International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 13 (2021) pp. 300-307

Submitted: 15 Jan 2021; Accepted: 27 May 2021; Publish: 8 Sep. 2021

A Study of Computer Users' Attitude and Awareness towards Cyber Security

Gopal Datt[1], Naveen Tewari[2]

[1] School of Vocational Studies, Uttarakhand Open University,
Haldwani, Uttarakhand, India
gdatt1986@gmail.com

[2] School of Computing, Graphic Era Hill University,
Bhimtal, Uttarakhand, India
navtewari@gmail.com

***Abstract*: The term Cybersecurity surrounded us all around. The Cyber-world or Cyberspace is more than just the Internet. It means an online environment where many participants are involved in social interactions and can touch and influence each other. People are interacting on the Internet through digital media. In this situation, Cybercrimes are rising day-by-day. Users can be safe by becoming more and more aware of security measures used to deal with cybercrimes. This study investigates and analyzed user's attitudes and awareness towards Cybersecurity, and also lightens the approach about the common security threats to deal with. The study also checks the differences in cybersecurity awareness gender-wise, employment status wise, and participants IT related qualification wise. During this study, a survey-based questionnaire was used for collecting primary data about computer user's perceptions towards cybersecurity awareness. The key results are discussed here, where more than 34% of female and 28% male participants are unaware of risks related to sharing personal information among users on the Internet. As such 41% to 51% female, as well as 27% to 38% male, participants are unaware of basic security issues such as-phishing attacks, social engineering attacks, and risks of using public Wi-Fi, etc. All the participants who are involved in this study to participate are well in IT skills. The IT skills are measured in three groups, such as IT fundamentals, Basic office application, and Internet skills. In such categories, more than 85% of participants are either excellent or good. The findings of this study will help in suggesting appropriate measures taken to protect from various cyber-attacks.**

***Keywords*:** Cybersecurity, Impacts of IT literacy, Information security, cyber attacks.

I. Introduction

Today's digital era is also known as the cyber era, where we are surrounded by various digital activities, tools, and techniques because we are highly dependent on the data which is digitally stored in cyberspace or hard drives. This is our self-responsibility to make our things e.g. data, devices, and programs; secure and safe from unauthorized access where we require awareness, skills, and some set of safeguards. In the context of cyber safekeeping, we frequently used the two terms e.g. cybersecurity and information security or data security. Generally, we used both terms interchangeably, but there is quite a difference between both.

The term Cybersecurity denotes the range of security technologies that are intended to protect networks, networks-based programs, and devices, or even whole cyberspace from cyber threats, attacks, and unauthorized access to resources. In today's global conception of reachability of business, this is more crucial to becoming aware of cyber threats and security techniques, because the role of cyber expertise is evolving more and more to protect yourself from the risks related to cyber hacking. In this global scenario, all Internet users having the responsibility of making themselves aware of cyber threats, security breaches, and protect their resources from unethical access. Today's either individuals or organizations are constantly in the race to defend against potential cyber-attacks. A properly cyber educated and well aware staff or individuals are the need of time to keep the resources safe and secure from the cyber-attacks. In this consequence, the proposed study is useful to assess the level of cyber awareness with the impact of IT literacy among computer users. To maintain the integrity and confidentiality of data is known as information security. The term "data" and "information" are closely related to each other. Data means raw facts or figures whereas meaningful facts or processed data are known as information. In the current digital era, we are surrounded by data all over the globe so that our responsibilities are much broader than earlier to protect our systems e.g. programs and information from unauthorized access or misuse.

There is an urgent need to change the attitude of individuals concerning information management practices and preventive measures regarding information privacy and cybersecurity vulnerabilities. In the current scenario, where we are stepping forward for digitized society e.g. smart cities, etc., there is an increasing need of cyber skilled and knowledgeable individuals to cope up with the cybersecurity threats [1].

This study investigates the impacts of IT literacy on cybersecurity awareness among computer users. The author(s) analyzed the responses collected through a questionnaire about IT literacy skills and their impacts on the level of awareness of cybersecurity among computer users. Something is necessary to know about the various issues that are closely related to cybersecurity, such issues are- the role of a strong password, risks related to passing personal information using networks, risks related to unknown e-mail attachments and links, knowing the role of Firewall and Anti-virus, precautionary measures about phishing attacks, social engineering attacks, man-in-the-middle attacks and many more.

II. Material and Methods

A. Review of Literature

Grobler, Vuuren, and Zaaiman [2] conducted a study on "Preparing South Africa for Cyber Crime and Cyber Defense". In their study, they discussed how to deal with making the civil community aware of Cyber Crime and also suggested a defense mechanism against Cyber Crime among Internet users and international cooperation about cyber defense. Kortjan and Solms [3] conducted a study on "A conceptual framework for cyber-security awareness and education in SA". In their study, they pointed out the risks related to cyberspace, of which many Internet users are not aware. The emphasis on the government to initiate and sponsor the cyber-security awareness and education initiatives in the country. They proposed a cyber-security awareness and education framework for Internet users, to assist in creating a cyber-secure culture in the country (SA).

