İşletme Bilimi Dergisi
Journal of Business Science

E-ISSN : 2148-0737
Publisher : Sakarya University

Vol. 13, No. 1, 138-157, 2025
DOI: https://doi.org/10.22139/jobs.1623655

Research Article

Digital Age Workplace Security: Cyber Hygiene Approach in Remote Work

Faruk Dursun

Sakarya University, Business School, Management Information Systems, Sakarya, Türkiye,
farukdursun@sakarya.edu.tr,
ror.org/04ttnw109

Received: 20.01.2025
Accepted: 13.03.2025
Available Online: 24.03.2025

Abstract: In this study, the importance and effectiveness of cyber hygiene in remote working environments during the digital age were examined. The results revealed that many employees lack sufficient knowledge about cybersecurity, and companies face difficulties in implementing cyber hygiene policies. With the increase in remote working, the necessity of taking stronger measures against cyber threats has been emphasized. Cyber Hygiene Training: Regular cybersecurity training should be provided for employees. Security Policies: Special cybersecurity policies for remote work should be developed and implemented. Security Software: Antivirus and other security software should be used and kept up to date. Two-Factor Authentication (2FA): 2FA should be made mandatory to enhance account security. Data Encryption: End-to-end encryption methods should be applied for sensitive data. Data Backup: Regular data backup policies should be followed. Audits: Regular cybersecurity audits should be conducted, and vulnerabilities should be addressed. Awareness Campaigns: Campaigns should be organized to raise employees' awareness of cyber threats. These recommendations provide strategic steps to enhance cybersecurity in remote working environments and minimize cyber threats.

Keywords: Cyber Hygiene, Remote Work, Cybersecurity, Cyber Attacks

1. Introduction

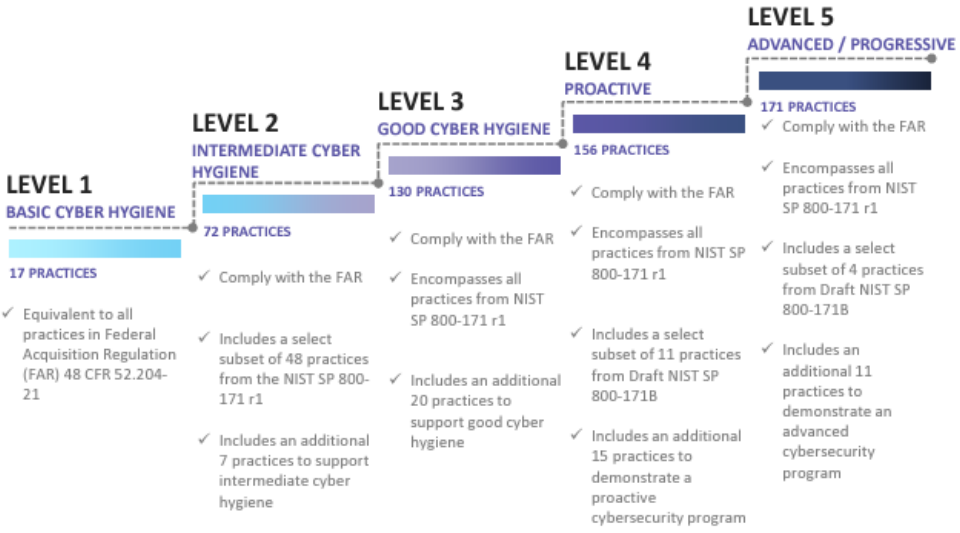
The frequency and complexity of cyber-attacks and crimes are increasing. Such attacks can have personal effects as well as threatening the private and public sectors (Shah & Agarwal, 2023). Cyber-physical attacks like Stuxnet, Triton, etc., have created concerning awareness about the vulnerability of critical infrastructure, including water, electricity, and gas distribution systems (Khan & Madnick, 2022). Therefore, cyber security, in other words data security, brings cyber hygiene understanding to the forefront (Karanfiloğlu, 2022). According to Stifel and colleagues (2022), examining high-profile cybersecurity cases over the last decade shows that basic cyber hygiene is an accessible and practical approach to mitigating such cases, increasing confidence in the use of information and communication technologies, and ultimately advancing cyber peace. One of the key factors affecting how quickly a vulnerability is exploited is the node's overall cyber hygiene. Exploiting a known vulnerability on a host with good cyber hygiene will take longer compared to a host with normal cyber hygiene. Conversely, less time will be required to exploit a host with poor cyber hygiene (Meshkat & Miller, 2022). Cyber hygiene is inspired by the concept of personal hygiene in public health literature (Vishwanath et al., 2020). The report published by the European Union Agency for Network and Information Security (ENISA) contains the observation and recommendation that "cyber hygiene should be treated the same way as personal hygiene, and when properly integrated into an organization, it will become simple daily routines, good behaviors, and occasional checks to ensure the organization's online health is at its best." Cyber hygiene, which is included in cybersecurity measures developed to protect information technology systems and devices, involves adopting and maintaining healthy digital behaviors. In this context, users occasionally exhibit good and bad cyber hygiene behaviors (Aslan et al., 2020). Cybercriminals traditionally exploit corporate IT infrastructures for different reasons such as i) entertainment and challenge; ii) money; iii) stealing intellectual property rights; iv) hacktivism; v) misusing a computer system; and vi) causing disruption and chaos (Awan & Dahabiyeh, 2018). Therefore, public authority sets standards for strong cyber hygiene behavior (Petrykina et al., 2021). CMMC (Cybersecurity Maturity Model Certification) is a unified cybersecurity standard for future DoD

Cite as(APA 7): Dursun, F. (2025). Digital age workplace security: Cyber hygiene approach in remote work, *İşletme Bilimi Dergisi*, 13(1), 138-157. https://doi.org/10.22139/jobs.1623655

acquisitions. This procedure indicates the level of adoption of standards and specifies the set of requirements an organization meets at all levels from Level 1 to Level 5. The CMMC framework lists the most common practices and processes mapped through 17 maturity capability domains (Skarga-Bandurova et al., 2021).

