure 16 shows the four major responses received. The above responses imply that many people still lack primary control, such as passcode or authentication mechanisms. 51% do not use MFA for connection to organization network or other applications.

### 6.2.3 Securing Network and Communications

This section examines the user knowledge about organization policies regarding network communications when teleworking. Users were asked if their company had issued any guidelines regarding the use of network and access points. 74% of the users agreed that they received information and instructions to use networks and technologies while teleworking. 17% said they did not receive any guidelines, and 9% said they were not aware of any guidelines issued by their organization regarding network and access points when teleworking.

The next question asked to the users was regarding MFA's presence to connect to the organization's network. The pie-chart in figure 17 shows the percentage of multi-factor authentication for the network; 92% users agreed and confirmed the provision of MFA for network access, whereas 5% denied and 3% do not know about it.

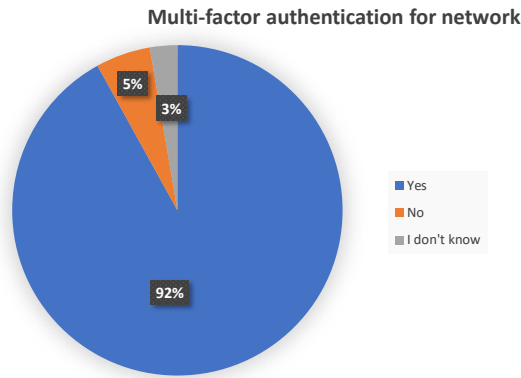


Figure 17. Provision of MFA for network access to the organization.

The following figure 18 examines the authentication type for home networks. Above 52% people use WPA2 authentication for home networks, whereas 38% do not have any knowledge about their network authentication, 6% use WPA, 2% use WEP, and 2% use open networks.

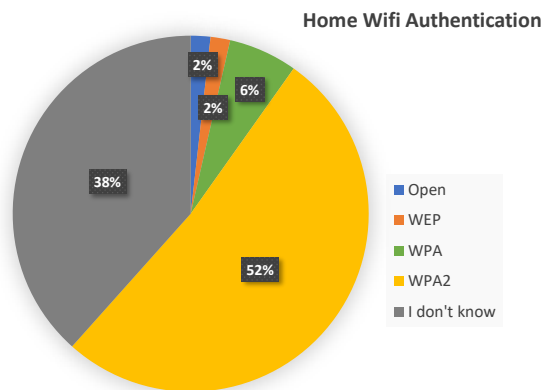


Figure 18. Authentication type for home networks

#### 6.2.4 Reminders/guidelines about phishing and scams

As discussed in the section 2.2.1, phishing and scam is the greatest threat that has emerged during the COVID-19 situation. The section includes the question to analyze user awareness and knowledge of online scams and phishing emails.

Firstly, the user was asked if their organization issued any guidelines and training to identify phishing attempts. Although most users, i.e., 82% agreed, 10% denied, and the rest were not aware of the company's guidelines to identify phishing and online scams. Next, the users were asked if they aware of the term phishing. The users were provided with the following four choices:



1. A type of malware that threatens to publish the victim's data unless a ransom is paid.
2. The process of attempting to acquire sensitive information by posing as trustworthy entity.
3. A technique for catching fish include hand gathering, spearing, and trapping.
4. I don't know

87.5% of the participants choose the correct(second) option. However, 8% choose the incorrect option, and the remaining 4.5% choose the fourth option because they were not aware of the term phishing.

Next, the users were provided with illustrations which help identify a phishing or scam message.

On the next page, users were provided with three images and asked to choose if it were a scam/phishing attempt or an authentic message. Following is the summary of the responses received.

- *First Image.* The image was a phishing email which posing to originate from the WHO to provide safety measures regarding the pandemic. 93.7% of users choose the correct option, whereas 3.5% failed to identify the phishing attempt and the remaining 2.7% said they did not know if it was a phishing attempt or a real message.
- *Second Image.* The second image is also a phishing attempt and posed as a popular payment service asking the recipient to review the account by clicking a link. The majority of users, i.e., 94.6% identified the phishing email, 3.5% users choose the incorrect option, and the remaining 1.9% had no idea about it.
- *Third Image.* The image consists of two similar-looking messages: scam and the other a real message. The users were provided with five choices that included *first is real and second is a scam, first is a scam and second is real, both are a scam, both are real, I do not know.* 63.3% users choose the correct option, 29.4% choose the incorrect option, and the rest 7.3% said they are not aware of it.

From the above responses, it can be said that the majority of users are competent enough to find the common phishing attempts. However, in the case of elevated and advanced attempts, many users fail to identify it.

### **6.3 Comparing organization and end-user perspective**

This section compares the organization's perspective to the end-user perspective. In this section, the result of the interview will be compared to the result from surveys. The dataset from two medium-sized companies is taken for analysis. The number of end-user responses received from the other seven companies is not enough to derive a logical conclusion. The

two companies will be hereafter referred to as Company A and Company B. The number of end-user respondents from company A and B were 39 and 37 respectively. The following is a list of significant findings when the data were compared on different aspects.

- In the interview, both company A and B said that they allowed laptops for personal use but denied the use for kids and other family members. 35.8% of company A and 45.9% of company B users are not aware of family members could use corporate laptops.
- In the interview, the IT manager of company A said that at the start of lockdown, they provided information and guidelines regarding the use of the internet, network technologies. 23% of the users said that there was no information or guidelines for network tools. Usage provided or that they were not aware of it. The interviewee from company B said that their company has been issuing regular guidelines for network and remote solutions since the coronavirus outbreak. The majority of users, i.e.80% accepted that the company issued the guidelines; however, 19% said they did not receive the guidelines or were not aware of them.
- 29.4% of users from both companies A and B were either using wireless with weak security or not aware which security applies to their internet connection or WiFi. The IT Managers agreed they did not issue any information on home or WiFi security.
- From the interview, it was stated that both companies A and B use multi-factor authentication for remote connection to the corporate network. The end-users confirmed the provision of MFA as most of them, i.e., 97.4% and 94.5% of companies A and B respectively, agreed to it.
- Guidelines regarding phishing and scams were issued by both companies A and B. Most of the users knew the concept of phishing and identified an average phishing attempt. However, when presented with an image consisting of a similar-looking scam and original message, 25.7% of company A and 48.7% of company B choose the incorrect option.

