Journal of Computing and Security

Research Article, 2023, Volume 10, Number 1 (pp. 1–16)

http://www.jcomsec.org

RSAM: A Questionnaire for Ransomware Security Awareness Measurement

Fakhroddin Noorbehbahani [a,*], Anahita Taghiyar [b], Azadeh Rezvani [b]

[a] *Faculty of Computer Engineering University of Isfahan, Isfahan, Iran.*

[b] *Faculty of IT Engineering Sheikh Bahaei University, Isfahan, Iran.*

ARTICLE INFO.

Article history:

Received: 28 August 2022

Revised: 25 December 2022

Accepted: 28 December 2022

Published Online: 8 April 2023

Keywords:

Ransomware, Security Awareness, Questionnaire Design, Cybersecurity, Security Behaviors.

ABSTRACT

Today ransomware is a significant security threat to both organizations and humans in the e-commerce and digital era. Poor human security awareness is a critical vulnerability that increases the risk of ransomware attacks. To protect against ransomware, an established and effective strategy is to improve the security awareness of employees and users about ransomware. To implement this strategy, in the first step, it is vital to measure the ransomware awareness of the users and, next, try to enhance the level of awareness through education, training, and knowledge sharing about the attack. To our best knowledge, there does not exist any questionnaire specially designed to assess ransomware awareness. In this paper, a novel questionnaire development process is presented and applied to produce a questionnaire for measuring security awareness about ransomware called RSAM. The Persian version of the questionnaire (RSAM-P) is developed and validated using a sample of 216 participants completing the questionnaire. The reliability and validity testing of the RSAM-P indicate that the questionnaire consisting of 21 questions is effective and reliable in assessing ransomware awareness. Moreover, in this paper, RSAM-E, the English version of the RSAM, is presented.

1 Introduction

Ransomware is a type of computer malware that usually encrypts or locks the data and requests ransom money to enable the victim to regain access to the data. The cost of ransomware mitigation is increasing. According to the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN), in the first half of 2021, there was $590 million in ransomware-related activity, indicating about a 40% increase regarding the reported $416 million in ransomware costs in the whole of 2020 [1]. The Cybersecurity Ventures predicts that ransomware costs will reach $265 billion by 2031, and every 2 seconds, a new ransomware attack will be occurred, representing a significant acceleration from recent years [2]. The advent of the COVID-19 pandemic has raised ransomware attacks targeting various institutions such as healthcare, financial organizations, government, etc. This phenomenon may be the consequence of remote and home-based work that is less secure than on-site and office work [3].

Ransomware could be classified into five main categories regarding attack methods: screen locker, crypto-ransomware, file-less ransomware, VM-based

* Corresponding author.

Email addresses: noorbehbahani@eng.ui.ac.ir (F. Noorbehbahani), anahitataghiyar1993@gmail.com (A. Taghiyar), msrezvani65387@gmail.com (A. Rezvani)

https://dx.doi.org/10.22108/JCS.2022.134927.1104

ISSN: 2322-4460

ransomware, and ransomware with data exfiltration [4]. The screen locker type locks the computer system and requests a ransom to unlock the victim's computer. Screen locker ransomware can lock the whole OS or display fake warnings to threaten users. Crypto-ransomware (cryptographic ransomware) applies cryptography methods to block the users' access to data. This type of ransomware has been becoming predominant recently (90% of ransomware attacks in 2019 belong to this category). Fileless ransomware runs without injecting the executables into file systems, instead, it employs command scripts (e.g., JavaScript, PowerShell, batch commands) or Remote Desktop Protocol (RDP) to perform attacks. VM-Based ransomware uses a VM on the victim's system to hide its presence from malware detection tools and encrypts the host files in the VM. The last type is ransomware with data exfiltration that, instead of threatening users to block their access, blackmails them with a data leak of sensitive data [4].

Ransomware protection strategies include detection, defense, and prevention which are proactive, reactive, and preemptive approaches, respectively. Access control and user awareness have been reported as prevention mechanisms in the literature on ransomware mitigation. Access control restricts access to the files to prevent ransomware encryption, and user awareness tries to restrain ransomware attacks by improving the security awareness of the users, consequently lessens human errors [3].

Khando et al. reviewed and summarized information security awareness methods and factors to improve employee awareness in private and public sector organizations [5]. Their findings imply that theoretical models and gamification are the methods widely applied in both private and public organizations, while the constructivist approach and violation detections are some of the methods applied only in private organizations. Private organizations apply security awareness methods focusing on the individual level, and PDCA (Plan-Do-Check-Act) model is effective in content creation for awareness programs. Management support, education and training, culture, ISP (Information Security Policies) provision, and SETA (Security Education Training Awareness) programs are the common factors for elevating awareness in both types of organizations.

Chung emphasized the importance of employee awareness to defend against ransomware attacks [6]. The author suggested five prevention tips as follows: install and apply antivirus or anti-malware software on every computer and mobile device in use, choose strong and unique passwords for personal and work accounts, regularly back up files to an external hard drive disconnected from the Internet, never open suspicious links and email attachments, and employ mirror shielding technology (such as NeuShield) as a failsafe data protection measure.

Thomas examined how users can protect themselves from phishing attacks which are usually considered a prerequisite of ransomware attacks [7]. The author suggested segmenting company employees by considering features such as familiarity with phishing and the level of their job's sensitivity. Then, for each segment, targeted training should be developed, including real-life examples, case studies, potential damages caused by phishing, and actual incidents the company faces.

A significant and effective tactic for ransomware prevention is to educate, train and raise users' and employees' awareness about ransomware. That is why Kaspersky introduced raising employees' awareness as an essential factor to protect against ransomware in 2021 [8]. Before any education and training to elevate ransomware awareness, it is essential to measure and evaluate the current awareness of the users to gauge the respected vulnerability level.

There are some instruments to assess user awareness, such as the information security user awareness assessment published by the information security office of Louisville University [9], a self-completion questionnaire presented in [10], and HAIS-Q [11], however, it is beneficial to develop self-assessment instruments specially designed to measure a certain type of awareness. Because today, ransomware attacks are prevalent and the imposed mitigation costs are too high, there is a strong need to develop a questionnaire for measuring ransomware awareness. To our best knowledge, there does not exist such a self-assessment measure.