Figure 1

Cyber Hygiene Levels



According to Yilmaz (2023), cyber hygiene is part of cybersecurity action with its human dimension. Although cybersecurity and cyber hygiene are two concepts that evoke each other, and although both are practices that need to be done to prevent cyber threats, cyber hygiene is characterized as a personal factor while cybersecurity policies are an institutional approach (Fenech et al., 2024). Olivares-Rojas and colleagues (2023) argue that the traditional approach to addressing cybersecurity issues often doesn't see the human factor as the main component, therefore, having better personal cybersecurity practices based on the social and human aspect of the cyber hygiene concept will ensure systems have better cybersecurity performance. Karayel and colleagues (2024) draw attention to cultural differences among the factors affecting the degree of cyber hygiene and point out that cross-cultural differences need to be considered to understand the social and subjective norms that affect these behaviors. While the results of a study conducted in Saudi Arabia reveal that 50% of participants lack knowledge about password security and types of cyber attacks, a study conducted in the USA shows that the vast majority of participants have knowledge about these two concepts. In his study on librarians in three Baltic countries - Estonia, Latvia, and Lithuania - Kont (2023) found that Estonian librarians have a higher cyber awareness compared to their Latvian and Lithuanian colleagues, while detecting that cyber hygiene behaviors among this population begin to decrease from the age of 45. Fikry and colleagues (2023) add cyber hygiene knowledge and demographic factors to the factors affecting cyber hygiene practices. Users should ideally maintain good cyber hygiene by developing regular software updates and unique passwords as an effective way to be resilient against cyber attacks. However, it is clearly evident from high-volume attacks that many users keep cyber hygiene weak due to sharing personal information through social networks and freely sharing their passwords. Hackers prefer finding a technical vulnerability or stealing someone's information as the easiest way to access a system (Kioskli et al., 2023). Cyber hygiene includes common cybersecurity practices such as defense in depth, strong password requirements, and network isolation (Sweeney & Tran, 2022). Cain and colleagues (2018) list effective cyber hygiene practices in the table below:

Table 1

Cyber Hygiene Practices

Update your apps, software, and operating systems
Secure your browser and extensions
Backup your data and files
Secure your wireless network
Use firewalls
Use antivirus and separate antispyware software
Do not open emails or attachments from unknown sources
Use hard-to-guess passwords and keep them secret
Protect your Wi-Fi with a password
If in doubt, do not visit the website
Turn off the router when not in use
Encrypt sensitive files on the computer
Perform weekly antivirus scans

According to Sweeney and Tran (2022), the categories of cyber hygiene are listed in the table below:

Table 2

Cyber Hygiene Categories

Full segregation of the network infrastructure at all levels.
Additional network monitoring outside the firewall.
Properly configured firewalls.
Limited internet access.
Multiple Internet Service Providers to increase bandwidth.
No external devices used within workspaces.
Upgraded and enhanced equipment.
Improved virus scanning.
System redundancy.
Traffic flow control.
Implementation of a defense-in-depth methodology.
Use of VPNs to secure data.

A report published by Tripware (2018) includes six necessary elements for healthy cyber hygiene.

Control 1: Inventory and control of hardware assets: It advises organizations to maintain an accurate network inventory, providing visibility of devices that could pose security threats or should not be on the network at all.

Control 2: Inventory and control of software assets: This focuses on the software inventory, in line with the hardware inventory. Organizations can control malicious software and software that should not be running on their network by applying this control.

Control 3: Continuous security vulnerability management: A robust vulnerability management program supported by proper tools allows the organization to control its own security and manage risks from both internal and external threats.

Control 4: Controlled use of administrator privileges: This investigates how well administrator privileges are managed and protected by organizations.

Control 5: Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers: Configuration management becomes increasingly challenging in complex technology environments consisting of multiple systems, asset owners, and applications with different configuration states and business requirements. Businesses should leverage technologies that automate the evaluation, monitoring, and management of configurations across all systems to ensure continuous security and compliance.

CIS Control 6: Maintenance, monitoring, and analysis of audit logs: Security logs and analysis help IT teams locate attackers, detect malware, and monitor activities on victim machines.

Cyber hygiene involves adopting and maintaining fundamental cybersecurity behaviors. Regularly checking technological devices for threats and hacking attempts, renewing passwords and avoiding reuse, keeping antivirus software updated, securely storing online data, and conducting necessary security scans are examples of these healthy and adaptive behaviors (Neigel et al., 2020). Indeed, based on the critical role of nurses in patient information security, Kamerer and McDermott (2023) suggest that adding cyber hygiene to the nursing curriculum will be effective in protecting patients, organizations, and staff from the impacts of a cyber attack. Supporting this study, Webb and Dayal (2017) highlight that end users and physicians must exhibit effective cyber hygiene behavior to reduce cybersecurity risks and that cooperation among all stakeholders must be increased. They also emphasize that cyber hygiene spans a broad range, from controlling cybersecurity standards for medical devices to installing the latest updates and patches released by manufacturers. Similarly, Argyridou and colleagues (2023) found that their proposed cyber hygiene methodology improved the perceptions and behaviors of healthcare sector personnel regarding cyber hygiene. Çelik and Çeliktaş (2018) note that to protect individuals, institutions, and organizations from ransomware threats, it is necessary to ensure that logical cyber hygiene programs, such as vulnerability and patch management, security awareness training, strict email screening measures, and a comprehensive off-site backup plan, are in place. Wong and colleagues (2022) suggest that the risks and losses caused by a cyber attack in SMEs, which play a critical role in supply chain processes, can be mitigated by giving priority to preventive measures and cyber hygiene practices that align with those measures. Ncubukezi and colleagues (2020) show that cyber hygiene varies between industries in SMEs. The lack of detailed rules, standards, procedures, and guidelines to promote good cybersecurity hygiene results in weak cyber hygiene in SMEs. The findings also demonstrate the limitations of using and implementing existing security measures. Additionally, the insufficient knowledge of SME employees in handling cyber attacks causes significant gaps. Kalhoro and colleagues (2021) indicate that software development organizations are vulnerable to cyber attacks due to a lack of a proper cybersecurity culture and emphasize that the danger will persist unless these organizations have effective cyber hygiene behaviors. Szczepaniuk and Szczepaniuk (2022) argue that adherence to cyber hygiene principles reduces security vulnerabilities caused by human weaknesses, which can be achieved by keeping the user training level up to date and improving it. Mohammadi and colleagues (2019) suggest that, beyond technical measures, cyber hygiene behaviors can be improved through staff training and awareness activities. Stifel and colleagues (2022) similarly stress the importance of investing in human resources, as technological resources alone are insufficient. In a study conducted by Oravec (2017) to ensure IoT device cyber hygiene, he highlights the importance of creating educational materials to empower households in building cyber hygiene routines and addressing concerns related to IoT. Zhang and Malacaria (2023) emphasize that good training and awareness programs in IoT device usage encourage users to maintain good cyber hygiene habits and stay aware of ongoing cyber attacks. Changing the default password of the home router and being aware of local network anomalies are important examples of cyber hygiene behavior. In a study on mobile health systems, Pool and colleagues (2020) relate data protection successes and failures to contextual factors such as systems, users, tasks, services, geographical factors, and causal mechanisms like unauthorized access, device theft, loss and sharing, and lack of cyber hygiene. Olivares-Rojas and