From the above statistics, it can be said that most of the employees are aware and adhere to the guidelines issued by their company to ensure information security when teleworking. However, many end-users are still not aware of the security control and practices one should be aware of while working remotely. According to the findings from interviews and surveys, users are not aware of the control when it is either not communicated or described properly; for instance, in the case of corporate devices usage by family and kids and securing home networks.

Communication is a critical aspect while teleworking. Based on the interview, it was identified that the type of communication used by the SMEs to provide guidelines and notifications to its users mostly includes asynchronous communications such as email

broadcast, posting in communication channels such as Microsoft Teams and Sharepoint. It notifies the employees but does not confirm it has been read and conveyed to the masses. Organizations should use unconventional methods such as quizzes and survey to identify the reach of guidelines issued for users while teleworking.

Identifying phishing and scams is another aspect that is important as it is one of the largest security threats amid the pandemic. The security managers should assess the organization's exposure to phishing using tools such as Gophish[60] and King Phisher[61].

## **6.4 Company, Age, and Gender**

In this study, Pearson's chi-square was conducted in order to determine whether (1) security and related measures and (2) risky behaviors were significantly associated with (3) company, age group, or gender.

All measures with missing data, essentially empty cells, needed first to be recoded as missing concerning the specific data points, which was done using SPSS[62], which was also used for all bivariate analyses conducted. This consisted initially of running frequencies on all study measures included in the bivariate analyses to examine all response categories and the associated sample sizes relating to each response category. This was done in order to determine whether there were any response categories present with very low sample sizes, as well as to check for any errors in the data, and to determine whether any response categories needed to be recoded prior to analysis. Several recodes were conducted on the study variables based on a review of these frequency tables. This consisted of the following: first, three individuals did not respond to gender, with these three data points recoded as missing prior to any of these analyses being conducted. Besides, any measures which contain responses of "I don't know" had these specific data points recoded as missing prior to these analyses being conducted. Regarding the question asking respondents which of the following securities apply to their current Internet connection or Wi-Fi, these data were recoded such that WPA and WPA2 were combined into a single WPA2 category, with "Open Access" retained, and with all other categories of response recoded as missing. In addition, the question asking respondents whether they use removable media such as pen drives and external hard drives to store data had data points recoded in the following way: one response of "If it is my personal PC/laptop, then yes. If its corporate laptop, then never" was recoded as missing, with the response of "Private cloud drive for company employers" recoded as "No", a response of "rarely" recoded as "Yes", and a response of "Yes, for working tasks, like HW upgrades, etc. " also recoded as "Yes". Finally, regarding the question asking about multi-factor authentication, the response of "I bought a very secure device in general" was recoded as missing.

The initial set of analyses focused upon the company but only incorporated the companies A and B as in the previous section. While other companies were included in this data set,

they were associated with smaller sample sizes and so were excluded from these analyses such that only these two companies were compared.

Table 3. *Result of Pearson's Chi-Square : Company Affiliation*

Measure/Behaviour	Result of Pearson's Chi-Square
Company allowed corporate computers for personal use during COVID-19	$\chi^2(1)=1.859, p=.173$
Respondent uses the corporate computer for personal use	$\chi^2(4)=10.795, p<.05$
Company allows corporate computers to be used by family and kids during COVID-19	$\chi^2(1)=.786, p=.375$
How often other people access or use the respondent's corporate laptop and PCI	$\chi^2(2)=1.091, p=.580$
Whether respondents use removable media to store data	$\chi^2(1)=11.779, p<.001$
Whether the respondent or company backs up information stored on the telework device	$\chi^2(1)=1.215, p=.270$
Whether the respondent's organization issued guidelines regarding the use of the Internet, network, and access points	$\chi^2(1)=0.97, p=.756$
Whether respondents use their personal devices to communicate with coworkers and share information and PCI	$\chi^2(4)=21.304, p<.001$
The presence of multi-factor authentication wherever possible	$\chi^2(1)=.404, p=.525$
Security associated with their Internet connection or WiFi	$\chi^2(1)=.191, p=.662$

The results from the end-user company affiliation and the behaviours or measures is as shown in table 3. The first analysis, examining the relationship between the company and whether the respondent's company allowed corporate computers for personal use during COVID-19, failed to achieve statistical significance,  $\chi^2(1) = 1.859, p = .173$ . However, the analysis conducted with whether the respondent uses the corporate computer for personal use was found to achieve significance,  $\chi^2(4) = 10.795, p < .05$ . Specifically, those working for Company A were found to be more likely to reply with responses of always, usually, sometimes, and never with employees of Company B more likely to provide responses of rarely. This result indicates that employees of Company A were more likely to use the corporate computer for personal use.

Next, the company's analysis and whether their company allows corporate computers to be used by family and kids during COVID-19 failed to achieve statistical significance,  $\chi^2(1) = .786, p = .375$ . Significant findings were also not indicated in the analysis conducted with how often other people, such as family and kids, access or use the respondent's corporate laptop,  $\chi^2(2) = 1.091, p = .580$ . However, a significant relationship was indicated between company and whether respondents use removable media such as pen drives and external hard drives to store data,  $\chi^2(1) = 11.779, p < .001$ . This result found that employees of Company A were significantly more likely to use removable media such as pen drives

and external hard drives to store data as compared with employees of Company B. The following analysis, conducted between company and whether the respondent or their company backs up information stored on the telework device, failed to achieve statistical significance,  $\chi^2(1) = 1.215$ ,  $p = .270$ .

Significance was also not indicated when examining the association between the company and whether the respondent's organization issued guidelines regarding the use of the Internet, network, and access points,  $\chi^2(1) = .097$ ,  $p = .756$ . However, the following analysis results, focusing upon whether respondents use their personal devices such as their Mobile Phone to communicate with coworkers and share information, indicated a significant association,  $\chi^2(4) = 21.304$ ,  $p < .001$ . This result found employees of Company A to be more likely to respond with always or usually in response to this question, with employees of Company B more likely to respond with responses of never, rarely, or sometimes. The following question, asking about the presence of multi-factor authentication, failed to indicate a significant association,  $\chi^2(1) = .404$ ,  $p = .525$ . Significance was also not achieved in the analysis conducted with security associated with their Internet connection or WiFi,  $\chi^2(1) = .191$ ,  $p = .662$ . The following set of analyses, which incorporated all cases, examined the relationship between age category and gender alongside this same set of study measures.