In this research, a Ransomware Security Awareness Measurement in Persian called RSAM-P is developed and validated. After translation and cultural adaptation of the RSAM-P, an English version of the RSAM is also proposed called RSAM-E.

To develop our proposed ransomware security awareness questionnaire, it is vital to apply an effective questionnaire development process with the following features:

- Defining sub-processes (phases) and activities needed to develop a questionnaire together with their relations and sequences
- Supporting the steps required to develop multilingual questionnaires
- Including all phases needed to develop a questionnaire i.e. design, data collection, and validation phases
- Being simple, usable, and easy to follow

According to our investigations, we did not find any questionnaire development process incorporating all the above-mentioned features. Therefore, we also propose a novel questionnaire development process, including design, data collection, and translation together with cultural adaptation phases.

The paper is organized as follows. Section 2 outlines related work in the field of measuring security awareness through questionnaires. In Section 3, the RSAM development process is described in detail. Section 4 discusses RSAM benefits, and finally, Section 5 concludes the study and highlights the feature work.

2 Related Work

Protecting computer systems and organizations from information security threats is not feasible through only technical solutions since human errors also play an important role in information security breaches. Therefore, organizations should put much attention to measuring their employees' information security awareness so that they can design and implement educational and awareness programs [12].

Alharbi and Tassaddiq studied and measured the level of cybersecurity awareness of undergraduate students of Majmaah university through a designed questionnaire [13]. They employed a quantitative research methodology to evaluate and analyze the hypotheses. They examined security concerns about electronic emails, computer viruses, phishing, forged ads, popup windows, and supplementary outbreaks on the Internet. The questionnaire encompasses 50 questions to cover different aspects of cybersecurity, including demographics (5 questions); Internet usage (10 questions); the use of security tools, such as antivirus and firewall (7 questions); phishing awareness (5 questions); cryptology (8 questions); browser security (5 questions); social networking (4 questions); and cybersecurity knowledge (6 questions).

Kusumawati applied human security awareness measurement to assess user awareness through a model that comprises 3 factors, namely knowledge, attitude, and behavior [14]. Each factor incorporates five key areas of focus consisting of two questions, and the total number of questions is 30. The information security awareness level is calculated based on the respondent's answer and the Multiple Criteria Decision Analysis (MCDA) method. The authors have not analyzed the validity and reliability of the proposed instrument.

Parson and her colleagues introduced an instrument called the Human Aspects of Information Security Questionnaire (HAIS-Q), to assess the information security awareness of the users by examining seven focus areas as follows: password management, email use, internet use, social media use, mobile devices, information handling, and incident reporting [11]. HAIS-Q consists of 63 specific statements which have been tested and validated in several ways reported in [12], [15], and [16].

Bijlsma et.al. presented a reduced version of the HAIS-Q including 45 questions called R-HAIS-Q [17]. R-HAIS-Q has been developed based on focus group interviews, including five focus areas password management, email use, social media use, mobile devices, and incident reporting based on KAB (Knowledge, Attitude, Behavior) model. The results of the R-HAIS-Q collecting data of headquarter and branch employees in the banking industry denote that within the 'mobile devices' and 'incident reporting' focus areas, no significant differences have been found, but, within the remaining three areas, several important differences between both groups were detected [17].

Schmidt et. al. presented three simple security awareness questions to measure the security awareness of employees in healthcare called SISA [18]. The questions are designed based on generalizing HAIS-Q that can be incorporated into a more extensive survey. The authors believe that it is not feasible to develop a survey intended only for measuring security awareness because of inherent problems such as associated costs and low response rates. They also mentioned that the SISA questions should be further validated.

Papp and Lovaas analyzed HAIS-Q to assess the relationship between employee knowledge, attitude, and behavior [19]. The author's findings imply that HAIS-Q could be enhanced because, regarding its question's constructs, some categories did not show a strong correlation as expected. Hence, they recommended redesigning the HAIS-Q questions to improve the content validity of the instrument and applying NIST SP 800–53 [20] and the FFIEC's Cybersecurity Assessment Tool [21], to redesign and develop a specialized version of the HAIS-Q for financial institutions. However, The results reported in [19] are highly questionable because the authors have employed a tiny sample (N=31) to evaluate the instrument.

Alzubaidi examined the level of cyber-security awareness in Saudi Arabia through a proposed questionnaire that includes four parts, namely, personal and skill information, cybersecurity activities, cybercrime consciousness, and case reporting [22]. The questionnaire consists of 36 questions which were tested on 1230 participants and its reliability and validity were analyzed, however, the authors mentioned that the questionnaire is too lengthy and a shorter version should be investigated.

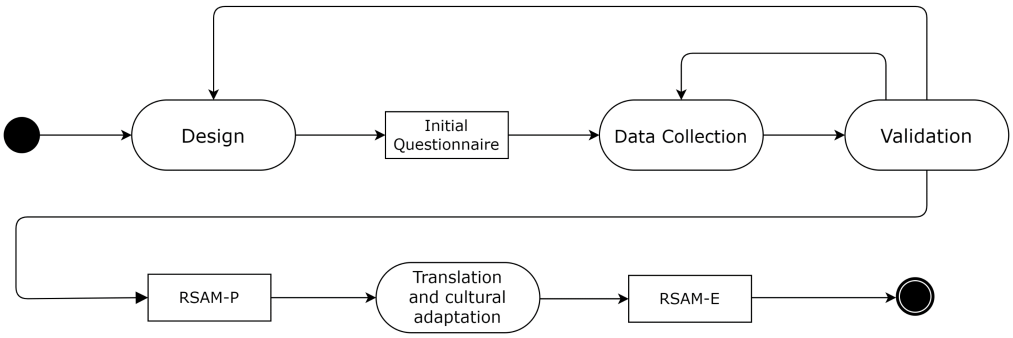

Figure 1. Questionnaire Development Process.