Kleij, Kleinhuis and Young [4] conducted a study in "Computer security incident response team effectiveness: A needs assessment". They discussed the effectiveness of Computer security incident response teams (CSIRTs) during the need when arise. They presented the potential solutions for the problems with performance in incident response and also suggested the list of challenges and needs that should resolve on time.

Aldawood and Skinner [5] conducted a study on "Reviewing Cyber Security Social Engineering Training and Awareness Programs- Pitfalls and Ongoing Issues". In their study, they highlighted pitfalls and ongoing issues that organizations encounter. They suggested preparing human capital as the cybersecurity knowledge base and employee profiling based on cyber awareness and proficiency. Haque [6] conducted a study on "Need for Critical Cyber Defence, Security Strategy, and Privacy Policy in Bangladesh- Hype or Reality?" In his study, he discussed common cyberspace vulnerability issues, cybersecurity strategy, and the need for data privacy policy in Bangladesh. He also denoted security breaching such common vulnerability issues like infecting the device with malware, Trojan, virus, etc.

Orozova, Kaloyanova, and Todorova [7] conducted a study on "Introducing Information Security Concepts and Standards in Higher Education". The author suggested incorporating information security concepts in courses of higher education because security issues are important in this cyber era where the interests of researchers are growing in this field aggressively. Zoto, Kianpour, Kowalski, and Lopez-Rojas [8] conducted a study on "A Sociotechnical Systems Approach to Design and Support Systems Thinking in Cybersecurity and Risk Management Education". They discussed Cybersecurity decisions and bridging the gap between the plan designed by institutions/policy developers and their implementation at the ground level. They further pointed out to promote cybersecurity education in society. They also suggested developing a tool for target users' skills in making quantitative risk decisions, deeper understanding, and the importance of cyber risk management.

Bino [9] advocates greater level of engagement with cyber security awareness among students. The cyber users should ensure to establish a culture of cyber awareness before entering into cyberspace through several connecting mediums. Al-Alawi and Al-Bassam [10] identified several factors related to cybersecurity awareness in banking sector, i.e. gaps between top management and cybersecurity professionals, lack of budgeting, cybersecurity compliance and culture. During the threatening period of COVID-19 global pandemic cyber criminals are targeting individuals as well as organizations to gain unauthorized access through several activities. Mashud [11] suggested the hygienic training, educational, and policy protocols which can help to overcome the dangers of cybercrimes. Moci [12] recommended in his study titled "Cybersecurity Awareness in Albania" to emphasize conducting cybersecurity training for the citizens/professionals because due to the Covid-19 pandemic affect the trend of work from home has practicing where the chances of cyber-attacks are increased.

A brief description of some of the key cyber attacks and threats with their countermeasures are discussed herewith.

B. Notable common security issues

1) Strong passwords

Password is the preliminary security in any information system [13]. A weak password is easily broken and can be used by the broker to threaten its user. It must be taken into consideration how secure and strong is the password at the time of its design. Various techniques are used to check and verify the security of a password [14]. Strong password intents several rules for creating a password e.g. a password should consist of at least 10 characters which necessarily includes a combination of digits, upper case letters, lower case letters, and special symbols And, as well the password should not be common for different logins by such user. Simultaneously, the password must not be a pattern e.g. dates of birth, first name, last name, contact number, etc. Security experts always recommend using a strong and unique password, but in usual practice, it is difficult to use a strong and unique password for the 'N' type of logins by the user.

2) Risk of giving personal information

One should be cautious with how many personal data are posted on the web. Sharing location, telephone number, birthday, and other individual data can mean one is in more danger of fraud, stalking, and badgering. This incorporates data posted via web-based networking media [15].

3) Risks with email attachments and links

Malware can be sent through email attachments. It must be a common policy not to open email messages from unknown

senders. These malicious files or emails must be blocked and stored to spam so that they can be filtered from other messages [16].

4) Firewall

A firewall is a network protection tool that monitors inward and outward traffic and determines whether to allow or block certain traffic based on a set of security rules prescribed in Firewall settings [17]. These rules defined in the firewall can be modified according to the condition and need of the network [18].

5) Anti-virus

The anti-virus software uses signatures of malware or viruses to identify and stop/block them. When this software reaches a particular file that has malicious code resembling an anti-virus database, it blocks its accesses in the computers [19].

6) A computer configured to be automatically updated

There are many applications in a computer that are configured to get automatic updates. These applications can get updates from an unknown source which can be subject to virus attack. Automatic updates must be disabled in the computer and enabled only when there is a sense of security in downloading them [20].

7) SSL (Secure Socket Layer)

SSL is a common standard security technology utilized on the internet for encouraging secure correspondence through validation, encryption, and decryption. This technique uses a private key to encrypt the data transferred over SSL communication. For checking whether a communication over the internet is SSL enabled or not we can check the protocol of the URL, it has to be https: instead of http: [21].

8) Phishing attack

When an attacker creates a copy of an existing webpage to deceive an online user forgetting his personal, password, or financial related information, then this is known as a Phishing attack [22]. This is a network type attack. This can also be done by email spoofing or instant messaging. Users have to take care of phishing attacks so that they cannot be a victim of such frauds [23].