Table 4. *Result of Pearson's Chi-Square : Age*

Measure/Behaviour	Result of Pearson's Chi-Square
Company allowed corporate computers for personal use during COVID-19	$\chi^2(4)=1.382$ , $p=.847$
Respondent uses the corporate computer for personal use	$\chi^2(16)=10.032$ , $p=.865$
Company allows corporate computers to be used by family and kids during COVID-19	$\chi^2(4)=1.497$ , $p=.827$
How often other people access or use the respondent's corporate laptop and PCI	$\chi^2(8)=1.569$ , $p=.992$
Whether respondents use removable media to store data	$\chi^2(4)=5.722$ , $p=.221$
Whether the respondent or company backs up information stored on the telework device	$\chi^2(4)=5.310$ , $p=.257$
Whether the respondent's organization issued guidelines regarding the use of the Internet, network, and access points	$\chi^2(4)=1.243$ , $p=.871$
Whether respondents use their personal devices to communicate with coworkers and share information and PCI	$\chi^2(16)=21.139$ , $p=.173$
The presence of multi-factor authentication wherever possible	$\chi^2(4)=1.988$ , $p=.738$
Security associated with their Internet connection or WiFi	$\chi^2(4)=10.408$ , $p<.05$

To summarize, with respect to age category as in table 4, significant results were not found when examining this measure alongside the following survey questions: whether the com-

pany allows corporate computers for personal use during COVID-19,  $\chi^2(4) = 1.382$ ,  $p = .847$ , whether they use the corporate computer for personal use,  $\chi^2(16) = 10.032$ ,  $p = .865$ , whether the company allows corporate computers to be used by family and kids during COVID-19,  $\chi^2(4) = 1.497$ ,  $p = .827$ , whether other people access or use their corporate laptop,  $\chi^2(8) = 1.569$ ,  $p = .992$ , whether they use removable media such as pen drives and external hard drives to store data,  $\chi^2(4) = 5.722$ ,  $p = .221$ , whether the information stored on the telework device is backed up by themselves or their company,  $\chi^2(4) = 5.310$ ,  $p = .257$ , whether their organization issued guidelines regarding the use of the Internet, network, and access points,  $\chi^2(4) = 1.243$ ,  $p = .871$ , whether they use their personal device to communicate with coworkers and share information,  $\chi^2(16) = 21.139$ ,  $p = .173$ , and the presence of multi-factor authentication,  $\chi^2(4) = 1.988$ ,  $p = .738$ . In sum, significant results were not found any case with the exception of the final variable, which asked respondents which of the following securities are applicable to their Internet connection or WiFi,  $\chi^2(4) = 10.408$ ,  $p < .05$ . When examining these data, individuals using open access were only found among the age categories of 18 to 24 and 45 to 54, with WPA/WPA2 being used among the remaining age categories of 25 to 34, 35 to 44, and 55 and above. These results indicate that the two middle-age categories only use encryption, while the youngest and oldest groups did not.

Table 5. Result of Pearson's Chi-Square : Gender

Measure/Behaviour	Result of Pearson's Chi-Square
Company allowed corporate computers for personal use during COVID-19	$\chi^2(1)=.635$ , $p=.426$
Respondent uses the corporate computer for personal use	$\chi^2(4)=6.408$ , $p=.171$
Company allows corporate computers to be used by family and kids during COVID-19	$\chi^2(1)=.102$ , $p=.749$
How often other people access or use the respondent's corporate laptop and PCI	$\chi^2(2)=6.562$ , $p=.05$
Whether respondents use removable media to store data	$\chi^2(1)=5.168$ , $p=.05$
Whether the respondent or company backs up information stored on the telework device	$\chi^2(1)=.098$ , $p=.754$
Whether the respondent's organization issued guidelines regarding the use of the Internet, network, and access points	$\chi^2(1)=1.157$ , $p=.282$
Whether respondents use their personal devices to communicate with coworkers and share information and PCI	$\chi^2(4)=2.615$ , $p=.624$
The presence of multi-factor authentication wherever possible	$\chi^2(1)=.217$ , $p=.642$
Security associated with their Internet connection or WiFi	$\chi^2(1)=.674$ , $p=.412$

The final set of bivariate analyses focused upon respondent gender and this measure's

relationship to these other study items. Similar to the analysis conducted with the age category, most of these analyses failed to indicate statistical significance as shown in table 5, suggesting that there was no relationship between respondent gender and these measures relating to security or risky behaviors. These analyses which failed to indicate significant findings consisted of the following: whether the company allows corporate computers for personal use during COVID-19,  $\chi^2(1) = .635$ ,  $p = .426$ , whether they use the corporate computer for personal use,  $\chi^2(4) = 6.408$ ,  $p = .171$ , whether the company allows corporate computers to be used by family and kids during COVID-19,  $\chi^2(1) = .102$ ,  $p = .749$ , whether the information stored on the telework device is backed up by themselves or their company,  $\chi^2(1) = .098$ ,  $p = .754$ , whether their organization issued guidelines regarding the use of the Internet, network, and access points,  $\chi^2(1) = 1.157$ ,  $p = .282$ , whether they use their personal device to communicate with coworkers and share information,  $\chi^2(4) = 2.615$ ,  $p = .624$ , the presence of multifactor authentication,  $\chi^2(1) = .217$ ,  $p = .642$ , or security applicable to their Internet connection or Wi-Fi,  $\chi^2(1) = .674$ ,  $p = .412$ . However, significance was found in the cases of whether other people access or use their corporate laptop,  $\chi^2(2) = 6.562$ ,  $p < .05$ , and whether they use removable media such as pen drives and external hard drives to store data,  $\chi^2(1) = 5.168$ ,  $p < .05$ . In the former case, males were more likely than females never to allow access to their corporate laptop, while with regard to removable media, males were approximately twice as likely as females to use removable media such as pen drives and external hard drives to store data. Previous research has found female employees to be more conforming to good IS practices regardless of their knowledge level[63]. In addition, male employees below 30 years of age who are well educated and held senior positions were inclined not to conform to good IS practices, despite having high IS knowledge. Those of below 30 years of age as well as those above 50 years of age with lower academic qualifications also tended not to conform to IS practices. These findings suggest that future program interventions must cater to different age groups and job positions. Those who were in the higher job positions should also be included in these intervention programs, especially if this group is composed of male employees and those who are below 30 years of age[63].