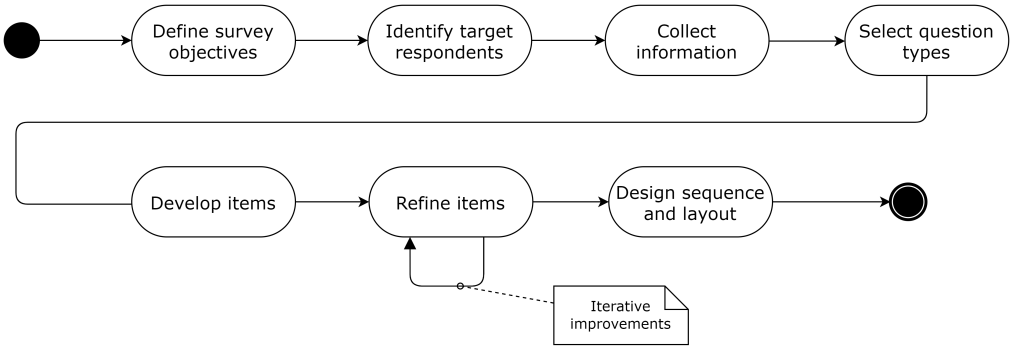

Figure 2. Questionnaire Design Activities.

Bitton et.al. presented a framework for measuring information security awareness of smartphone users about social engineering attacks [23]. The proposed framework relies on questionnaires (including 46 questions) and objective data sources (a mobile agent and a network traffic monitor) to analyze real users' behavior to assess security awareness.

Table1 compares security awareness questionnaires. Based on our investigations, the HAIS-Q questionnaire is a reliable and widely accepted instrument for measuring the security awareness of users and has been validated several times. However, there is no validated questionnaire for assessing security awareness in Persian. As mentioned before, today, ransomware attacks are the most observed and crucial security threat. To our best knowledge, there isn't any questionnaire to assess ransomware awareness. Therefore, the purpose of this paper is to prepare a questionnaire to measure the vulnerability of users to ransomware.

3 Questionnaire Development

To develop the questionnaire, we propose and apply the process depicted in Figure 1. The first step of the development process is to design the questionnaire. Next, in the data collection step, the Persian language respondents are asked to complete the questionnaire. After validation of the collected data and questionnaire modifications, RSAM-P (the Persian version) is produced. Then, translation and cultural adaptation of the RSAM-P rise to RSAM-E (the English version of the questionnaire). The activities of the questionnaire development process are described in more detail in the following sub-sections.

A. Questionnaire design

Figure 2 displays the questionnaire design activities elaborated in the following sections.

1) Define survey objectives

   The first activity of the design process is to define the objectives and aims of the questionnaire. This activity, should find the answers to the following questions: What is the main objective of the questionnaire? What information is gathered by the questionnaire?

   The objective of the RSAM is to measure the ransomware security awareness of users to gauge human vulnerability to ransomware. RSAM should gather any information about users reflecting their awareness of ransomware protection.

2) Identify target respondents

   After defining the objectives, it is time to identify the target respondents. This activity should answer the following questions: Who are the target users supposed to complete the questionnaire? What are

Table 1. Comparison of Questionnaires Measuring Security Awareness.

Questionnaire	# of items	Language	Reliability and validity evaluation	# of Participants	Applying a questionnaire development process	Including ransomware-specific items
Alharbi and Tassaddiq [13]	50	English, Arabic	Both	576	×	×
Kusumawati [14]	30	English	None	126	×	×
Parson et.al. [11]	61	English	Both	500	×	×
Bijlsma et.al. [17]	45	English	Reliability	71	×	×
Schmidt et. al. [18]	3	Danish	None	1621	×	×
Papp and Lovaas [19]	63	English	Both	31	×	×
Alzubaidi [22]	36	Arabic	Both	1230	×	×
Bitton et.al. [23]	46	English	None	162	×	×

their demographic, geographic, technographic, and other features? What are the respondent's primary languages?

The target respondents of the RSAM are users familiar with information technology or employees who use computers and the Internet at work. The primary language of the respondents is Persian, and they are located in Iran.

3) Collect information

To gather information to form the set of questionnaire items, there are several sources as follows:

- Existing related questionnaires
- Academic articles and books
- Expert interview
- Information and reports published by credible organizations and agencies
- Ransomware defense tips and guidelines

To develop RSAM, all the information sources mentioned above are explored. Based on our investigations, there does not exist any questionnaire for ransomware awareness evaluation. General security awareness questionnaires such as HAIS-Q can be applied to collect some items of the ransomware awareness questionnaire as well, however, it is also needed to incorporate specific questions to measure users' vulnerabilities regarding ransomware. Moreover, academic articles and books about ransomware prevention and protection (e.g. [24], [25], [26], [27], [28], [29], [30]) are reviewed. Five experts in the field of IT and e-commerce security are interviewed, and their knowledge about ransomware awareness is captured and documented. The specialties of the five chosen experts are intrusion detection systems, malware detection, electronic payment systems, network security, and software security. Two experts are assistant professors, two experts are CEOs of cybersecurity companies, and one expert is an e-commerce MSc student.

Other sources of information include CERT reports of several countries about ransomware (for instance Australia [1] , New Zealand [2] , United Kingdom [3] , and Singapore [4]) and AFTA guidelines for ransomware prevention and protection [5] . AFTA is Iran's strategic management of information security center organized by the presidential administration.

After collecting and categorization information related to ransomware awareness assessment, 10 categories, and 41 dimensions are defined as shown in Table2.

4) Select question types

Question types could be divided into two main types, namely, open-ended and close-ended questions. In open-ended questions, the respondents are free to answer questions and the answer is not limited. This type of question allows respondents to provide their explanations or point of view. In closed-ended questions, respondents can choose from predefined answers and they are not allowed to explain their selected answers. Some types of close-ended questions are: Yes/No, Rating, Multiple-choice, and Likert scales. Since, close-ended questions are easier and quicker to answer while helping in obtaining measurable and quantitative data, to develop the RSAM questionnaire, a 5-point Likert scale is employed.