colleagues (2021) demonstrate that cyber hygiene practices can improve smart meter cybersecurity and could be suitable for other sensitive smart grid components. Ngo and colleagues (2024) found that among individuals with limited English proficiency, demographic factors such as age, gender, marital status, education level, and employment status were significantly related to seven cyber hygiene practices (having antivirus software, using strong passwords, not sharing passwords, not using public Wi-Fi, not accepting strangers' requests, checking email sources, and not downloading unverified files) and that cyber hygiene measures predict eight types of cyber victimization (phishing, computer virus infections, online harassment and fraud, and hacking of email, social media, shopping, and other accounts). Additionally, focus group results showed that participants were motivated to adopt these practices despite having insufficient knowledge. Baraković and Husić (2023a) conducted a study on university students and found that while students had acceptable cyber hygiene behavior, their awareness was unsatisfactory, and their knowledge was quite low. They also identified relationships between cyber hygiene knowledge, awareness, and behavior, as well as the interaction and relationships between these outcomes, based on work, gender, and current education level. Salem and Sobaih (2023) developed a four-step "E" approach (Educate, Explore, Apply, Evaluate) and found that after adopting QEA, students in Saudi Arabia exhibited more positive cyber hygiene behaviors and attitudes toward online learning compared to before the adoption. Furthermore, female students showed more positive behaviors and attitudes after adopting QEA than male students. Kilhoffer and colleagues (2023) conducted a study with 16 U.S. high school teachers and 11 students and found that cyber hygiene training was ineffective in teaching young people and promoting safer online behavior. Generational differences made it difficult for teachers to connect with students. Mwangala and colleagues (2023) found weak cyber hygiene in Namibian Public Service institutions, including government departments, ministries, and agencies, due to the lack of password management, patch management, ineffective cyber user awareness training, the absence of third-party security assessment mechanisms, and generally weak cyber hygiene. Karimnia and colleagues (2022) found that among 616 high school students in Hormozgan, Iran, students had low hygiene knowledge levels and engaged in excessive VPN use. Baraković and Husić (2023b) showed that the COVID-19 pandemic altered the level of awareness, behavior, and knowledge of cyber hygiene among 746 university students at the University of Sarajevo, improving these aspects during the pandemic. However, after the easing of protective measures and decreased use of digital services post-pandemic, there was a trend of reduced cyber hygiene knowledge. Whitty and colleagues (2024) highlighted that employees' cyber hygiene practices before the COVID-19 pandemic were far from ideal. In a study at the University of Nigeria, Nsukka, Ugwu and colleagues (2022) found that 50.32% of the 316 participants had a low cyber hygiene culture. Blythe and colleagues (2019) found that the usage manuals of 270 IoT devices from 220 different manufacturers did not provide consumers with adequate information on cyber hygiene.

2. Method

The aim of this article is to emphasize the importance of cybersecurity measures in remote work environments in the digital age and to explore the concept of "cyber hygiene" in this context. With the digital transformation and the increasing prevalence of remote work practices, there is a greater need for sensitivity to cybersecurity threats. This article aims to raise awareness among remote workers and businesses about cyber hygiene practices and to develop actionable strategies in this regard. The findings of the study will contribute to the development of applicable security strategies for both employers and employees. Employers can use these strategies to create more resilient policies against cyber threats, while employees can act more consciously at the individual level. Moreover, this study will fill a gap in the academic literature concerning the relationship between remote work and cybersecurity, guiding future research. As a result, this research will serve as an important guide for creating a secure and sustainable work culture suitable for the working models of the digital age.

Maintaining business continuity, preventing data breaches, and raising digital security awareness will provide a safer and more efficient working environment in the long run.

The data for the study were collected using the Cyber Hygiene Scale adapted into Turkish by Aslan, Aktaş and Akbıyık (2020). The data collection form was distributed online to 400 white-collar employees working remotely. Out of the 400 forms distributed, 385 individuals participated in the study. MacCallum and Widman (1999) state that a sample size 5 to 10 times the number of variables is sufficient. The scale used in the study contains 17 items. All items meet the factor loading requirements. Therefore, no items were removed from the scale. The sample size in our study is 385. Based on this, it can be concluded that the sample size is sufficient. There are no missing data in the dataset. The study utilized a convenience sampling method. According to Golzar and Tajik (2022), in convenience sampling, data are collected from the population in an easy, fast, and economical manner.

2.1. Data collection method

Questionnaire technique was used to collect data in the research. The research data were collected with the decision numbered "08" taken at the meeting of Sakarya University Social and Human Sciences Ethics Committee dated 16.01.2025 and numbered 80.

3. Findings

The data analysis was conducted using the SPSS 23.0 statistical program. In the reliability analysis of the data, the Cronbach's Alpha value was found to be 0.910. According to Taber (2018), this value is considered strong (0.91–0.93). Factor analysis was performed on the data collected using the scale, and the KMO value was found to be 0.814. According to Kaiser (1974), values above 0.90 are considered excellent, values above 0.80 are high, values above 0.70 are medium and fair, values above 0.50 are weak, and values below 0.50 are considered unacceptable. Based on these data, it can be concluded that the obtained KMO value is high.

Table 3

Demographic Findings

	Frequency	**Percent**			**Frequency**	**Percent**
Gender	Male	180	46,8	Banking-Finance	50	13
	Female	205	53,2	Construction	5	1,3
Age	18-24	95	24,6	Healthcare	25	6,5
	25-34	165	42,8	Manufacturing	15	3,9
	35-44	100	25,9	Information Technology	95	24,7
	45-54	25	6,7	Education	35	9,1
Graduation	High School	45	100	Services	65	16,9
	Associate's Degree / Bachelor's Degree	270	11,6	Advertising	5	1,3
	Graduate	70	70,1	Automotive	25	6,5
Sector	Private	315	18,3	Tourism	20	5,2
	Public	70	81,8	Retail	15	3,9
				Security	5	1,3
				Food	5	1,3
				Telecommunications	20	5,2

Occupation Field

Of the 385 participants in the study, 205 are female and 180 are male. The study includes participants from the age ranges of 18-24, 25-34, 35-44, and 45-54, with the highest number of participants being

165 from the 25-34 age range and 100 from the 35-44 age range. This participation range is considered significant as it reflects the age spectrum in the workforce. Among the participants, 270 have an associate's degree or bachelor's degree, while 70 have a graduate degree. The fact that most participants are highly educated is noteworthy in the context of educational outcomes. 81.8% of participants work in the private sector. Additionally, the participation from the public sector is significant for comparing the two sectors. There is a wide range of professions from banking and finance to telecommunications. The notable occupational groups are banking and finance (13%), information technology (24.7%), and services (16.9%).