While our work corroborates some findings of earlier research, our results also answer research question 4 in the affirmative, that (4a) company, (4b) age category, and (4c) gender are contributing independent factors related to risk. As was found in previous research, males and younger users are at greater risk of malware encounters overall, though the direction and magnitude of the gender and age differences varied depending on the type of malware[64]. Interestingly, certain types of malware were associated with nontrivial age differences (e.g. ransomware and rogue malware), whereas others were associated with gender differences that shifted from a risk factor to a protective factor (e.g. adware). While the authors found clear evidence that differences by age group and gender exist in the context of malware victimisation, they also question the origins of these associations,

or their causality. They posit that differences in attitude towards risk taking and differences in computer and Internet usage, which have been reported to change with age and gender, could explain the differences in malware victimisation[64].

Gender and age are two key demographics that predict phishing susceptibility[65]. Specifically, women click on links in phishing emails more often than men do, and also are much more likely than men to continue to give information to phishing websites. In part, this difference appears to be because women have less technical training and less technical knowledge than men. There is also a significant effect for age: participants aged between ages 18 and 25 are much more likely than others to fall for phishing. This group appears to be more susceptible because participants in this age group have a lower level of education, fewer years on the Internet, less exposure to training materials, and less of an aversion to risk. Educators can bridge this gap by providing anti-phishing education to high school and college students[65]. In the current study, age was only found to be associated with Wifi security, which is contrasted with the findings just presented drawn from previous research. In addition, with regard to gender, our study only found a significant relationship between gender and allowing access to their laptop, as well as storing data on removable media. While males presented less risky behavior with regard to letting others use their laptop, they also presented with more risky behavior with regard to storing data on removable media. Overall, these results were in contrast to those found in previous literature. Further research would be required in order to explore the bases behind these apparent discrepancies.



## 7. Recommendations

In the previous section, the controls for enterprise and end-user were discussed from the interview and survey. This section will discuss the various aspects of security while teleworking and list a set of controls that can be used to strengthen or assess the information security posture in SMEs. This list is derived from the matrix of frameworks and results from interviews/surveys. It is based on two perspectives again; employer and employee.

### **Enterprise:**

- *Develop a policy.* A policy that includes but not limited to:
  1. Forms of remote access methods permitted and used in the organization.
  2. Use of telework devices.
  3. Security measures for information accessed and stored on telework devices.
- *Physical Security.* Controls to avoid the use of telework devices when the owner is not around or in case of devices loss and theft, such as:
  1. Enforce session locking on PC after it has been idle for some time.
  2. Encrypt the end-user device's storage or at least the sensitive data on it.
- *Securing Network and Remote Access.* Measures to securely access information while teleworking which may include:
  1. Access to corporate network and applications only via encrypted communication channels (SSL VPN, IPsec VPN).
  2. Avoid direct exposure to remote system access interfaces (e.g., RDP).
  3. Use of multi-factor authentication for all remote network access originating from outside the enterprise network.
  4. Develop rules for access management and enforce them.
  5. Audit and monitor user activities.
  6. Automatically disconnects remote access sessions after a period of inactivity to prevent unauthorized access.
- *Telework Client Device Security.* Defining controls to secure telework devices including PCs and Mobile devices along with the data accessed/stored on them:
  1. Antivirus or Anti-malware must be installed and be fully updated.
  2. Ensuring system and applications are patched and updates.
  3. Data at rest, e.g., local drives, should be encrypted.

4. A properly configured firewall installed and enabled to stop network-based threats.
  5. Use of limited privilege accounts for regular work and use a separate administrative account only for tasks that require administrator-level access, such as some software updates.
  6. Periodic backups of data.
  7. In the case of mobile devices, determine if the device manufacturer provides updates and patches; if so, ensure that they are applied.
  8. Ensuring users have basic authentication on mobile devices and MFA for access to the company's resources.
  9. Use of mobile device management (MDM) and mobile application management (MAM) solutions to strengthen and enforce mobile device security.
- *User Training and Guidelines.* All staff should be notified or trained to be aware of matters including:
    1. Phishing and scam emails.
    2. Usage of remote access and technologies such as VPN and RDP.
    3. Use of home networks such as WiFi and securing them.
    4. Kids and family access to telework devices.
    5. Encouraging users to the company-owned cloud or network storage instead of local and removable media.

### **End-Users:**

- *Phishing and Scam Attempts.* Users should be able to detect and identify attempts of phishing or online scam. Following matters should be taken into consideration:
  1. Pay attention to notification and training's from enterprises regarding phishing attempts.
  2. Be suspicious of emails from unknown people, especially if they ask to connect to links or open files.
- *Physical Security.* Physical security for users is critical, especially if the user lives in a shared space. Following guidelines should be followed:
  1. Lock screen at all times and do not leave the device unattended.
  2. Be aware of surroundings when working on sensitive information such as authentication.
- *Use of Home Networks.* The use of home networks and security requirements for configuration of wireless networks:
  1. Do not use open, free or public WiFi networks.
  2. Ensure that wireless networks use strong authentication such as WPA2.
- *Segregation of Devices.* Apt usage of corporate device and personal devices:

1. Use corporate rather than personal devices where possible.
2. Avoid the exchange of sensitive corporate information (e.g., via email) through possibly insecure connections.
3. Do not allow the corporate computer to be used by family or friends if prohibited by the company. In case of use, supervise the usage to ensure security.

The above control or measures may or may not be included in other policies, but they need to be considered with a different perspective that focuses on telework. For instance, physical control is a ubiquitous control. However, the context changes when teleworking, and organizations need to consider how devices' physical security can be ensured while people are working remotely from home. Similarly, other control could be a part of usual cyber hygiene, but its significance increases when teleworking as there is low visibility on users and their devices.

The findings and discussion of this thesis can be used by policymakers, security and business managers, and cybersecurity researchers as a starting point of discussion for:

1. Understand various security threats that are associated with teleworking arrangements during the COVID-19 pandemic.
2. Understand what frameworks and standards list in terms of controls and guidelines for teleworking.
3. Use the matrix developed in this study to include and check security controls against listing in ISO 27001, NIST, and other security management guidelines in their organization.
4. Design and develop a telework security policy.
5. Reference, the list of controls SMEs, should consider to strengthen and improve their security while teleworking.