9) Public Wi-Fi networks

Also called hotspots placed in public places such as railway-stations; tourist places, etc. are inadequately monitored and are in-secured. Lots of users when got the opportunity to access these free hotspots, directly access them without knowing how secure these connections are [24].

10) Social engineering attacks

Social networking is growing at a very rapid rate reported above 3% a week. These networking sites like Facebook, LinkedIn, and Twitter, etc provide a way to find new friends. Therefore, lots of people engage themselves in these websites, without knowing the security and privacy factors. These sites are targeted by the attackers frequently for getting the user's identity and then threatening them [25].

11) Risks related to online shopping

The web-based businesses have made incredible walks in giving a helpful, quick, and secure shopping experience for customers. In any case, there is as yet a huge bit of customers whose security fears sway how they go through their cash on the web. Along these lines, security issues related to internet business and client locales must be continually assessed and refreshed with suitable countermeasures [26].

12) Risks related to using public computers

Public PCs are not as sheltered as close to home computers since you don't have the foggiest idea whether the most recent security conventions, like antivirus, have been introduced. You additionally don't have a clue who has utilized the PC before you and if any clients have undermined the gadget security. For example, a thief could introduce a key logger application or equipment to catch each secret phrase composed into the PC. At the point when you enter your email, personal information, web-based shopping, or different passwords that data could go legitimately to a hoodlum [27].

13) Man-in-the-middle attack

When two people communicate through the internet, there is a possibility that the third person can capture the data that is being communicated. This is known as a Man-in-the-middle attack [28]. The Man-in-the-middle can catch the message from the sender and send his message to the beneficiary [29].

C. Need and Scope

Cybersecurity is the fundamental need of a nation in today's digital world. As a country focusing on the digital India program in such a scenario the importance of cybersecurity cannot be obsolete. Notable cybercriminal activities have led the attention towards protecting one's data/infrastructure from unauthorized access. Secure cyberspace protects us from any kind of cyber attacks, such as Malware, Phishing, Man-in-the-middle, Denial-of-service, DNS Tunneling, etc. With the exponential growth of digitization and the tremendous increase in Internet users, there has been a great demand for future cybersecurity experts. This study analysis the role and awareness of computer users towards maintaining secure cyberspace. Here, the author(s) discussed different types of cyberattacks and their counter-measures as well a questionnaire-based survey has been conducted to identify the awareness level of computer users towards cybersecurity.

D. Methodology

This study follows a survey-based descriptive research methodology. It has been carried out to examine the awareness of cybersecurity of computer users, especially in the state of Uttarakhand. The data required for this study was collected from primary sources in the form of a questionnaire. The questionnaire has been prepared and validated through the cybersecurity experts in light of the objectives of this study. The questionnaire contains closed-ended questions and is comprised of three main sections i.e. general information, the status of IT literacy, and awareness of cybersecurity among computer users.

E. The questionnaire

The questionnaire has organized into three sections, section one is about general questions, the second section two is about

to IT Literacy status of the participants and section three is about the status of cybersecurity among computer users. Section one includes several general questions, i.e. Gender, Age Group, Highest Qualification, Employment Status, IT-related Qualification and, etc. Section two includes fourteen questions related to IT literacy and measured using the Likert scale, such questions are grouped into three groups, i.e. Group 1- IT Fundamentals, Group 2- Office Applications, and Group 3- Internet Skills. Section three includes fifteen questions related to cybersecurity awareness. The responses to such questions were recorded in the form of awareness (Yes) and Unawareness (No). The survey results are evaluated using suitable statistical tools, i.e. simple mean, percentage, etc.

F. The Participants/Respondents

The questionnaire for this study was sent through e-mail/WhatsApp/other social mediums to the more than 200 participants (respondents) across the state of Uttarakhand. The total number of 137 complete responses was received on time. The survey was open to the participants to fill for 40 days. The selection of survey participants was based on random sampling with the following criteria having in mind, the age group, the qualification, employment status, etc.

III. Results and Discussion

This study presents a real understanding of various issues related to cybersecurity and also examines the level of cyber awareness among computer users. The general findings from the survey are that there is an urgent need of spreading more awareness regarding cybersecurity, i.e. data/information security, Internet skills, and security. Too many participants are unaware of different cyber-attacks which can become the cause of severe damages. This study organized into three sections; each section is discussed in detail herewith- (1) Demographics (2) IT Literacy (3) Cybersecurity awareness status.

A. Demographics

Gender Wise Demography	
Indicators	**Contribution (%)**
Male	61.3
Female	38.7
Age Group Wise Demography	
19 to 25 Years	30.7
26 to 35 Years	36.5
36 to 45 Years	27.7
46 Years and above	5.1
Highest Qualification Wise Demography	
Graduation or equivalent	29.2
Post-Graduation or equivalent	51.8
Ph. D.	19.0
Employment Status Wise Demography	
Employed	62.8
Unemployed	37.2
IT Related Qualification Wise Demography	
Having IT related Qualification	78.1
Do not having IT related Qualification	21.9
Source: Data Collected Through Questionnaire.	