Table 4

Cybersecurity Concept Awareness

		Frequency	Percent			Frequency	Percent
Phishing	I Haven't Heard of It	195	50,6	Trojan	I Haven't Heard of It	165	42,9
	I Have Heard of It, but I Don't Know the Content	90	23,4		I Have Heard of It, but I Don't Know the Content	80	20,8
	I Know the Content	100	26,0		I Know the Content	140	36,4
Whaling	I Haven't Heard of It	235	61,0	Trojan Horse Malware	I Haven't Heard of It	90	23,4
	I Have Heard of It, but I Don't Know the Content	90	23,4		I Have Heard of It, but I Don't Know the Content	70	18,2
	I Know the Content	60	15,6		I Know the Content	225	58,4
Baiting	I Haven't Heard of It	265	68,8	Virus	I Have Heard of It, but I Don't Know the Content	25	6,5
	I Have Heard of It, but I Don't Know the Content	80	20,8		I Know the Content	360	93,5
	I Know the Content	40	10,4	Worms	I Haven't Heard of It	200	51,9
Scareware	I Haven't Heard of It	175	45,5		I Have Heard of It, but I Don't Know the Content	125	32,5
	I Have Heard of It, but I Don't Know the Content	130	33,8		I Know the Content	60	15,6
	I Know the Content	80	20,8	Ransomware	I Haven't Heard of It	255	66,2
Malware	I Haven't Heard of It	215	55,8		I Have Heard of It, but I Don't Know the Content	85	22,1
	I Have Heard of It, but I Don't Know the Content	80	20,8		I Know the Content	45	11,7
	I Know the Content	90	23,4	Spyware	I Haven't Heard of It	220	57,1

Table 4 (Continued)

Adware	I Haven't Heard of It	185	48,1		I Have Heard of It, but I Don't Know the Content	90	23,4
	I Have Heard of It, but I Don't Know the Content	110	28,6		I Know the Content	75	19,5
	I Know the Content	90	23,4				

When examining the participants' awareness levels regarding concepts that pose significant threats to cybersecurity hygiene, it is noticeable that they have either never heard of or have heard of but do not know the content of concepts such as phishing, whaling, baiting, scareware, malware, adware, trojan, worms, ransomware, and spyware. These concepts, which are essential methods for cyber attack actions, reveal a lack of conceptual awareness. Participants indicated that they only knew the content of the terms "trojan" and "virus." A significant portion of female participants stated that they had either never heard of or had heard of but did not know the content of all terms except for trojan and virus. This data is important in revealing the conceptual deficiencies of female participants. Similar findings apply to the age group category as well. Participants of all age ranges do not know the concepts other than trojan and virus, or they have a lack of information regarding their content. These findings are also valid for graduation level, sector, and profession. An interesting and noteworthy observation here is that the concept knowledge levels of IT sector employees show a fluctuating distribution. In other words, contrary to expectations, IT sector employees did not predominantly select "I know the content" in response to this question, which aimed to identify awareness levels using the options "I haven't heard of it," "I've heard of it," "I don't know the content," and "I know the content." Instead, they responded with "I haven't heard of it" and "I've heard of it, but I don't know the content." At this point, it was determined that there were conceptual deficiencies in all demographic characteristics, and the awareness levels were insufficient.

Table 5

Cybersecurity Awareness of Preventive Measures

		Frequency	**Percent**			**Frequency**	**Percent**
Has your company or organization organized any seminars or training related to information security?	Yes	180	46,8	Can you access your work email from your personal computer?	Yes	255	66,2
	No	130	33,8		No	130	33,8
	I don't know	75	19,5				
Has your company or organization provided necessary training regarding the applications you will use during remote work? (For example; VPN usage, remote desktop access, etc.)	Yes	225	58,4	Has a tracking program been installed on your work computer?	Yes	95	24,7
	No	145	37,7		No	195	50,6
	I don't know	15	3,9		I don't know	95	24,7
				Has authorization been defined for accessing company or organizational information?	Yes	240	62,3
Do you work from the computer provided by the company or organization while working from home?	Yes	270	70,1		No	145	37,7
	No	115	29,9				
				Have you signed a contract for information security?	Yes	165	42,9

Table 5 (Continued)

Are you asked by company or organization officials to perform regular virus scans?	Yes	125	32,5		No	220	57,2
	No	235	61,0				
	I don't know	25	6,5	Are periodic and/or random audits conducted within the organization?	Yes	180	46,8
Do you need to use the VPN system provided by the company or organization?	Yes	240	62,3		No	205	53,3
	No	145	37,7				
Do you need to perform two-step authentication (SMS/Email verification) when logging into your work computer?	Yes	220	57,1	Are there any restrictions on internet access on your work computer?	Yes	195	50,6
	No	165	42,9		No	190	49,4
Do you perform your tasks by connecting through Remote Desktop or Virtual Machine?	Yes	160	41,6	Is your ability to send emails from your work email to an external email address restricted or monitored?	Yes	165	42,9
	No	215	55,8		No	220	57,2
	I don't know	10	2,6				
Are application installation requests on your work computer carried out by the IT department upon request?	Yes	200	51,9	Do you need to perform two-step authentication (SMS/Email verification) when logging into company or organization accounts?	Yes	225	58,4
	No	185	48,1		No	160	40,6
Can you access your personal email from your work computer?	Yes	290	75,3				
	No	95	28,7				