## **7.1 Future work**

The future work based on this study could be as follows:

- This study has geographic restrictions and is based on the closed-group survey; therefore, the author suggests a bigger data-set involving different geographic demographics.
- A detailed study focusing on user-behavior and knowledge regarding security while teleworking could give better insights on end-users' viewpoint.
- A study, including a provision of BYOD and related security controls for SMEs can be carried to extend the scope of this study.
- The examination of the relationships between the company, age category, and gender

and security measures, and risky behaviors were only able to examine associations between these measures and not causality as cross-sectional data were used in this study. Future research could expand upon this by incorporating panel data, which would allow for the examination of causal relationships between these measures.

- Future studies incorporating random sampling would allow for the generalization of the larger population's results. This would increase the external validity of the study.

## 8. Summary

The COVID-19 pandemic and its impact on teleworking, as well as the concomitant security implications inherent in teleworking and its recent increase, has served as a significant impetus for this study. Previous literature was used to examine telework and how it is differed during the COVID-19 pandemic, analyzing security threats that commonly surface during the COVID-19 pandemic. It was noted by the researcher that while teleworking has increased sharply in recent times. While the impact of COVID-19 on teleworking is clear, little has been done to examine associated security implications or the security control and measures used by SMEs. In the background study, it was found that there are existing standards or frameworks which guide security in the context of teleworking. However, these are not enough to manage the security for teleworking during the COVID-19 situation. There are controls that organizations might want to edit based on the massive teleworking arrangement during the pandemic. Although teleworking has been present before the COVID-19, the SMEs had the lower provision of this arrangement as compared to large and micro firms. The large enterprises have a mature model and abundant resources to develop and maintain security while teleworking during the pandemic, which is not the same for SMEs. There is no simple and straightforward approach to assess and manage security while teleworking.

The study has developed a novel approach to assess SMEs' information security posture, including both enterprise and end-user perspectives. The assessment model is developed based on existing security standards and guidelines issued during COVID-19 for teleworking. A pilot study for the assessment model was carried out with Estonian SMEs in the form of a series of interviews with IT/security managers and a survey with end-users. The significant finding includes the communication gap when teleworking due to some end-users not being aware of the controls, organizations have failed to issue guidelines for aspects such as the security of home networks and the use of telework devices by kids and family members. This study suggests a list of controls that can be used by SMEs as a reference to improve their security when teleworking. A list of controls based on existing frameworks and the pilot study was then proposed, which SMEs can use to tighten security during this crisis.

In addition, the data collected through the end-user survey was used to determine associations between demographic factors such as company affiliation, age group, or gender and security measures or risky behaviors. Pearson's chi-square, a bivariate method of

statistical analysis, was used to find significant associations in the data-set. Significant findings include the relationship between gender and allowing access to their laptop, as well as storing data on removable media. While males presented less risky behavior with regard to letting others use their laptop, they also presented with more risky behavior with regard to storing data on removable media.

This study explored the security aspects for teleworking, considering the enterprise and end-user perspectives, further guiding SMEs to help improve their information security in the new normal '*teleworking era*'.

## Bibliography

- [1] *WHO Statement regarding cluster of pneumonia cases in Wuhan, China*. URL: <https://www.who.int/china/news/detail/09-01-2020-who-statement-regarding-cluster-of-pneumonia-cases-in-wuhan-china> (visited on 05/19/2020).
- [2] Thirumalaisamy P. Velavan and Christian G. Meyer. *The COVID-19 epidemic*. Mar. 2020. DOI: 10.1111/tmi.13383.
- [3] WHO World Health Organization. *WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020*. 2020. URL: <https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020> (visited on 03/30/2020).
- [4] *Remote Work Increasing Exponentially Due to COVID-19 - Netskope*. URL: <https://www.netskope.com/blog/remote-work-increasing-exponentially-due-to-covid-19> (visited on 05/25/2020).
- [5] *Coronavirus Impact Index by Industry | Computer Economics – for IT metrics, ratios, benchmarks, and research advisories for IT management*. URL: <https://www.computereconomics.com/article.cfm?id=2788> (visited on 04/08/2020).
- [6] Deborah Golden. “Cyber Management Critical for Remote Workforces - CFO Journal. - WSJ”. In: *The Wall Street Journal* (2020). URL: <https://deloitte.wsj.com/cfo/2020/04/03/cyber-management-critical-for-remote-workforces/>.
- [7] *How COVID-19 Is Changing the Way We Work: Zoom Boom + MFA is the Way | Okta*. URL: <https://www.okta.com/blog/2020/04/how-covid-19-is-changing-the-way-we-work-zoom-boom-mfa-is-the-way/> (visited on 05/18/2020).
- [8] *The Latest Zoom Security Vulnerabilities: What You Need to Know*. URL: <https://blog.rapid7.com/2020/04/02/dispelling-zoom-bugbears-what-you-need-to-know-about-the-latest-zoom-vulnerabilities/> (visited on 05/11/2020).

- [9] *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic — FBI*. URL: <https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic> (visited on 05/11/2020).
- [10] *Who has banned Zoom? Google, NASA, and more - TechRepublic*. URL: <https://www.techrepublic.com/article/who-has-banned-zoom-google-nasa-and-more/> (visited on 05/13/2020).
- [11] Deloitte. *COVID-19 executive cyber briefing: 6 April 2020 | Deloitte Global*. URL: <https://www2.deloitte.com/global/en/pages/risk/articles/covid-19/global-cyber-covid-19-weekly-executive-cyber-briefing.html> (visited on 04/09/2020).
- [12] Margarita Mayo et al. “Leader beliefs and CSR for employees: the case of telework provision”. In: *Leadership and Organization Development Journal* 37.5 (July 2016), pp. 609–634. ISSN: 01437739. DOI: 10.1108/LODJ-09-2014-0177.
- [13] Angel Belzunegui-Eraso and Amaya Erro-Garcés. “Teleworking in the Context of the Covid-19 Crisis”. In: *Sustainability* 12.9 (May 2020), p. 3662. ISSN: 20711050. DOI: 10.3390/su12093662. URL: <https://www.mdpi.com/2071-1050/12/9/3662>.
- [14] European Union commission. *User guide to the SME Definition*. 2003. ISBN: 9789279453229. DOI: 10.2873/782201.
- [15] *BYOD: Security and privacy considerations*. 2012. DOI: 10.1109/MITP.2012.93.
- [16] Jack M. Nilles. “Telecommunications and Organizational Decentralization”. In: *IEEE Transactions on Communications* 23.10 (1975), pp. 1142–1147. ISSN: 00906778. DOI: 10.1109/TCOM.1975.1092687.
- [17] Susan L Handy and Patricia L Mokhtarian. “Planning for Telecommuting - Measurement and Policy Issues”. In: *Journal of the American Planning Association* 61.1 (1995), pp. 99–111. ISSN: 1939-0130. DOI: 10.1080/01944369508975623. URL: <https://www.tandfonline.com/action/journalInformation?journalCode=rjpa20>.
- [18] David Lamond. *Defining Telework: What is it Exactly?* URL: [https://www.academia.edu/20588605/Defining\\_Telework\\_What\\_is\\_it\\_Exactly](https://www.academia.edu/20588605/Defining_Telework_What_is_it_Exactly).
- [19] David Lamond. *Defining Telework: What is it Exactly?* URL: [https://www.academia.edu/20588605/Defining\\_Telework\\_What\\_is\\_it\\_Exactly](https://www.academia.edu/20588605/Defining_Telework_What_is_it_Exactly).