Table 1. Demographic Status of the Respondents (N=137)

The demographic results are shown in Table 1, and the results are evaluated in terms of Gender, Age group, highest qualification, Employment status, and IT related qualification. The results reveal that 61.3% of males and 38.7% of females contributed their opinion to this study. The age group wise contribution of participants are- 19 to 25 years is 30.7%, 26 to 35 years is 36.5%, 36 to 45 years is 27.7% and above 46 years is 5.1%. In the case the highest qualification wise demographic results are revealed as- Graduation or equivalent is 29.2%, post-Graduation or equivalent is 51.8%, and Ph. D. is 19%. The employment status wise representation of demography is- 62.8% are employed and 37.2% contributors are unemployed. 78.1% of respondents having any formal qualification related to IT whereas only 21.9% of respondents do not have any qualifications related to IT.

B. IT Literacy Status-

The basic computing skills/computer savvy skills of participants are measured using a set of fourteen questions which are further grouped into three categories, i.e. IT fundamentals, Office applications, and Internet skills (see appendix 1). The objectives behind to include this section in our study are to identify the basic practical knowledge of computation and the working ability of participants. The results of such IT literacy/skills are measured using a five-point grade scale, as- Excellent, Good, Average, Poor, and Very Poor. Further, during the processing of results; the responses are combined as- Above Average (Excellent and Good), Average and Below Average (Poor and Very Poor).

Table 2 reveals that in the case of IT fundamentals, 98.5% male and 94.3% female participants are shown as above average whereas in the case of utilizing office applications 97.9% male and 92% female participants are shown as above average. In the case of Internet skills 95.6% male and 86.8%, female participants are recorded as above average.

IT Literacy Indicators	**Nature of Responses Excellent (5), Good (4), Average (3), Poor (2), Very Poor (1)**								
	Male (%)			**Female (%)**			**Total (%)**		
	5, 4	**3**	**2, 1**	**5, 4**	**3**	**2, 1**	**5, 4**	**3**	**2, 1**
Group 1-IT Fundamentals	98.5	1.5	0	94.3	2.8	2.8	96.4	2.2	1.4
Group 2- Office Applications	97.9	2.1	0	92	3.3	4.7	94.9	2.7	2.4
Group 3- Internet Skills	95.6	3.8	0.6	86.8	4.1	9.1	91.2	3.9	4.9
Source: Data Collected Through Questionnaire.									

Table 2. Status of IT Literacy- Gender Wise (N=137)

Table 3 reveals the IT skills of participants into three set of parameters i.e. IT Fundamentals, Office Applications, and Internet Skills. In the case of IT fundamentals, 98.5% employed and 94.1% unemployed participants are shown above-average whereas in the case of working ability on office tools 97.4% employed and 92.6% unemployed participants are shown above average. In the case of Internet skills 93% employed and 90.8%, unemployed participants are recorded as above average.

IT Literacy Indicators	**Nature of Responses Excellent (5), Good (4), Average (3), Poor (2), Very Poor (1)**

	Employed (%)			Unemployed (%)			Total (%)		
	5, 4	3	2, 1	5, 4	3	2, 1	5, 4	3	2, 1
Group 1- IT Fundamentals	98.5	1.2	0.3	94.1	3.4	2.5	96.3	2.3	1.4
Group 2- Office Applications	97.4	1.5	1.2	92.6	4.4	2.9	95	2.9	2.1
Group 3- Internet Skills	93	3.3	3.7	90.8	4.9	4.2	91.9	4.1	4

Source: Data Collected Through Questionnaire.

Table 3 - Status of IT Literacy- Employment Status Wise (N=137)

C. Cybersecurity Awareness-

Cybersecurity awareness makes us aware to protect and develop the ability to identify the harms related to such cyber-attacks. The awareness regarding cybersecurity is a combination of two such related things, i.e. "to know" and "to act" to protect one's digital assets. Table 4 reveals the status of cybersecurity awareness gender-wise and employment status-wise through fifteen key points to maintain the secure digital world. The participant's opinion is recorded as either they are aware or unaware of the security issues, i.e. needs of strong passwords, enabling a firewall, installing and enabling anti-virus software, configuring the computer system automatically updated on, etc.