When looking at the responses given by participants to the "Remote Working Cyber Security Measures Inventory" questions, it is more appropriate to focus on the "no" and "I don't know" responses rather than the "yes" answers. This is because a "yes" answer indicates that the necessary requirement is being met. Among the responses about whether information security seminars or training are organized by their company or institution, 130 participants answered "no" and 75 answered "I don't know." When combined, this corresponds to 205 people. Considering the total number of participants is 385, this indicates that 53% of the responses are negative. Regarding the question about whether employees received training on applications such as VPN usage and remote desktop access, 145 participants answered "no" and 15 answered "I don't know." Additionally, 115 people reported that they use their own computers for work because their company or institution did not provide them with one. 260 participants expressed a negative opinion about whether company or institution officials require regular virus scans. There are 145 participants who do not use the VPN system provided by the company or institution while working remotely. 165 participants do not use two-step authentication when logging into their work computers. 225 participants responded "no" or "I don't know" to the question about whether they connect to work through remote desktop or a virtual machine. 48.1% of the participants indicated that application installation on work computers is not carried out by the IT department. It was found that 255 participants can access their work emails from their personal computers. 145 participants stated that no authorization has been defined for accessing company or institution data. 220 participants indicated that they have not signed a contract for information security,

which corresponds to 57.2% of the participants. The number of participants who reported that periodic or random internal audits are not conducted is 205. 190 participants reported that there are no restrictions on internet access on their work computers. 220 participants indicated that sending emails from their work email to an external email address is neither restricted nor monitored. 160 participants stated that they do not use two-step authentication when accessing company or institution accounts, and 290 participants indicated that they can access their personal emails from their work computers. The answers provided by 385 participants to the questions in Table 5 highlight the severity of the situation. In light of the relevant table and answers, the fact that information leakage and data security are neglected both in the private sector and public institutions stands out. Issues such as accessing personal email addresses from work computers, lack of authorization for accessing company or institution data, failure to sign contracts for information security, and no request for regular virus scans are some of the factors that create suitable conditions for cyberattacks and violate cybersecurity hygiene policies.

Table 6

Cyber Hygiene Factors

	Storage Space and Device Hygiene	Data Transmission Hygiene	Social Media Hygiene	User Information Hygiene	Email Hygiene	Mean	Std Deviation	Cronbach's Alpha
How often do you update your antivirus software?	0,834							
How often do you back up important files to a cloud-based server? (e.g., Google Drive, Dropbox)	0,801					3,0087	1,04024	,866
How often do you perform a virus scan on a new USB drive or external storage device?	0,756							
How often do you check for the encryption of a website by looking for the padlock icon in your web browser? (Also known as SSL)		0,844						
When performing online financial transactions, how often do you check the quality of the SSL certificate?		0,842				2,5801	1,11337	,843
How often do you check the electronic access of other people who can connect to your computer on public internet networks?		0,743						
How often do you reassess your social media friends/connections?			0,904			2,7208	,91552	,868

Table 6 (Continued)

How often do you check who you are friends with on social media?	0,800					
How often do you check your privacy settings on social media platforms?	0,783					
How often do you evaluate the trustworthiness of social media friends and information requests?	0,727					
How often do you create complex usernames and passwords?		0,892				
How often do you create new/unique usernames and passwords for all online memberships?		0,787				
How often do you enable two-factor or multi-factor authentication for sessions? (SMS or email verification)		0,587		2,9708	,80685	,796
How often do you change default passwords on all devices with internet access?		0,485				
How often do you check the subject of incoming emails?			0,815			
How often do you check for grammar or spelling errors in email requests?			0,731	3,5801	1,04223	,903
How often do you check the email domain of a sender? (The part after the "@" symbol in emails)			0,721			

The expressions used in the data collection form have been grouped under five factors. These factors are, in order: Storage space and device hygiene, data transmission hygiene, social media hygiene, user information hygiene, and email hygiene. Under storage space and device hygiene, there are 3 expressions; under data transmission hygiene, there are 3 expressions; under social media hygiene, there are 4 expressions; under user information hygiene, there are 4 expressions; and under email hygiene, there are 3 expressions. Since the expressions in the scale carry factor loads, no expression has been removed. The factors explain 79% of the total variance. When looking at the reliability analysis of the factors, the values are as follows: storage space and device hygiene 0.866, data transmission hygiene 0.843, social media hygiene 0.868, user information hygiene 0.796, and email hygiene 0.903. Among the factors, the one with the highest level of attention from participants is email hygiene. Users frequently check the subject of incoming emails, often check the grammar and spelling of requests in the email content, and regularly check the part after the "@" symbol in emails. This suggests that users are paying attention to phishing attacks, which are a very old and widespread form of cyber attack, and are being

cautious to avoid potential attacks via email. However, there is not enough statistical data to discuss this as a conceptual awareness. In other words, the data in Table 4 regarding the knowledge level of the concepts shows that the percentage of participants who know the content of the phishing concept is equal to the percentage of those who have never heard of it or have heard of it but do not know its content. Therefore, while it is difficult to say whether this care is based on conceptual awareness or sensory information, it is important to note that participants who possess email hygiene should also be supported by conceptual knowledge. According to Chaudhry et al. (2015), users do not have a magic wand to overcome phishing attacks, but they need good cyber hygiene to make these attacks more difficult. The factor that users showed the least care for is data transmission hygiene. Participants rarely check SSL certificates on the websites they visit, and also rarely check SSL certificates when performing financial transactions online. SSL (Secure Socket Layer), developed by Netscape in 1995, forms the basis of secure internet communication. The HTTP protocol used for data transfer transmits data unencrypted and is not considered reliable. In contrast, the HTTPS protocol, with its "S" (SSL), creates a secure communication channel. Therefore, SSL technology is an indispensable solution for data security (Saleem, 2019). Based on the importance of SSL certificates, it can be observed that this certificate does not receive sufficient recognition among the research participants. The importance of this certificate for online transactions (e.g., finance, e-commerce) or usage should be adequately communicated to users. Especially when connecting to the internet through public networks, the device, regardless of how hygienic it may be, can pose a security risk due to the unsecured shared network. Once connected to a network, it becomes possible to access the data of users on that network, which threatens data security. Social media hygiene is another area where participants are weak. Here, participants rarely check their social media friends and connections. They also rarely check who they are friends with, the privacy settings of their accounts, or the reliability of social media friends and information requests. In addition to the well-known malicious methods such as malware, phishing attacks, denial-of-service attacks, worms, and viruses, methods such as fake profiles, anonymization attacks, cyber harassment, and information manipulation have become widespread due to the rapid development of social media (Teke & Lale, 2021). Therefore, addressing users' low security perception regarding social media hygiene and raising their awareness is crucial for both private and public sectors in terms of information security. In the context of factor evaluation, it is also seen that participants do not have sufficient knowledge of user information hygiene, and their responses to the expressions are "rarely." Users, especially on devices with internet access, change their passwords only occasionally. They also use two-factor authentication only occasionally. When creating online memberships, they also express their reactions with the "rarely" response regarding creating new and unique usernames and passwords. Methods such as brute force, dictionary, and rainbow tables can predict and steal users' passwords. Passwords that are easy to guess, such as those related to important dates like birthdates, or passwords that are not designed with uppercase letters, lowercase letters, numbers, and special characters, are more easily compromised.