- [20] “Telework: A New Way of Working and Living”. In: *International Labour Review* ().
- [21] Margrethe H. Olson. “Remote office work: Changing work patterns in space and time”. In: *Communications of the ACM* 26.3 (1983), pp. 182–187. ISSN: 15577317. DOI: 10.1145/358061.358068.
- [22] Bongsik Shin, Olivia R. Liu Sheng, and Kunihiro Higa. “Telework: Existing research and future directions”. In: *Journal of Organizational Computing and Electronic Commerce* 10.2 (2000), pp. 85–101. ISSN: 10919392. DOI: 10.1207/S15327744JOCE1002\_2.
- [23] Yehuda Baruch and Nigel Nicholson. “Home, Sweet Work: Requirements for Effective Home Working”. In: *Journal of General Management* 23.2 (Dec. 1997), pp. 15–30. ISSN: 0306-3070. DOI: 10.1177/030630709702300202.
- [24] Diane E. Bailey and Nancy B. Kurland. *A review of telework research: Findings, new directions, and lessons for the study of modern work*. June 2002. DOI: 10.1002/job.144.
- [25] Gigi G Kelly et al. “The Telecommuting Life: Managing Issues of Work, Home and Technology”. In: ().
- [26] Tabrez Ahmad. “Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity”. In: *SSRN Electronic Journal* (Apr. 2020). DOI: 10.2139/ssrn.3568830.
- [27] INTERPOL. “CYBERCRIME : COVID-19 IMPACT”. In: 8 (2020).
- [28] Prem Mahadevan. “Threats during the COVID-19 pandemic”. In: (Apr. 2020).
- [29] Checkpoint. *Threat actors join in the race towards a coronavirus vaccine - Check Point Software*. URL: <https://blog.checkpoint.com/2020/08/11/threat-actors-join-in-the-race-towards-a-coronavirus-vaccine/> (visited on 08/28/2020).
- [30] Interpol. “Global Landscape on Covid-19 Cyberthreat”. In: (Apr. 2020).
- [31] Navid Ali Khan and Noor Zaman. “Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic”. In: (May 2020). DOI: 10.36227/techrxiv.12278792.
- [32] *First ransomware-related death reported in Germany | 2020-09-21 | Security Magazine*. URL: <https://www.securitymagazine.com/articles/93409-first-ransomware-related-death-reported-in-germany> (visited on 09/25/2020).
- [33] *ISO - ISO/IEC 27001 — Information security management*. URL: <https://www.iso.org/isoiec-27001-information-security.html#ISMS> (visited on 08/27/2020).

- [34] *Teleworking – Information security through ISO 27001 safeguards*. URL: <https://advisera.com/27001academy/blog/2017/03/22/how-to-apply-information-security-controls-in-teleworking-according-to-iso-27001/> (visited on 07/28/2020).
- [35] *ISO - ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls*. URL: <https://www.iso.org/standard/54533.html> (visited on 08/29/2020).
- [36] Murugiah Souppaya and Karen Scarfone. “SP 800-46 Rev. 2 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security”. In: *NIST Special Publication 800-46.2* (2016), p. 53. DOI: 10.6028/NIST.SP.800-46r2. URL: <http://dx.doi.org/10.6028/NIST.SP.800-46r2%20https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf>.
- [37] Murugiah Souppaya and Karen Scarfone. “NIST Special Publication 800-114 Revision 1 User’s Guide to Telework and Bring Your Own Device (BYOD) Security”. In: *NIST Special Publication* (2016). DOI: 10.6028/NIST.SP.800-114r1. URL: <http://dx.doi.org/10.6028/NIST.SP.800-114r1>.
- [38] *ENISA*. URL: <https://www.enisa.europa.eu/> (visited on 09/26/2020).
- [39] *Top ten cyber hygiene tips for SMEs during covid-19 pandemic — ENISA*. URL: <https://www.enisa.europa.eu/news/enisa-news/top-ten-cyber-hygiene-tips-for-smes-during-covid-19-pandemic> (visited on 08/17/2020).
- [40] *Top Tips for Cybersecurity when Working Remotely — ENISA*. URL: <https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely> (visited on 07/30/2020).
- [41] *Tips for cybersecurity when working from home — ENISA*. URL: <https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home> (visited on 07/28/2020).
- [42] *Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards*. URL: <https://www.pcisecuritystandards.org/> (visited on 11/19/2020).
- [43] *How the PCI DSS Can Help Remote Workers*. URL: <https://blog.pcisecuritystandards.org/how-the-pci-dss-can-help-remote-workers> (visited on 11/19/2020).
- [44] *Protecting Payments While Working Remotely*. URL: <https://blog.pcisecuritystandards.org/protecting-payments-while-working-remotely> (visited on 11/19/2020).