Note- Aware (1), Not Aware (2)								
Cyber awareness and information security Indicators	Gender Wise				Employment Status Wise			
	Male (%)		Female (%)		Employed (%)		Unemployed (%)	
	(1)	(2)	(1)	(2)	(1)	(2)	(1)	(2)
Q1- Aware of utility of strong passwords.	95.2	4.8	88.7	11.3	94.2	5.8	90.2	9.8
Q2- Aware of filling personal information in websites/apps without knowing the risks related with it.	71.4	28.6	66.0	34	66.3	33.7	74.5	25.5
Q3- Aware of opening unknown e-mail attachments/links.	83.3	16.7	75.5	24.5	86	14	70.6	29.4
Q4- Aware of enabling Firewall.	81	19	73.6	26.4	82.6	17.4	70.6	29.4
Q5- Aware of enabling/automatic updating about Anti-virus.	83.3	16.7	79.2	20.8	83.7	16.3	78.4	21.6
Q6- Aware of enabling Windows/Operating System automatically updated.	72.6	27.4	58.5	41.5	73.3	26.7	56.9	43.1
Q7- Aware of SSL (Secured Socket Layer).	65.5	34.5	45.3	54.7	60.5	39.5	52.9	47.1
Q8- Aware of phishing attack.	73.8	26.2	56.6	43.4	72.1	27.9	58.8	41.2
Q9- Aware of risks related to public Wi-Fi.	76.2	23.8	58.5	41.5	72.1	27.9	64.7	35.3
Q10- Aware of social engineering attacks.	65.5	34.5	41.5	58.5	58.1	41.9	52.9	47.1
Q11- Aware of whom to contact, if hacked.	61.9	38.1	49.1	50.9	58.1	41.9	54.9	45.1
Q12- Aware of risks related to online shopping.	81	19	75.5	24.5	79.1	20.9	78.4	21.6
Q13- Aware of risks related to using public computers e.g. cyber cafe, etc.	83.3	16.7	79.2	20.8	81.4	18.6	82.4	17.6
Q14- Aware of man-in-the-middle attack.	64.3	35.7	47.2	52.8	54.7	45.3	62.7	37.3

Source: Data Collected Through Questionnaire.

Table 4- Status of Cyber Security awareness- Gender Wise and Employment Status Wise (N=137)

Table 4 defines the matrix of participant's cybersecurity awareness, in this instance (Q1) 4.8% male, 11.3% female, 5.8 % employed, and 9.8% unemployed participants are recorded as unaware of the utility of strong password. To overcome such a security breach, one should define the importance of a strong password, because such passwords not easy to predict/guess. In the case of (Q2) filling personal information in any website or application without knowing the security risks, 28.6% male, 34% female, 33.7 % employed, and 25.5% unemployed participants are recorded to unaware of such risks. To overcome such severe risks of security, one should organize awareness workshops/training camps, and also explain the risks of sharing personal information among the participants.

In the case of (Q3) opening any unknown e-mail attachments or links, 16.7% male, 24.5% female, 14% employed, and 29.4% unemployed participants are recorded as unaware of such risks. In today's scenario, this is the prime cause of online fraud, where one should well aware of such online links, phone calls, messages, e-mails, social media posts, lottery offers, and greedy offers from various mediums of communications. To make our citizens safe and aware of such kinds of fraud needs to have a pan-India campaign. In the case of (Q4) enabling Firewall, 19% male, 26.4% female, 17.4% employed, and 29.4% unemployed participants are recorded to unaware to activate firewalls in their machines. A firewall is an interface or a kind of gateway between two networks. Its purpose is to control the data traffic and to protect its network from unwanted data traffic. The participants should always aware to enable firewalls in their computer system.

In the case of (Q5) enabling/automatic updating Anti-Virus, 17.7% male, 20.8% female, 16.3% employed, and 21.6% unemployed participants are recorded to unaware. To maintain a secure cyber-world, one should ensure to enable anti-virus applications, and also it should be updated from time to time. In the case of (Q6) enabling Windows/Operating System automatically updated, 27.4% male, 41.5% female, 26.7% employed, and 43.1% unemployed participants are recorded to unaware of such issues. The recorded responses are producing red signals towards cybersecurity measures. The awareness of Secured Socket Layer (Q7), phishing attacks (Q8), risks related to using public Wi-Fi (Q9), and social engineering attacks (Q10) is recorded as- 65.5%, 73.8%, 76.2%, and 65.5% respectively among male participants and 45.3%, 56.6%, 58.5%, and 41.5% among female participants. Among the same security factors, employment status wise awareness of employed participants is 60.5%, 72.1%, 72.1%,

58.1%, and unemployed participants are 52.9%, 58.8%, 64.7%, and 52.9% respectively.

In the case of (Q11) whom to contact, if someone hacked your device, 38.1% male, 50.9% female, 41.9% employed, and 45.1% unemployed participants are recorded to unaware of such issue. This issue needs to address on a priority basis because of providing instant help to such victims. The awareness of risks related to online shopping (Q12) and risks related to using public computers e.g. ybercafé, etc. (Q13) is recorded as- 81%, and 83.3% respectively among male participants and 75.5%, and 79.2% among female participants. Among the same security factors, the employment status wise awareness level of employed participants is 79.1%, and 81.4% and unemployed participants are 78.4%, and 82.4% respectively. In the case of (Q14) man-in-the-middle attacks, 35.7% male, 52.8% female, 45.3% employed, and 37.3% unemployed participants are recorded to unaware of such attacks. To overcome such kinds of attacks, this issue needs to address on a priority basis.