[1] www.cyber.gov.au/ransomware
[2] www.cert.govt.nz/business/guides/protecting-from-ransomware
[3] www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
[4] www.csa.gov.sg/singcert/advisories/ad-2020-006
[5] www.afta.gov.ir/files/ransomware.pdf

5) Develop items
   When the information collected from sources is integrated and categorized, a list of items is generated based on collected dimensions to create a pool of questions. Next, some items are eliminated because they are related to the IT department and IT staff activities while the objective of the questionnaire is to measure the ransomware awareness of the employees and users.
6) Refine Items
   After collecting the items, the questions are developed and revised. This activity is iterative and performed multiple times for further improvements. The questions are reviewed and edited by 3 information security and 2 linguistic experts. To discover respondents who completed the questionnaire inattentively, some reverse score questions are incorporated into the questionnaire. After completion of this activity, a questionnaire containing 40 questions was provided.
7) Design sequences and layouts
   At this stage, the order of questions and questionnaire presentation is designed. Any skip rules (if respondents are allowed to skip questions) and whether questions are displayed one by one or entirely should be determined. Since some IT jargon (e.g., Patch, Crack, File extension, Macro, etc.) might be unknown to the respondents, it is essential to add some explanations to those RSAM questions containing such terms. We also incorporated some images to clarify the questions by displaying some examples, as shown in Figure 3.

B. Data collection

To ensure that the target respondents are familiar with information technology or use computers and the Internet at work, the target candidates have been chosen from university students and employees of IT-based companies located in Isfahan. Moreover, the following pre-screening questions were incorporated into the questionnaire as well as demographic questions. How much are you familiar with information technology? How often do you use computers and the Internet at work?

In the data collection activity, 348 Persian-language Iranian candidates were asked to complete the RSAM-P, and 216 candidates responded to the request (response rate = 0.62). Of the 216 participants, 97 (45%) were females, and 119 (55%) were males aged between 17 and 65. The educational level of the participants distributes as 9.5% (Secondary school), 51.8% (BSc), and 38.7% (M.Sc. or Ph.D.). We employed Google forms for creating and sharing the questionnaire.

C. Questionnaire validation

As shown in Figure 4, to evaluate RSAM, it is necessary to conduct reliability, and validity testing explained in the following sections in detail. Regarding the questionnaire development process depicted in Figure 1, if validation results don't demonstrate adequate reliability and validity, the data collection or the design phase might be run again.

Reliability evaluation deals with testing the results collected by an instrument in case of repeated trials to measure the stability and consistency of scores over time. Validity refers to how accurately an instrument assesses what it is supposed to measure [31]. Validity tests are categorized into two broad types, namely, theoretical and empirical validities. The former verifies the degree to which the instrument measures the construct of interest and how well the idea of a theoretical construct is represented in an instrument. The latter measures how meaningful the instrument is when it is in practical application. Face validity and content validity are two subtypes of theoretical validity type while criterion-related and construct validity belong to empirical validity [31].

In this study, Cronbach's Alpha coefficient was applied to evaluate the reliability of the questionnaire, and factor analysis was employed for validity evaluations of the RSAM.

1) Reliability evaluation
   To test the reliability of RSAM-P, Cronbach's Alpha coefficient was calculated to measure the discriminative power and internal consistency of the questionnaire. In this study, IBM SPSS statistical package 24.0 is applied for reliability testing. The Cronbach's alpha coefficient of the RSAM-P, including 40 items, is 0.857, which lies in the acceptable range for the alpha coefficient (i.e., higher than 0.7) [32]. The results of the reliability evaluation are displayed in Table3.
2) Validity evaluation
   Factor analysis is considered the most commonly used method for establishing construct validity measured by an instrument. In this study, EFA (Explanatory Factor Analysis) and CFA (Confirmatory Factor Analysis) methods are employed to validate the RSAM empirically. Before factor analysis, it is necessary to test the adequacy of the data for such a method. To determine the sampling adequacy for factor analysis, Bartlett's test and Kaiser-Meyer-Olkin (KMO) measures were applied. KMO assesses the appropriateness of applying factor analysis to the data set. Bartlett's test of sphericity examines the null hypothesis that the variables in the population correlation matrix are uncorrelated.

Table 2. Collected Information Related to Ransomware Awareness Assessment.

Category	Dimensions
Email usage	• Scanning received emails • Clicking on suspicious links in emails • Responding to the suspicious emails • Completing the forms received by emails • Running email attachments without verifying the sender
Internet and network usage	• Pop-up allowance • Following pop-ups • Downloading Internet files without validating the sources • Using add-ons and extensions of browsers • Checking the credibility and authenticity of the websites when sending sensitive data • Using public Wi-Fi networks
Password management	• Employing weak password • Using the same passwords for several systems • Password sharing • Writing passwords on paper or saving them in digital formats • Saving passwords in browsers
System security	• Disabling autoplay for external storage • Remote desktop usage • Turning off Bluetooth and wireless after finishing work • Enabling file Extension visibility and noticing the file extension when running files • Not logging in as admins when it is not necessary • Periodic backing up data applying online or external storage
Antivirus usage	• Installing and updating antivirus • Installing and updating anti-ransomware tools • Periodic antivirus scanning
Software usage	• Updating OS and software • Using SaaS instead of installing software • Using authorized and recommended software in the organization • Using cracked software • Patching software • Allowing and applying office macros
Incident reporting	• Reporting suspicious emails • Reporting suspicious events and incidents
Social media usage	• Social media usage during work time • Sharing sensitive data with social media
Physical security	• Shoulder surfing • Preventing removable disk connection • Preventing colleagues from using systems • Locking or logging out of the system when it is idle
Knowledge acquisition and attitude	• Following ransomware news, technical papers, and related reports • Believing that all systems are at risk of ransomware