Table 7

Demographic Characteristics and Relationships Between Factors

		p			p
Gender	Storage Space and Device Hygiene	,151	Sector	Storage Space and Device Hygiene	,000
	Data Transmission Hygiene	,000		Data Transmission Hygiene	,000
	Social Media Hygiene	,000		Social Media Hygiene	,004
	User Information Hygiene	,000		User Information Hygiene	,000
	Email Hygiene	,000		Email Hygiene	,000
Age	Storage Space and Device Hygiene	,000	Occupation Field	Storage Space and Device Hygiene	,000
	Data Transmission Hygiene	,000		Data Transmission Hygiene	,000
	Social Media Hygiene	,000		Social Media Hygiene	,000
	User Information Hygiene	,000		User Information Hygiene	,000
	Email Hygiene	,000		Email Hygiene	,000
Graduation	Storage Space and Device Hygiene	,000			
	Data Transmission Hygiene	,000			
	Social Media Hygiene	,000			
	User Information Hygiene	,000			
	Email Hygiene	,000			

When examining the relationship between factors and gender, no significant relationship was found regarding storage and device hygiene (p = ,151, p > ,05), while significant relationships were identified between other factors. It appears that male participants are more cautious about data transmission hygiene, user information hygiene, and email hygiene factors. On the other hand, female participants were found to be more sensitive to social media hygiene. This gender-based difference may arise from male participants not using social media as extensively, or it may stem from women paying more attention to social media processes. There is a significant relationship between age range and all factors. Participants in the 25-34 age range pay attention to Storage and Device Hygiene, Data Transmission Hygiene, Social Media Hygiene, User Information Hygiene, and Email Hygiene factors. This level of attention may be explained by their early career stages or the fact that they are progressing toward the maturity stage of their careers, which makes them strive for error-free behavior. It is difficult to assume that participants in other age ranges, such as 18-24, 35-44, and 45-56, exhibit the same level of attention. Factors such as exposure to technology, lack of education, indifference, and resistance may explain the lack of attention in the 45-56 age range. However, the deficiencies observed in the 18-24 age group require further explanation, as the lack of attention due to education is a dangerous outcome.

There is a significant relationship between graduation and the factors. As participants' education levels increase, their attention to the factors also increases. The low level of attention from high school graduates to the factors highlights the need for more detailed and developed technology education at the high school level. When examining the relationship between industries and factors, it has been found that private sector employees pay more attention to these factors. The fact that public sector employees are not as sensitive to these factors as their private sector counterparts serves as a warning for the public sector. Public sector employees are crucial in protecting sensitive information they have access to, so it is essential for them to behave with caution. Therefore, it is important to consider this impact when planning cybersecurity hygiene training programs for public sector employees. Regarding occupation, employees in technology-intensive sectors are more sensitive to cybersecurity hygiene aspects. While this may not be a surprising result, other sectors show noticeable cybersecurity hygiene deficiencies. Regardless of the occupation or sector, the importance of cybersecurity hygiene can be

understood from the sectoral attack chart published by IBM in 2024, which includes data from the last 5 years. According to the chart, while attacks have been increasingly concentrated on the manufacturing sector, other sectors are also targeted. Therefore, in every sector and occupation involving data, it is possible for such attacks to occur, and the misuse of obtained data for personal gain could lead to various damages and victimization.

Table 8

Cyber Attacks by Sector Over the Years

Sector	2023	2022	2021	2020	2019
Manufacturing	25,7	24,8	23,2	17,7	8
Finance and Insurance	18,2	18,9	22,4	23	17
Professional, Scientific, and Technical Services	15,4	14,6	12,7	8,7	10
Energy	11,1	10,7	8,2	11,1	6
Retail and Wholesale	10,7	8,7	7,3	10,2	16
Healthcare	6,3	5,8	5,1	6,6	3
Public Sector	4,3	4,8	2,8	7,9	8
Transportation	4,3	3,9	4	5,1	13
Education	2,8	7,3	2,8	4	8
Media and Telecommunications	1,2	0,5	2,5	5,7	10

In the report published by IBM, looking at the methods used in attacks in 2023, a wide range of attacks were carried out, from ransomware and backdoor remote access to data exfiltration. These attacks were conducted using malicious software and tools. In other words, 43% of the attacks used malware, and 32% used tools. Additionally, 18% of the attacks involved server access, 7% were Business Email Compromise (BEC), and 6% involved Spam campaigns. The diversity of attack methods, the impacts they created, and the differences in the methods used stand out. In this context, it is important to emphasize the significant role that information users play in establishing the concept of cyber hygiene in organizations and companies.

Table 9

Cyber Attack Methods

Action	Percent (%)	Category
Ransomware	20	Malware
Backdoor	6	Malware
Cryptominer	5	Malware
Information Stealer	4	Malware
Downloader	4	Malware
Bot	4	Malware
Other	3	Malware
Downloader	2	Malware
Webshell	2	Malware
Worm	2	Malware
Credential Theft	13	Tool
Data Exfiltration	11	Tool
Remote Access	10	Tool
Reconnaissance and Scanning	6	Tool

4. Conclusion and Recommendations

With the changing work habits in the digital age, remote work has become increasingly widespread, and this has raised cybersecurity risks. In our study, the importance and effectiveness of cybersecurity hygiene practices in remote working environments were evaluated. The findings revealed that many employees do not have sufficient knowledge of cybersecurity, and businesses face challenges in implementing cybersecurity hygiene policies. Specifically, it was found that individuals who are unaware of cyber threats often engage in careless behaviors, leading to security vulnerabilities in remote work environments. Additionally, businesses were found to have shortcomings in keeping their security policies up to date and communicating these policies to their employees.

Recommendations:

Cyber Hygiene Training Programs:

Businesses should organize comprehensive training programs to increase their employees' knowledge of cybersecurity. These training programs should cover basic cyber hygiene practices, such as creating strong passwords, performing regular software updates, and using secure internet connections. Regular repetition of these training sessions will ensure that employees stay up to date on cybersecurity best practices.

Development of Company Internal Policies and Protocols:

Special cybersecurity policies should be developed for remote work conditions. These policies should clearly specify what security measures employees must take while working remotely and how the company will approach security breaches. The policies should be communicated to all employees and their applicability should be continuously monitored.