And, finally on average of more than 92% of participants recorded their opinion that cybersecurity measures are necessary for individuals. There is a momentous understanding of cybersecurity in both male and female participants. Females have low awareness (41% - 58%) in topics asked in Q6 to Q11 and Q14. These questions involve SSL, phishing attacks, Wi-Fi risks, hacking, man-in-the-middle attacks, etc. which require technical understanding. The use of SSL is also not known to 34% of males. This trend is also seen in employed and unemployed users. The topics that require more technical knowledge has a low level of awareness, i.e. about 39% to 41% employed persons and about 35% to 47% unemployed persons.

Table 5 reveals cybersecurity awareness among the participants those having IT related qualification and those do not have such qualifications. 95.3% of participants with IT qualification are aware of strong passwords (Q1) whereas participants those do not carry any such qualification is less aware (83.3%). It shows a clear gap between the participants having any formal technical qualifications and nontechnical background. In the case of filling in personal information in any website or application without knowing the security risks, 26.2% of IT qualification holders, and 46.7% of non-IT qualification holders are recorded to unaware of such risks. This is an alarming situation for the authorities and security experts. In the case of opening any unknown e-mail attachments or links, 18.7% of IT qualification holders, and 23.3% of non-IT qualification holders are recorded to unaware of such risks.

Note- Aware (1), Not Aware (2)				
Cyber awareness and information security Indicators	**Do you have IT related Qualification?**			
	IT (%)		**Non-IT (%)**	
	(1)	**(2)**	**(1)**	**(2)**
Q1- Aware of utility of strong passwords.	95.3	4.7	83.3	16.7
Q2- Aware of filling personal information in websites/apps without knowing the risks related with it.	73.8	26.2	53.3	46.7
Q3- Aware of opening unknown e-mail attachments/links.	81.3	18.7	76.7	23.3
Q4- Aware of enabling Firewall.	79.4	20.6	73.3	26.7
Q5- Aware of enabling/automatic updating about Anti-virus.	83.2	16.8	76.7	23.3
Q6- Aware of enabling Windows/Operating System automatically updated.	67.3	32.7	66.7	33.3
Q7- Aware of SSL (Secured Socket Layer).	65.4	34.6	30	70
Q8- Aware of phishing attack.	72	28	50	50
Q9- Aware of risks related to public Wi-Fi.	73.8	26.2	53.3	46.7
Q10- Aware of social engineering attacks.	61.7	38.3	36.7	63.3
Q11- Aware of whom to contact, if hacked.	60.7	39.3	43.3	56.7
Q12- Aware of risks related to online shopping.	81.3	18.7	70	30
Q13- Aware of risks related to using public computers e.g. cyber cafe, etc.	86	14	66.7	33.3
Q14- Aware of man-in-the-middle attack.	64.5	35.5	33.3	66.7
Q15- Are cybersecurity measures necessary for individuals?	94.4	5.6	83.3	16.7

Source: Data Collected Through Questionnaire.

Table 5 - Status of Cyber Security awareness- IT related qualification wise (N=137)

Author(s) wants to lighten the areas where more than 30% IT/ non-IT qualification holder participants are recorded to unaware of cybersecurity issues, i.e. aware of enabling Windows/Operating System automatically updated, aware of Secured Socket Layer, aware of phishing attacks, aware of risks related to public Wi-Fi, aware of social-engineering attacks, aware of whom to contact if hacked, aware of risks related to online shopping, aware of risks related to using public computers, and aware of man-in-the-middle attacks.

IV. Conclusion

Cybersecurity is important for individuals as well as for organizations because everything moving towards digitization. Cybersecurity vulnerabilities are increasing day-by-day because of growing information technology systems and the careless approach of computer users towards cybersecurity. This study focuses on the importance and issues involved with cybersecurity among computer users. In this digital world, security measures are of prime concern to ensure the data integrity, data safety, and security of the digital infrastructure. This study indicates the pre-mature level of cybersecurity awareness among computer users. In such a scenario, it is very difficult to save our digital resources i.e. data, programs, networks, and devices from unauthorized access. Cybersecurity awareness is the need of time, and as well it is very urgent to make it practically applicable.

This study found that the participants who hold any IT related qualifications are having a somehow better level of cybersecurity awareness (refer to Table 5). The basic knowledge/understanding of the operational computer system i.e. firewall, anti-virus, software configuration, and information security is shown by such users. The cybersecurity awareness status of the computer users among

fourteen key points of cybersecurity indicators is not satisfactory. To overcome such issues the policymakers/authorities must plan a mass awareness about cybersecurity vulnerabilities through different mediums of communication as well as hands-on-training.

The present study is limited in terms of survey sample size and location because of limited availability of resource used for the research. A more specific survey for assessing cyber awareness of the participants based on their job roles and location can be expected to conduct in future. Such expected study will have better insights about to assessing the awareness of cyber security among the participants.

Cybercrime activities are the key terrorizations we are facing in currently. We should have aware of such crimes and be able to stop and save ourselves from these threats. There is a need for proper tackling of security measures at the personal and professional levels. Table 5, clearly shows that the participants having IT-related qualifications are also having a good level of cybersecurity awareness. This gives us the reason for concluding the following points in terms to increase cybersecurity awareness.