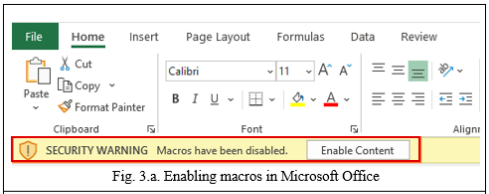

Fig. 3.a. Enabling macros in Microsoft Office

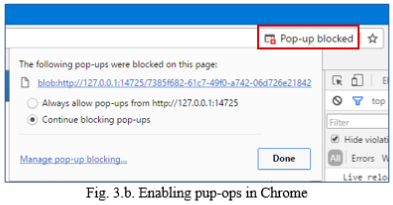

Fig. 3.b. Enabling pup-ops in Chrome

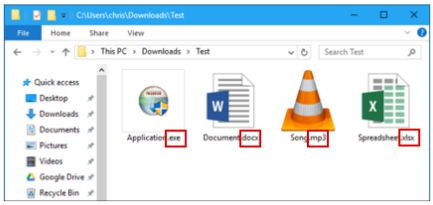

Fig. 3.c. File extentions in Windows 10 example

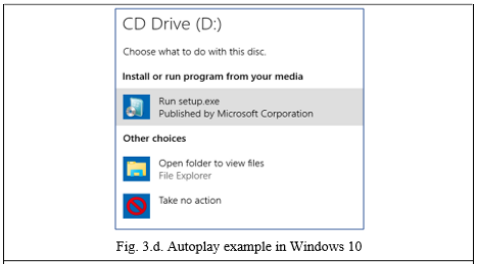

Fig. 3.d. Autoplay example in Windows 10

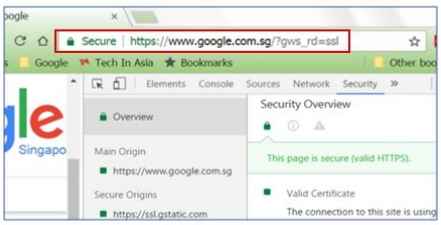

Fig. 3.e. Checking URL

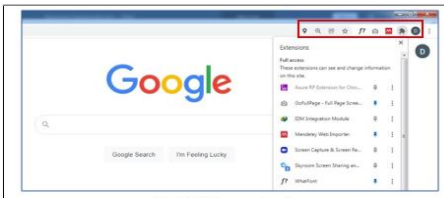

Fig. 3.f. Chrome extensions

Figure 3. Images Added to Questions for Clarification.

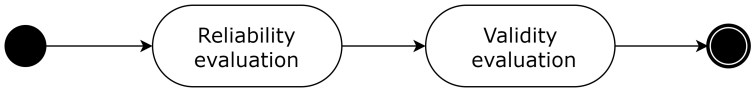

Figure 4. Questionnaire Validation Process.

Table 3. Cronbach's Alpha.

N of Valid Cases	N of Items	Cronbach's Alpha
216	40	.857

The KMO statistics range from 0 to 1, with values closer to 1 indicating greater adequacy of the factor analysis (KMO $\geq$ 0.6 indicates low adequacy, KMO $\geq$ 0.7 indicates medium adequacy, KMO $\geq$ 0.8 indicates high adequacy, KMO $\geq$ 0.9 indicates very high adequacy, and If KMO $<$ 0.5 or the result of Bartlett's test is greater than 0.05, factorial analysis cannot be applied).

As depicted in Table4, the value of the KMO measure is 0.768 reflecting the medium adequacy. Bartlett's test results denote that the chi-square value is 2808.248 with 780 degrees of freedom at a significance of 0.000, which is less than p $<$ 0.01. Based on the result, it is appropriate to proceed with factor analysis to examine the factors for the study.

a) Explanatory Factor Analysis (EFA)

EFA is an approach to data analysis proceeding in an exploratory manner to examine how and to what extent the variance of observed variables can be explained by their underlying latent variables.

Researchers apply EFA when the relationships between the observed and latent variables are unknown or uncertain. They often benefit from EFA to determine a small number of factors representing a relatively large number of observed variables [33].

In this study, IBM SPSS Statistics 24.0 has been employed to identify factors and loadings for EFA analysis. As displayed in Table 5, the total variance is explained by identifying twelve factors affecting the assessing user's awareness of ransomware. These factors were extracted for the study because their eigenvalues were greater than "1". The twelve extracted factors were able to explain 63.733 percent of the variance.

In this study, factor extraction is conducted by applying PCA. A scree plot shows the eigenvalues of the

Table 4. KMO and Bartlett's test.

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		**.768**
Bartlett's Test of Sphericity	Approx. Chi-Square	2808.248
	df	780
	Sig.	.000

Table 5. The Total Cumulative Variance.

Component	**Initial Eigenvalues**			**Extraction Sums of Squared Loadings**			**Rotation Sums of Squared Loadings**		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6.639	16.597	16.597	6.639	16.597	16.597	2.699	6.748	6.748
2	3.250	8.124	24.720	3.250	8.124	24.720	2.649	6.623	13.372
3	2.776	6.939	31.659	2.776	6.939	31.659	2.478	6.196	19.568
4	2.295	5.738	37.397	2.295	5.738	37.397	2.415	6.038	25.605
5	1.761	4.402	41.799	1.761	4.402	41.799	2.355	5.889	31.494
6	1.543	3.857	45.656	1.543	3.857	45.656	2.142	5.354	36.848
7	1.426	3.565	49.222	1.426	3.565	49.222	2.140	5.349	42.197
8	1.283	3.209	52.430	1.283	3.209	52.430	2.013	5.031	47.228
9	1.214	3.035	55.465	1.214	3.035	55.465	2.006	5.015	52.243
10	1.133	2.832	58.297	1.133	2.832	58.297	1.904	4.761	57.004
11	1.089	2.723	61.020	1.089	2.723	61.020	1.543	3.857	60.862
12	1.085	2.713	63.733	1.085	2.713	63.733	1.149	2.871	63.733
13	.966	2.415	66.148						
14	.896	2.239	68.387						
15	.857	2.142	70.529						
Extraction Method: Principal Component Analysis.									