Use and Updating of Security Software:

Reliable antivirus programs and security software should be installed on all employee devices, and these programs must be kept up to date. Additionally, applying security patches regularly will help protect devices from cyber threats.

Mandatory Two-Factor Authentication (2FA):

Businesses should enforce the use of two-factor authentication mechanisms for accessing their systems. This measure will help protect accounts from unauthorized access by adding an extra layer of security beyond just passwords.

Data Encryption Practices:

End-to-end encryption techniques should be used to protect sensitive data. Encryption methods should be applied in internal and external data exchanges, email communications, and cloud storage services. This will ensure that data remains secure from cyber attacks.

Regular Data Backups:

Regular backup of important data is a critical measure to prevent data loss. Businesses should encourage employees to back up their data and establish a centralized backup system to ensure secure data storage.

Cybersecurity Audits:

Businesses should conduct regular security audits to assess the effectiveness of cybersecurity measures and identify potential vulnerabilities. These audits can be carried out by external experts and allow the company to continuously improve its security protocols.

Awareness Campaigns:

Internal awareness campaigns should be organized to raise employee awareness of cyber threats. Specifically, awareness should be increased about common threats such as phishing attacks, malware, and social engineering.

These recommendations provide comprehensive strategies aimed at improving cybersecurity in remote work environments. By adopting and implementing these recommendations, businesses and individuals can create a more secure and resilient digital workspace. Ultimately, cyber hygiene, if carried out perfectly in an ideal world, could prevent 95% of attacks, but in the real world, it is merely a speed bump for sophisticated attackers with specific targets (Bochman, 2018). According to Güler and Arkın (2019), the goal for cybersecurity hygiene should not be to add it to the corporate culture but to internalize it.

References

Argyridou, E., Nifakos, S., Laoudias, C., Panda, S., Panaousis, E., Chandramouli, K., Navarro-Llobet, D., Mora Zamorano, J., Papachristou, P., & Bonacina, S. (2023). Cyber hygiene methodology for raising cybersecurity and data privacy awareness in health care organizations: Concept study. *Journal of Medical Internet Research, 25*, 1–17. https://doi.org/10.2196/41294

Aslan, T., Aktaş, B., & Akbıyık, A. (2020). Kullanıcıların bilgisayar güvenliği davranışını inceleme: Siber hijyen. *7. Uluslararası Yönetim Bilişim Sistemleri Konferansı "Sağlık Bilişimi ve Analitiği"*, İzmir, Türkiye.

Awan, M. S., & Dahabiyeh, L. (2018). Corporate attractiveness index: A measure for assessing the potential of a cyber attack. *9th International Conference on Information and Communication Systems*, Irbid, Jordan.

Baraković, S., & Husić, K. B. (2023a). Cyber hygiene knowledge, awareness, and behavioral practices of university students. *Information Security Journal: A Global Perspective, 32*(5), 347–370. https://doi.org/10.1080/19393555.2022.2088428

Baraković, S., & Husić, J. B. (2023b). Impact of COVID-19 pandemic circumstances on cyber hygiene of university students. *International Journal of Human–Computer Interaction*, 1–20. https://doi.org/10.1080/10447318.2023.2247577

Blythe, J. M., Sombatruang, N., & Johnson, S. D. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? *Journal of Cybersecurity, 1–10*. https://doi.org/10.1093/cybsec/tyz005

Bochman, A. (2018). The end of cybersecurity. *Harvard Business Review*, 1–27.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications, 42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Çelik, S., & Çeliktaş, B. (2018). Güncel siber güvenlik tehditleri: Fidye yazılımlar. *Cyberpolitik Journal, 3*(5), 105-132.

Chaudhry, J. A., & Rittenhouse, R. G. (2015). Phishing: Classification and countermeasures. *7th International Conference on Multimedia, Computer Graphics and Broadcasting*, Jeju, South Korea.

Fenech, J., Richards, D., & Formosa, P. (2024). Ethical principles shaping values-based cybersecurity decision-making. *Computers & Security, 140*, 1–17. https://doi.org/10.1016/j.cose.2024.103795

Fikry, A., Hamzah, M. I., Hussein, Z., & Saputra, D. H. (2023). Cyber hygiene practices from the lens of professional youth in Malaysia. *11th ASIAN Conference on Environment-Behaviour Studies*, Kuala Terengganu, Malaysia.

Golzar, J., & Tajik, H. (2022). Convenience sampling. *International Journal of Education and Language Studies, 1*(2), 72–77. https://doi.org/10.22034/ijels.2022.162981

Güler, A., & Arkın, A. K. (2019). Siber hijyenin sağlanmasında iç denetimin rolü. *Denetişim, 9*(19), 17–40.

Kaiser, H. F. (1974). An index of factorial simplicity. *Psychometrika, 39*(1), 31-36.

Kalhoro, S., Rehman, M., Ponnusamy, V. A., & Shaikh, F. B. (2021). Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review. *IEEE Access, 9*, 99339–99363.

Kamerer, J. L., & McDermott, D. S. (2023). Cyber hygiene concepts for nursing education. *Nurse Education Today, 130*.

Karanfiloğlu, M. (2022). Digital literacy in increasing data security: An evaluation from the communicator's perspective. In N. Çokluk & N. Kara (Eds.), *Privacy in the digital age: Digital communication and personal data* (pp. 43–60). Literatürk Academia.

Karayel, T., Aktaş, B., & Akbıyık, A. (2024). Human factors in remote work: Examining cyber hygiene practices. *Information & Computer Security, 33*(1), 1–21. https://doi.org/10.1108/ICS-11-2023-0215

Karimnia, R., Maennel, K., & Shahin, M. (2022). Culturally-sensitive cybersecurity awareness program design for Iranian high-school students. *Proceedings of the 8th International Conference on Information Systems Security and Privacy*.