A. The ICT/cybersecurity-related training programs should be organized at the school, department, and office levels, to enhance the working knowledge of such types of tools and also achieving the advanced level of skill.

B. Workshops on Cybersecurity and awareness should be conducted mandatorily on regular basis and it should be planned for different kinds of workforce accordingly to their needs and job role. So that new threats and their security measures can also be suggested to such type of users.

C. All the computer/smart device users must have a minimum level of cybersecurity awareness so that such type of users can easily determine the do's and don't do's about security issues. And also, can prevent man-made attacks/frauds.

D. Simultaneously with cybersecurity awareness programs, IT literacy programs must be encouraged to make their reachability to the remotest and deprived sections of the society so that the end-user can also protect himself from such cyber attacks.

E. One should have the knowledge of whom to contact for reporting/emergency response if someone's computer system / smart device/ programs are hacked.

F. All the smart device users must have a minimum level of IT skills and attitude to read the alerts/ messages and behave accordingly. At the time of the installation of any new application, every user must read and understand the 'terms and conditions' option. In many cases, it has been noted that the control of your device transferred to the hackers, because of ignoring the alerts/messages that popped up during the installation of a new application.

G. At last, but not least, all smart device users must have a minimum moderate level of knowledge about cyber laws and related issues. Cybersecurity related short duration and low cost either online or offline courses should be offered through local/regional languages so that maximum reachability can be ensured. Simultaneously, for the sake of Internet users, they should have a good understanding of social media uses/limits/related laws, and rights.

References

[1] Burkell, J. A., Fortier, A., Valentino, L. D. and Roberts, S. T. (2015). Enhancing Key Digital Literacy Skills: Information Privacy, Information Security, and Copyright/Intellectual Property. *FIMS Publications*. https://ir.lib.uwo.ca/fimspub/35

[2] Grobler, M., Vuuren, J. J. V. and Zaaiman, J. (2013). Preparing South Africa for Cyber Crime and Cyber Defense. Systemics, *Cybernetics And Informatics*. Vol. 11(7), pp. 32-41, ISSN: 1690-4524.

[3] Kortjan, N. and Solms, R. V. (2014). A conceptual framework for cyber-security awareness and education in SA. *SACJ* No. 52, pp. 31-41.

[4] Kleij, R. V. D., Kleinhuis, G. and Young, H. (2017). Computer security incident response team effectiveness: A needs assessment. *Frontiers in Psychology*, Vol. 8, DOI: 10.3389/fpsyg.2017.02179

[5] Aldawood, H. and Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs- Pitfalls and Ongoing Issues. *Future Internet*. Vol. 11(73), doi:10.3390/fi11030073

[6] Haque, A. B. (2019). Need for Critical Cyber Defence, Security Strategy and Privacy Policy in Bangladesh-Hype or Reality? *International Journal of Managing Information Technology (IJMIT)*, Vol. 11 (1), pp. 37-50. DOI: 10.5121/ijmit.2019.11103

[7] Orozova, D., Kaloyanova, K. and Todorova, M. (2019). Introducing Information Security Concepts and Standards in Higher Education. *TEM Journal*, Vol. 8(3), Pp. 1017-1024, ISSN 2217-8309, DOI: 10.18421/TEM83-46.

[8] Zoto, E., Kianpour, M., Kowalski, S. J., and Lopez-Rojas, E. A. (2019). A Socio Technical Systems Approach to Design and Support Systems Thinking in Cybersecurity and Risk Management Education. *Complex Systems Informatics and Modeling Quarterly (CSIMQ)*. Article 106, Issue 18, pp.65–75, https://doi.org/10.7250/csimq.2019-18.04

[9] Bino, J. V. (2021). Cyber Security Awareness By Using Social Media Platforms Among Students. *International Journal of Research*, 8(5), 581-589, p-ISSN: 2348-6848, e-ISSN: 2348-795X.

[10] Al-Alawi, A. I. & and Al-Bassam, S. A. (2019). Assessing The Factors of Cybersecurity Awareness in the Banking Sector. *AGJSR*, 37(4), 17-31.

[11] Mashud, A. (2020). Some Cyber Security Hygienic Protocols for Teleworkers in Covid-19 Pandemic Period and Beyond. *International Journal of Scientific & Engineering Research (IJSER)*, 11(4), 1401-1407, ISSN 2229-5518.

[12] Moci, E. (2021). Cybersecurity Awareness in Albania. *European Journal of Interdisciplinary Studies*, 7(1), 1-6, ISSN (P)- 2411-958X, ISSN(O)- 2411-4138.

[13] Song, J., Wang, D., Yun, Z. and Han, X. (2019). Alphapwd: A Password Generation Strategy Based on Mnemonic Shape. *IEEE Access*, vol. 7, pp. 119052-119059, ISSN: 2169-3536, Doi: 10.1109/ACCESS.2019.2937030.

[14] Galbally, J. Coisel, I. and Sanchez, I. (2017). A New Multimodal Approach for Password Strength Estimation- Part I: Theory and Algorithms. *IEEE Transactions on Information Forensics and Security*. vol. 12(12), pp. 2829-2844, ISSN(P): 1556-6013, ISSN(E): 1556-6021, Doi: 10.1109/TIFS.2016.2636092.