- [45] CIS. *Center for Internet Security*. URL: <https://www.cisecurity.org/> (visited on 11/05/2020).
- [46] CIS. *Telework and Small Office Network Security Guide*. URL: <https://www.cisecurity.org/white-papers/cis-controls-telework-and-small-office-network-security-guide/> (visited on 11/10/2020).
- [47] CIS. *CIS Controls SME Companion Guide*. URL: <https://www.cisecurity.org/white-papers/cis-controls-sme-guide/> (visited on 11/10/2020).
- [48] Toshihiro Okubo. “Research on Telework and the Actual Conditions of Workers”. In: *Covid Economics* (2020), pp. 1–5.
- [49] Stijn Baert et al. “The COVID-19 Crisis and Telework : A Research Survey on Experiences , Expectations and Hopes”. In: *IZA Discussion Paper* 13229 (2020), pp. 1–37. URL: <http://hdl.handle.net/10419/216771>.
- [50] William Riggs. “Telework and Sustainable Travel During the COVID-19 Era”. In: *SSRN Electronic Journal* 19 (2020), pp. 1–58. ISSN: 1556-5068. DOI: 10.2139/ssrn.3638885.
- [51] Alice Sturgeon. “Telework: threats, risks and solutions”. In: *Information Management Computer Security* 4.2 (May 1996), pp. 27–38. ISSN: 09685227. DOI: 10.1108/09685229610121017.
- [52] Huiyi Yang et al. “Security Risks in Teleworking : A Review and Analysis”. In: (2012), pp. 1–15.
- [53] Takashi Hatashima and Yasuhisa Sakamoto. “Study on Effect of Company Rules and Regulations in Telework Involving Personal Devices”. In: (2017). DOI: 10.1587/transinf.2016OFL0001.
- [54] F. Clear. “SMEs, electronically-mediated working and data security cause for concern”. In: *International Journal of Business Science and Applied Management* 2.2 (2007), pp. 1–20. ISSN: 1753-0296.
- [55] J.W. Creswell and J.D. Creswell. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications, 2017. ISBN: 9781506386713. URL: <https://books.google.ee/books?id=KGNADwAAQBAJ>.
- [56] Sheskin, David J. *Handbook of Parametric and Nonparametric Statistical Procedures, Fifth Edition*. 2020. ISBN: 9781000083279.
- [57] Google. *Google Forms: Free Online Surveys for Personal Use*. URL: <https://www.google.com/forms/about/> (visited on 10/30/2020).
- [58] Faye Hussain Alqahtani. “Developing an Information Security Policy: A Case Study Approach”. In: *Procedia Computer Science*. Vol. 124. Elsevier B.V., Jan. 2017, pp. 691–697. DOI: 10.1016/j.procs.2017.12.206.

- [59] In: *International Journal of Control and Automation* 13.4 (2020), pp. 1088–1099. ISSN: 2005-4297. URL: <https://www.researchgate.net/publication/342378341>.
- [60] *Gophish - Open Source Phishing Framework*. URL: <https://getgophish.com/> (visited on 12/09/2020).
- [61] *WifiPhisher - The Rogue Access Point Framework*. URL: <https://wifiphisher.org/> (visited on 12/09/2020).
- [62] *SPSS Statistics - Overview | IBM*. URL: <https://www.ibm.com/products/spss-statistics> (visited on 12/11/2020).
- [63] “A typology of employees’ information security behaviour”. In: Institute of Electrical and Electronics Engineers Inc., Sept. 2016. ISBN: 9781467398794.
- [64] Fanny Lalonde Lévesque, Jose M M Fernandez, and Dennis Batchelder. “Age and gender as independent risk factors for malware victimisation”. In: BCS Learning Development, July 2017. DOI: 10.14236/ewic/hci2017.48. URL: <http://dx.doi.org/10.14236/ewic/HCI2017.48>[www.appesteem.com](http://www.appesteem.com).
- [65] Steve Sheng et al. *Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions*. 2010. ISBN: 9781605589299. URL: <http://www.brubandwithamnesty.org/bandwidth/agree.htm>.

# Appendices

## Appendix 1 - Interview Questionnaire

Dear Participant,

I would like to invite you to participate in this research project which is part of my master's dissertation research. Please take the time to read the following information carefully. The purpose of the study is to analyze the posture of information security while teleworking during the COVID-19 crisis. Note: Teleworking in this survey refers to regular home-based work(work from home) carried out during the COVID-19. The survey will take you approximately 10-15 minutes to complete. It is targeted to professionals who are responsible for information security in an organization. Participation is completely voluntary. You should only take part if you want to and choosing not to take part will not disadvantage you in any way. Your answers will be treated confidentially and the information you provide will not allow you to be identified in any research outputs/publications. Please note that information such as email, the company name is collected is for the sole purpose of data classification and will not be used elsewhere. The results of the study will be summarised as part of my master's dissertation. Thank you for taking the time to read this information. The research paper about this study will be found in <https://digikogu.taltech.ee/> once the study is completed. If you have any questions or require more information about this study, please contact me via email at [kayada@ttu.ee](mailto:kayada@ttu.ee).

Kapil Yadav

MSc - Cyber Security

Tallinn University of Technology

Estonia

- Company name
- Size of your organization (micro/small/medium)

**General information**

- How would you define the percentage of people working remotely from home before the outbreak of coronavirus?
- How would you define the percentage of teleworkers during the COVID-19 situation in your organization?
- Which of the following IT security frameworks does your organization adhere/refer? (ISO 27001,NIST,COBIT,etc)
- Does your organization have a policy for telework?
- How did your organization handle the telework practice during the COVID-19 situation?

### **Protection against major threats**

- Did you change the access of internal resources during the COVID-19 crisis to be available for users remotely while working from home? If yes, how do you secure the internal resources of a company from external access?
- How do you ensure security over external/unsecured networks used by telework users?
- Do you have controls to ensure the physical security of client telework devices? What are these controls?
- How do you secure the internal networks of the company from infected or compromised devices?

### **Remote access methods**

- What all remote access methods are enabled for users to access the internal resources of your company?
- How do you secure the information being accessed using remote access methods mentioned in the previous question?
- Did security arrangements for remote access methods change during the COVID-19 situation? If yes, please describe.
- Did you face any challenges to maintain security on remote servers or remote access solutions during the COVID-19 situation? If yes, what were these challenges, and how did you overcome them?

### **Telework client device security**

- What practices are used to ensure the security of telework PCs?
- What practices are used to ensure the security of telework Mobile Devices?
- What controls are used to protect the data on telework client devices?

- Did you face any challenges to maintain security on Telework Client Devices during the COVID-19 situation? If yes, what were these challenges, and how did you overcome them?