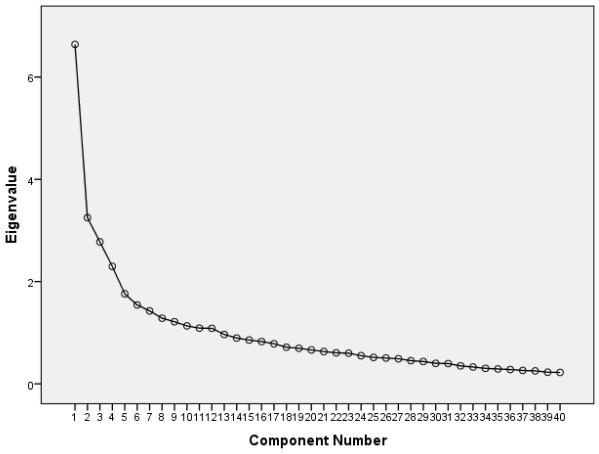

Figure 5. Scree Plot.

factors or components, ordered from the first (largest) to the last (smallest). The scree plot in Figure 5 displays the number of factors extracted based on eigenvalue > 1. This figure is reinforced by the result of factor extraction based on the eigenvalue represented in Table5, indicating twelve factors have been extracted from this analysis.

The rotated component matrix is displayed in Tables 6 and 7, and item factoring based on EFA is demonstrated in Tables 6 and 7. Item Q32 does not correlate with the other items, so it should be eliminated consequently, 11 factors remained.

b) Confirmatory Factor Analysis (CFA)

CFA is a confirmatory method typically used to test a theory. This implies that the analyst should have some knowledge or hypothesis about the potential relationships among variables before performing CFA. The purpose of CFA is to examine the hypothesized relationships between the latent factors and observed variables [26].

We employed IBM SPSS Amos 24.0 to run CFA for validating RSAM-P. To examine the goodness-of-fit of

Table 6. Rotated Component Matrix.

	Component											
	1	2	3	4	5	6	7	8	9	10	11	12
Q1	.174	-.197	.226	.039	-.113	.021	-.010	.607	.274	.020	.043	.196
Q2	.074	.106	.081	.678	.024	.107	.171	.118	.198	-.068	.029	.215
Q3	-.060	.391	.037	.641	.154	-.045	-.042	-.228	.157	-.009	-.016	-.055
Q4	.018	.354	.141	.534	.130	.167	-.105	-.193	.177	.119	-.055	-.297
Q5	.044	.509	-.037	.481	.060	.196	-.075	-.253	.282	-.019	.131	.087
Q6	-.020	.139	.014	-.158	.172	.108	.049	.699	.101	.277	-.096	-.001
Q7	.216	-.159	-.006	.087	-.095	.089	-.012	.716	.013	.032	.038	-.058
Q8	.141	-.058	-.063	.125	.636	-.058	.118	-.349	.035	.181	-.085	.207
Q9	-.127	.220	-.012	.177	.094	.018	.191	.082	.587	-.152	.123	.108
Q10	.256	-.011	.076	.175	.105	.159	.102	.108	.654	.015	.006	.014
Q11	.275	.044	.123	.006	.070	.235	.096	.083	.681	-.087	-.028	-.286
Q12	.028	.047	.091	-.067	-.137	-.031	-.014	.109	-.093	.709	.038	-.023
Q13	.165	-.101	.131	.493	-.140	.022	.073	.241	.022	.465	.174	-.049
Q14	.045	.002	-.074	-.010	.650	-.126	.115	-.023	.161	-.269	.081	-.035
Q15	.026	.211	-.023	.077	.763	-.053	.012	.065	.087	-.027	.119	-.079
Q16	.028	.156	-.024	.218	-.340	.154	.132	.094	-.099	.455	.138	.258
Q17	.071	.124	.078	.042	.536	.299	-.158	.182	-.094	-.241	.381	-.037
Q18	.697	.001	.062	.092	.291	.087	.027	.152	.041	-.009	-.021	.112

the model with the given samples, CFI (Comparative Fit Index), TLI (Tucker-Lewis Index), NFI (Normed Fit Index), and RMSEA (Root Mean Square Error of Approximation) were employed.

The results of CFA indicate an insufficient fit of the model to the data (CFI = 0.574, TLI = 0.690, NFI = 0.729, and RMSEA = 0.064). Consequently, the model was fitted to data weakly, and model adjustment is required. To modify the model, the areas of the misfit should be detected regarding diagnostic information provided by Amos. To refine the model, the paths with factor load below the acceptable threshold are removed by applying the model-trimming method. Next, associated relationships are added to the model to improve model fit according to the model-building method [34]. After model adjustment 21 questions remained. The final results of the model adjustment are summarized in Table9 and Figure 6.

In Figure 6, the nine-factor CFA model after a model adjustment has been displayed. Factor loading, factor correlation, correlated errors, and error variance have been also shown in Fig 6. Items yielded a factor loading less than 0.4, have been excluded and 21 questions remained.

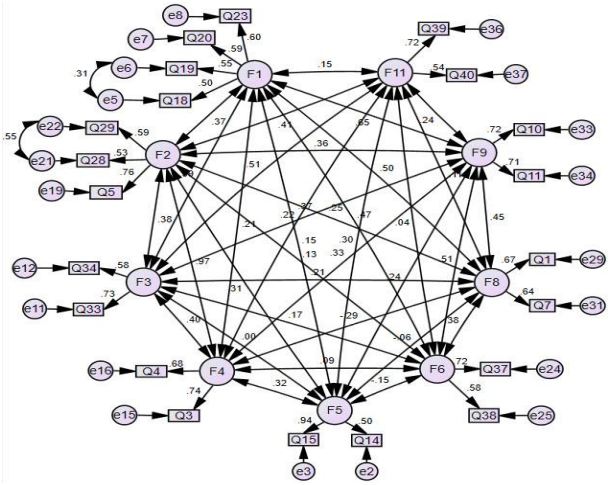

Figure 6. Graphical nine-factor CFA model after model adjustment.