[15] Personal Information and privacy (nd.), Accessed online at https://www.cyber.gov.au/acsc/view-all-content/advice/personal-information-and-privacy, Last Accessed- 2020/08/11

[16] Vaisanen, T., Trinberg, L., and Pissanidis, N. (2016). I accidentally malware - what should I do... is this dangerous? Overcoming inevitable risks of electronic communication. *NATO Cooperative Cyber Defence Centre of Excellence*. https://ccdcoe.org/sites/default/files/multimedia/pdf/I%20accidentally%20malware.pdf

[17] Cheng, Y., Wang, W., Wang, J. & Wang, H. (2019). FPC: A new approach to firewall policies compression. *Tsinghua Science and Technology*. Vol. 24(1), pp. 65-76, ISSN: 1007-0214, Doi: 10.26599/TST.2018.9010003.

[18] Voronkov, A., Martucci, L. A. and Lindskog, S. (2020). Measuring the Usability of Firewall Rule Sets. *IEEE Access*. Vol. 8, pp. 27106-27121, ISSN: 2169-3536, Doi: 10.1109/ACCESS.2020.2971093.

[19] Ford, R. (2004). The wrong stuff? [computer viruses]. *IEEE Security & Privacy*. Vol. 2(3), pp. 86-89, ISSN(P): 1540-7993, ISSN(E): 1558-4046, Doi: 10.1109/MSP.2004.27.

[20] Alhamed, K., Silaghi, M. C., Hussien, I. and Yang, Y. (2013). Security by decentralized certification of automatic-updates for open-source software controlled by volunteers. *Florida Tech*.

[21] Alnatheer, M. A. (2014). Secure Socket Layer (SSL) Impact on Web Server Performance. *Journal of Advances in Computer Networks*. Vol. 2(3), pp. 211-217. Doi:10.7763/jacn.2014.v2.114.

[22] Merwe, A. V. D., Loock, M. and Dabrowski, M. (2005). Characteristics and responsibilities involved in a Phishing attack. *Proceedings of the 4th International Symposium on Information and Communication Technologies (WISICT 05). Trinity College Dublin*, pp. 249-254.

[23] Gupta, S., Singhal, A. and Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. International Conference on Computing, *Communication and Automation (ICCCA). Published by IEEE Xplore.* ISBN(E): 978-1-5090-1666-2, pp. 537-540, doi: 10.1109/CCAA.2016.7813778.

[24] Lugovic, S., Mrsic, L. and Korona, L. Z. (2019). Public WiFi Security Network Protocol Practices in Tourist Destination. In: Esposito C., Hong J., Choo KK. (eds) Pervasive Systems, Algorithms and Networks. I-SPAN 2019: *Communications in Computer and Information Science.* Vol. 1080. Published by Springer, Cham. Online ISBN: 978-3-030-30143-9. DOI: https://doi.org/10.1007/978-3-030-30143-9_27

[25] Krombholz, K., Hobel, H., Huber, M. and Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications.* Vol. 22, pp. 113-122, ISSN: 2214-2126, https://doi.org/10.1016/j.jisa.2014.09.005.

[26] Matbouli, H. and Gao, Q. (2012). An overview on web security threats and impact to e-commerce success. *Published in 2012 International Conference on Information Technology and e-Services, Sousse, Tunisia.* ISBN(E): 978-1-4673-1166-3, pp. 1-6, Doi: 10.1109/ICITeS.2012.6216645.

[27] Keep Yourself Safe When Using Public Computers (nd.), Accessed online at - https://www.idtheftcenter.org/keep-yourself-safe-when-using-public-computers/ Last Accessed- 2020/08/11

[28] Glass, S. M., Muthukkumurasamy, V. and Portmann, M. (2009). Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks. Published by IEEE Xplore. Published in 2009 *International Conference on Advanced Information Networking and Applications, Bradford, UK*. ISSN(E): 2332-5658, DOI: 10.1109/AINA.2009.131

[29] Wang, Y., Wang, H., Li, Z. and Huang, J. (2009). Man-in-the-middle attack on BB84 protocol and its defence. *Published by IEEE Explore. 2nd IEEE International Conference on Computer Science and Information Technology, Beijing.* pp. 438-439, ISBN: 978-1-4244-4519-6, doi: 10.1109/ICCSIT.2009.5234678.

Author Biographies

Dr Gopal Datt is currently working as an Assistant Professor in Uttarakhand Open University, Haldwani, Uttarakhand, India and has a total of 12 years of teaching experience in higher education. His area of interest is E-Learning, Learner support services in Open and Distance Learning (ODL), Web-based programming. His area of interest is e-learning, web-based programming.

Dr Naveen Tewari is currently working as an Associate Professor in the School of Computing at Graphic Era Hill University, Bhimtal, Uttarakhand, India. He has more than 12 years of teaching experience at graduate and post-graduate level. His area of interest is Cloud Computing, Digital programming, Fog computing.