### **User control and guidelines**

- Did your organization release special guidelines or awareness programs for users teleworking during COVID-19?
- What aspects were communicated to the users as part of the user training/guidelines while teleworking during COVID-19?
- Do you have security monitoring for information accessed remotely by the users? Please describe it.

### **Suggestions and Feedback**

- Did you face any other challenges to maintain the information security of your organization during the COVID-19? if yes, please describe them and how did you deal with them?
- Feel free to leave any other additional comments or suggestions here.

## Appendix 2 - Survey Questionnaire

Dear Participant,

I want to invite you to participate in this research project, which is part of my master's dissertation research. Please take the time to read the following information carefully. The study aims to analyze the posture of information security while teleworking during the COVID-19 crisis. The survey will take you approximately 5-10 minutes to complete. Your responses will nevertheless be treated confidentially, and the information you provide will not allow you to be identified in any research outputs/publications. The results of the study will be summarised as part of my master's dissertation. Thank you for taking the time to read this information. The research paper about this study will be found in <https://digikogu.taltech.ee/> once the study is completed. If you have any questions or require more information about this study, please contact me via email at [kayada@ttu.ee](mailto:kayada@ttu.ee).

Kapil Yadav

MSc - Cyber Security

Tallinn University of Technology

Estonia



## Definitions

TELEWORK/TELEWORKING in this survey refers to regular home-based work(work from home) carried out during the COVID-19.



TELEWORK DEVICE in this survey refers to a company-issued device used to work remotely such as a laptop or a phone.



## General Information

- Age Group
- Gender
- How would you define the frequency of working remotely before the outbreak of coronavirus?
- How would you define the frequency of telework during the COVID-19 crisis?

### **Securing information on telework devices**

- Does your company allow corporate computers for personal use during COVID-19?
- Do you use the corporate computer for personal use?
- Does your company allow corporate computers to be used by family and kids during COVID-19?
- How often do other people (family and kids) access or use your corporate laptop?
- Do you use removable media such as pen drives and external hard drives to store data?
- Is the information stored on the telework device backed up by you/your company?

### **Securing networks and communication**

- Did your organization issue guidelines regarding the use of the internet, network, and access points?
- What measures or controls are you using to secure the communication through a mobile device?
- Is there multi-factor authentication for access to the network, application, and web services while working from home?
- Which of the following security is applicable to your internet connection or WiFi?

### **Ongoing reminders and guidelines about phishing scams**

- Did your organization issue an awareness campaign or guidelines to avoid phishing scams during COVID-19?
- Which of the following defines the term "phishing"?

## How to identify phishing or scam email?

The email looks like it's from a company you may know and trust.



The email/message is not addressed to you directly by name. For eg: The email has a generic greeting, "Hi Dear."



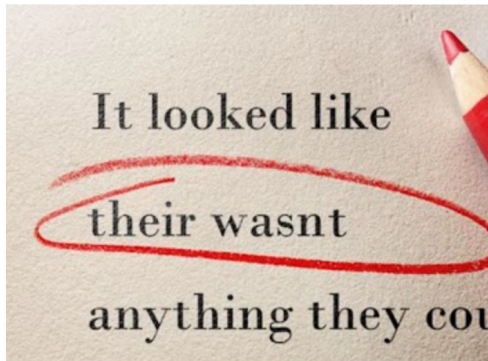
The email invites you to click on a link or download an attachment.



The email asks you for your personal or payment details.



The email/message contains grammatical mistakes.



Based on the information provided in the last page, please identify if the following images are phishing attempt or real.

## IMAGE 1

Re:SAFTY CORONA VIRUS AWARENESS WHO



World Health Organization



Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Safety measures

Symptoms common symptoms include fever, cough, shortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong  
Specialist wuhan-virus-advisory

## IMAGE 2

From Paypal

Subject **Your account access has been limited**


14/11/19, 5:51 am

**PayPal**


Hello Dear Customer,  
recently we have limited your account access due suspected and illegal uses.  
Please Check your account as soon as you can by Clicking the button below

Check it now

### IMAGE 3


SAMPLE 1
Receipt

APPLE ID		BILLED TO Apple Store	TOTAL <b>\$49.95</b>
DATE Oct 11, 2017			
ORDER ID <a href="#">MXJOHL83J1</a>	DOCUMENT NO. 126176719694		


iCloud	TYPE	PURCHASED FROM	PRICE
 <b>iCloud: 10 TB Storage Plan</b> Monthly   Oct 11, 2017	iCloud Storage		<b>\$49.95</b>
Subtotal			<b>\$49.95</b>
Tax			<b>\$0.00</b>
<b>TOTAL</b>			<b>\$49.95</b>

If you have any questions about your bill, [visit iTunes Support](#). This email confirms payment for the iCloud storage plan listed above. You will be billed each plan period until you cancel by [downgrading](#) to the free storage plan from your iOS device, Mac or PC.


You may contact Apple for a full refund within 15 days of a monthly subscription upgrade or within 45 days after a yearly payment. Partial refunds are available where required by law.

If you did not authorize this purchase, please visit the [Apple Store Cancellation Form](#)

Learn how to [manage your password preferences](#) for iTunes, iBooks, and App Store purchases.


SAMPLE 2
Receipt

APPLE ID <a href="#">ace@tidbits.com</a>		BILLED TO MasterCard Adam Engst <a href="#">50 Hickory Rd</a> <a href="#">Ithaca, NY 14850-9606</a> USA	TOTAL <b>\$7.87</b>
DATE Jan 25, 2018			
ORDER ID	DOCUMENT NO.		

iCloud	TYPE	PURCHASED FROM	PRICE
 <b>iCloud: 2 TB Storage Plan</b> Monthly   Feb. 25, 2018	iCloud Storage		<b>\$7.87</b>
Subtotal			<b>\$7.87</b>
Tax			<b>\$0.00</b>
<b>TOTAL</b>			<b>\$7.87</b>

If you have any questions about your bill, [visit iTunes Support](#). This email confirms payment for the iCloud storage plan listed above. You will be billed each plan period until you cancel by [downgrading](#) to the free storage plan from your iOS device, Mac or PC.

You may contact Apple for a full refund within 15 days of a monthly subscription upgrade or within 45 days after a yearly payment. Partial refunds are available where required by law.

### Feedback and Suggestions

- Did you face any challenges to maintain the information security of your organization during the COVID-19? if yes, please describe them and how did you deal with them?
- Feel free to leave any other additional comments or suggestions here.