The CFI, TLI, and NFI values should be equal to or above 0.90 to indicate a satisfactory model fit, and RMSEA < 0.11 indicates a reasonable fit [34]. Hence, as shown in Table8, the model adjustment has resulted in a sufficient fit of the model to the data.

Table 7. Rotated Component Matrix (Cont.).

	Component											
	1	2	3	4	5	6	7	8	9	10	11	12
Q19	.792	-.055	.030	-.044	-.011	.062	.093	.063	.251	-.009	.053	.015
Q20	.553	.389	.097	.106	-.087	.164	.094	.101	.039	.143	.003	-.119
Q21	.348	.457	.007	.104	.229	.186	.183	.179	-.064	.224	.102	-.204
Q22	.371	.114	.159	.480	.056	.017	.241	.202	-.277	-.075	.122	-.151
Q23	.390	.140	.344	.095	-.013	.264	.310	.184	-.059	-.262	-.151	-.122
Q24	.363	.122	.139	.187	.153	.103	.572	.013	.039	.209	.014	-.034
Q25	.111	.106	.125	-.005	.034	.055	.726	-.025	.107	-.096	.013	.203
Q26	-.026	.032	.043	.040	-.006	-.152	.751	.024	.124	.041	.164	-.130
Q27	.088	.081	-.058	.271	.123	.249	-.236	.132	.361	.314	.023	.098
Q28	.091	.767	.119	.107	.082	-.091	.105	-.068	.087	.032	.027	.104
Q29	-.015	.794	.230	.173	.032	-.066	.099	-.068	.006	.012	.074	.003
Q30	-.075	.038	.722	.105	.030	-.004	.124	.065	.033	.005	.089	-.004
Q31	-.078	.051	.534	-.046	.181	-.029	.375	.012	-.081	.343	-.229	.118
Q32	.166	.217	.474	.123	-.035	.217	.168	.066	-.041	.117	.086	.489
Q33	.180	.060	.511	.306	-.075	.019	.141	-.037	.121	.105	.185	-.353
Q34	.211	.197	.734	-.019	-.136	.020	-.047	.057	.063	.005	.085	.024
Q35	.342	.042	-.083	.189	.002	.571	-.141	-.024	.069	.098	-.064	.157
Q36	.400	.247	.410	.000	-.276	-.176	-.052	-.031	.190	.150	.121	.260
Q37	.101	.043	.063	-.051	-.153	.771	.059	.056	.157	-.154	.035	.097
Q38	-.020	-.149	.027	.100	.005	.731	-.009	.147	.144	.165	-.034	-.169
Q39	-.022	.192	.230	-.077	.101	.142	.070	-.008	.128	.401	.603	-.200
Q40	.035	.039	.082	.125	.133	-.123	.139	-.020	.023	.020	.831	.111
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.												
a. Rotation converged in 21 iterations.												

D. Translation and cultural adaptation

If one questionnaire is applied as a self-report measure for a new population having a different language and culture, it is essential to translate the questionnaire and perform cultural adaptations. A poor translation may bring about an instrument that is not equivalent to the original questionnaire. To translate and cultural adaptation to create an English version of the RSAM, we apply the process described in [35] (See Figure 7). The activities of the translation and cultural adaptation process are elaborated in the following sections.

1) Translation

The first step is the forward translation of the questionnaire to the target language. It is recommended that at least two forward translations be done by two bilingual translators whose mother language is the target language. This makes it possible to compare the translations and find inconsistencies to improve the translation. One translator should be aware of the questionnaire objective and the ransomware-related concepts, while the other translator is naïve to the ransomware domain and they don't have any background knowledge about ransomware.

2) Synthesis

In this stage, two translators synthesize their translations of the RSAM-P to form a questionnaire that both of them are confirmed. They discuss translations and remove any discrepancies and resolve issues.

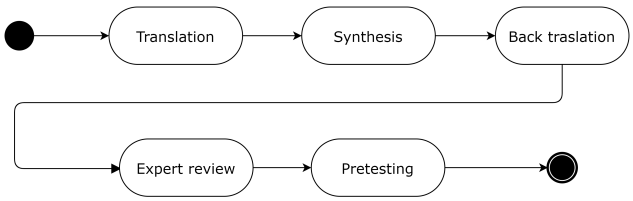

Figure 7. Questionnaire translation and cultural adaptation process.

Table 8. Item Factoring Based EFA.

Factors	Questions
1	Q18, Q19, Q20, Q23
2	Q5, Q21, Q28, Q29
3	Q30, Q31, Q33, Q34, Q36
4	Q2, Q3, Q4, Q13, Q22
5	Q8, Q14, Q15, Q17
6	Q35, Q37, Q38
7	Q24, Q25, Q26
8	Q1, Q6, Q7
9	Q9, Q10, Q11, Q27
10	Q12, Q16
11	Q39, Q40
12	Q32

Table 9. Goodness-of-fit statistics for the nine-factor CFA model.

Model tested	X_2	Df	CFI	TLI	NFI	RMSEA
Model performance	249.222	151	0.924	0.912	0.900	0.055
Criterion for goodness of fit	-	-	≥ 0.9	≥ 0.9	≥ 0.9	≥ 0.1

3) Back translation

The consentaneous translated questionnaire from the previous stage is back-translated by two translators into Persian. At this stage, both translators should neither be aware nor be informed of the questionnaire objective and ransomware awareness concepts.

4) Expert review

At this step, a committee of ransomware and security awareness experts evaluates the translation and cross-cultural equivalence of the questionnaires. The committee should review 5 translations (two forward translations, one synthesized translation, and two back translations) deeply. Semantic, idiomatic, experiential, and conceptual equivalences of translations are examined by experts to discover any discrepancies. If necessary, the translation and back-translation processes should be repeated to clarify how another wording of an item would work. After all editions, improvements, and the consensus of the experts, RSAM-E is generated.

5) Pretesting

After the preparation of the RSAM-E, the final stage is pretesting the questionnaire. 25 participants were asked to complete the RSAM-E while they were monitored and interviewed to probe their understanding/issues and check the meaning of questions. This activity ensures that RSAM-E is equivalent to RSAM-P. If pretesting stage reports critical issues, the expert review stage should be started again.