Khan, S., & Madnick, S. (2022). Cybersafety: A system-theoretic approach to identify cyber-vulnerabilities & mitigation requirements in industrial control systems. *IEEE Transactions on Dependable and Secure Computing, 19*(5), 1–17. https://doi.org/10.1109/TDSC.2021.3093214

Kilhoffer, Z., Zhou, Z., Wang, F., Tamton, F., Huang, Y., Kim, P., The, T., & Wang, Y. (2023). "How technical do you get? I'm an English teacher": Teaching and learning cybersecurity and AI ethics in high school. *IEEE Symposium on Security and Privacy*. https://doi.org/10.1109/SP46215.2023.10179333

Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0. *Applied Sciences, 13*. https://doi.org/10.3390/app13063410

Kont, K. R. (2023). Information security awareness of librarians in the Baltic countries: A comparative analysis. *Baltic Journal of Modern Computing, 11*(3), 450–474. https://doi.org/10.22364/bjmc.2023.11.3.07

MacCallum, R. C., & Widaman, K. F. (1999). Sample size in factor analysis. *Psychological Methods, 4*(1), 84–99. https://doi.org/10.1037/1082-989X.4.1.84

Mohammadi, F., Panou, A., Ntantogian, C., Karapistoli, E., Panaousis, E., & Xenakis, C. (2019). CUREX: Secure and private health data exchange. *Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence* (pp. 263–268). https://doi.org/10.1145/3358695.3361753

Mwangala, J., Bhunu Shava, F., & Chitauro, S. (2023). Human intelligence an enabler for cyber resilience: A case for Namibian public institutions. *IST-Africa 2023 Conference*, Tshwane, South Africa.

Ncubukezi, T., Mwansa, L., & Rocaries, F. (2020). A review of the current cyber hygiene in small and medium-sized businesses. *Proceedings of the 15th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, United Kingdom.

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security, 92*.

Ngo, F. T., Agarwal, A., & Holman, K. (2024). Cyber hygiene and cyber victimization among limited English proficiency (LEP) Internet users: A mixed-method study. *Victims & Offenders*, 1–23. https://doi.org/10.1080/15564886.2024.2329765

Olivares-Rojas, J. C., Reyes-Archundia, E., Gutiérrez-Gnecchi, J. A., Molina-Moreno, I., Méndez-Patiño, A., & Cerda-Jacobo, J. (2023). Cyber hygiene in smart metering systems. *Computación y Sistemas, 27*(2), 459-475.

Olivares-Rojas, J. C., Reyes-Archundia, E., Gutiérrez-Gnecchi, J. A., Molina-Moreno, I., Cerda-Jacobo, J., & Méndez-Patiño, A. (2021). A methodology for cyber hygiene in smart grids. *DYNA Ingeniería e Industria, 97*(1), 92-97.

Oravec, J. A. (2017). Emerging "cyber hygiene" practices for the Internet of Things (IoT): Professional issues in consulting clients and educating users on IoT privacy and security. *IEEE International Professional Communication Conference (ProComm)*, Madison, WI, USA.

Petrykina, Y., Schwartz-Chassidim, H., & Toch, E. (2021). Nudging users towards online safety using gamified environments. *Computers & Security, 108*.

Pool, J., Akhlaghpour, S., & Fatehi, F. (2020). Towards a contextual theory of mobile health data protection (MHDP): A realist perspective. *International Journal of Medical Informatics, 141*, 104196. https://doi.org/10.1016/j.ijmedinf.2020.104196

Saleem, F. (2019). *A novel multiple access quantum key distribution network for secure communication* [Doctoral dissertation, University of Bradford Repository]

Salem, M. A., & Sobaih, A. E. E. (2023). A quadruple "E" approach for effective cyber-hygiene behaviour and attitude toward online learning among higher-education students in Saudi Arabia amid COVID-19 pandemic. *Electronics, 12*(10), Article 2268. https://doi.org/10.3390/electronics12102268

Shah, P., & Agarwal, A. (2023). Cyber Suraksha: A card game for smartphone security awareness. *Information & Computer Security, 31*(5), 456–472.

Skarga-Bandurova, I., Kotsiuba, I., & Velasco, E. R. (2021). Cyber hygiene maturity assessment framework for smart grid scenarios. *Frontiers in Computer Science, 3*, Article 614337. https://doi.org/10.3389/fcomp.2021.614337

Stifel, M., Giroud, K., & Walsh, R. (2022). Cyber hygiene can support cyber peace. In S. J. Shackelford, F. Douzet, & C. Ankersen (Eds.), *Cyber peace: Charting a path toward a sustainable, stable, and secure cyberspace* (pp. 223–229). Cambridge University Press.

Sweeney, J., & Tran, V. (2022). Improving protection against cybersecurity attacks of emergency dispatch centers. In *Proceedings of the 17th International Conference on Information Warfare and Security* (pp. 134–142). Albany, New York, USA.

Szczepaniuk, E. K., & Szczepaniuk, H. (2022). Analysis of cybersecurity competencies: Recommendations for telecommunications policy. *Telecommunications Policy, 26*, 102145.

Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in Science Education, 48*, 1273–1296. https://doi.org/10.1007/s11165-016-9602-2

Teke, A., & Lale, A. (2021). Sosyal medyada etik, bilgi manipülasyonu ve siber güvenlik. *Akademik İncelemeler Dergisi, 16*(2), 45–60.

Tripware. (2018). *Tripwire state of cyber hygiene report*. https://static.fortra.com/tripwire/pdfs/guides/tw-dimensional-research-state-of-cyber-hygiene-gd.pdf (Erişim tarihi: 19 Ocak 2025).

Ugwu, C., Ani, C., Ezema, M., Asogwa, C., Ome, U., Obayi, A., Ebem, D., Olebra, C., & Ukwandu, E. (2022). Towards determining the effect of age and educational level on cyber-hygiene. In *Proceedings of the 4th International Conference on Disruptive Technologies for Sustainable Development*. Abuja, Nigeria. https://doi.org/10.1109/NIGERCON54645.2022.9803154

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems, 128*, 113167.

Webb, T., & Dayal, S. (2017). Building the wall: Addressing cybersecurity risks in medical devices in the U.S.A. and Australia. *Computer Law & Security Review, 33*(4), 419–432.

Whitty, M. T., Moustafa, N., & Grobler, M. (2024). Cybersecurity when working from home during COVID-19: Considering the human factors. *Journal of Cybersecurity, 10*(1), Article tyae001. https://doi.org/10.1093/cybsec/tyae001

Wong, L. W., Lee, V. H., Tan, G. W. H., & Ooi, K. B. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management, 66*, 102552.

Yılmaz, S. Z. (2023). *Siber uzayda özel hayatın gizliliği hakkını yeniden tartışmak* [Doctoral dissertation, Selçuk Üniversitesi].

Zhang, Y., & Malacaria, P. (2023). Keep spending: Beyond optimal cyber-security investment. In *Proceedings of the 36th Computer Security Foundations Symposium* (pp. 1–14). Dubrovnik, Croatia. https://doi.org/10.1109/CSF57540.2023.00024

Article Information Form

Conflict of Interest Disclosure: No potential conflict of interest was declared by the author.

Plagiarism Statement: This article has been scanned by iThenticate.