4 Disscussion

In this research, RSAM-P was validated and verified, then translated and adapted to the English version. After testing and validation of RSAM-P, 19 questions were eliminated. So, compared with HAIS-Q, RSAM consists of 21 questions while HAIS-Q includes 63 questions. The final RSAM-E questionnaires have been presented in Appendix 6 and, RSAME-P is accessible via the following link.

https://cloud.ui.ac.ir/index.php/s/ETPZDpjfDyaMMY2

While focus areas of other security awareness questionnaires e.g. HASIS-Q [15] have been determined by experts, RSAM constructs have been extracted using the EFA method. In comparison with the other general security awareness questionnaire, RSAM incorporates six specially designed items (i.e. questions 13, 14, 16, 19, 20, and 21) for measuring ransomware awareness. The remained questions could be considered as items for general security awareness measurement. Although these questions are somewhat similar to other questionnaires conceptually, the questions are not the same. Compared to HASIS-Q, RSAM incorporates 8 similar items (i.e. questions 1-6, 8, and 18), and some focus areas of RSAM are not supported by HASIS-Q including Pop-ups, Antiviruses, System security, and Preventive actions. Furthermore, to our best knowledge, there is no validated security awareness questionnaire in Persian.

We designed and validated RSAM because today ransomware becomes one of the most dangerous cyber threats in the world. However, perhaps some organizations might not need a special questionnaire to assess ransomware awareness. On the other hand, RSAM could be applied by those companies that emphasize ransomware prevention.

5 Conclusions and Future work

In this paper, a questionnaire for measuring users' ransomware awareness was presented in Persian and English versions consisting of 21 questions. We also proposed a novel questionnaire

development process for researchers to design, develop and validate new questionnaires. The proposed questionnaire development process can be exploited to produce new instruments in security and other domains.

Since RSAM-E has been developed using translation and cultural adaptation processes, further investigation is needed to test the validity and reliability of the RSAM-E through a sample of participants and statistical testing. Moreover, other versions of RSAM in various languages could be generated by translating, adapting, and testing RSAM-P in future work.

We added some explanations and examples to the RSAM to guide and inform those users who are not familiar with technical security and IT terms. However, more visualization techniques and explanations could be employed to ensure users understand and comprehend questions correctly.

The problems with questionnaire-based assessment are user frustrations and low response rates. To engage users to complete the questionnaire and increase response rates, gamification techniques, and serious games could be employed. In future work, we will develop a serious game based on RSAM-P to assess ransomware awareness of the users indirectly, which results in better and more effective measurement. A serious game as an instrument also enhances user engagement and satisfaction.

Last but not least future work is to design and develop methods to monitor and assess the actual behavior of the users to discover their vulnerability and level of awareness about ransomware.

6 Appendix: RSAM-E Questionnaire

References

[1] S. M. Kerner. Ransomware trends, statistics and facts in 2021. `https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts`, Date Accessed: 2021.

[2] D. Braue. Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. `https://cybersecurityventures.com/global-ransomware-damage-costs-predicted%20to-reach-250-billion-usd-by-2031/`, Date Accessed: 2021.

[3] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan. Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, 111:102490, 2021. doi:10.1016/j.cose.2021.102490.

[4] T. McIntosh, A. Kayes, Y. Chen, A. Ng, and P. Watters. Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions. *ACM Computing Surveys (CSUR)*, 54(9):1–36, 2021. doi:10.1145/3479393.

[5] K. Khando, S. Gao, S. M. Islam, and A. Salman. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security*, 106:102267, 2021. doi:10.1016/j.cose.2021.102267.

[6] M. Chung. Why employees matter in the fight against ransomware. *Computers & security*, 2019(8), 2021. ISSN 1361-3723. doi:10.1016/S1361-3723(19)30084-3.

[7] J. Thomas. Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. *Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business Management*, 12(3): 1–23, 2018. doi:10.5539/ijbm.v13n6p1.

[8] Ransomware protection: how to keep your data safe in 2021. `https://usa.kaspersky.com/resource-center/threats/how-to-prevent-ransomware`, Date Accessed: 12-Dec-2021.

[9] Information Security User Awareness Assessment. `Available:https://louisville.edu/security/files/user-awareness-questionnaire-pdf`, Date Accessed: 12-Oct-2021.

[10] J. Hammarstrand and T. Fu. Information security awareness and behaviour: of trained and untrained home users in sweden., 2015.

[11] J. Thomas. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business Management*, 12(3):1–23, 2018. doi:10.5539/ijbm.v13n6p1.

[12] A. McCormac, D. Calic, M. Butavicius, K. Parsons, T. Zwaans, and M. Pattinson. A Reliable Measure of Information Security Awareness and the Identification of Bias in Responses. *Australasian Journal of Information Systems*, 21, 2017. doi:10.3127/ajis.v21i0.1697.

[13] T. Alharbi and A. Tassaddiq. Assessment of Cybersecurity Awareness among Students of Majmaah University. *Big Data and Cognitive Computing*, 5(2), 2021. doi:10.3390/bdcc5020023.

[14] A. Kusumawati. Information Security Awareness: Study on a Government Agency. In *2018 International Conference on Sustainable Information Engineering and Technology (SIET)*, pages 224–229. IEEE, 2018. doi:10.1109/SIET.2018.8693168.

[15] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66(2):40–51, 2017. doi:10.1016/j.cose.2017.01.004.

[16] K. M. Parsons, E. Young, M. A. Butavicius, A. McCormac, M. R. Pattinson, and C. Jerram. The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, 9(2):117–129, 2015. doi:10.1016/j.cose.2017.01.004.

[17] A. Bijlsma and L. W. Rutledge. Information Security Awareness of bank employees: how differences between headquarter and branch employees affect ISA program design. *Open Universiteit*, 2020.

[18] Thomas Schmidt, Christian Nøhr, and Ross Koppel. A simple assessment of information security awareness in hospital staff across five danish regions. In *Public Health and Informatics*, pages 635–639. IOS Press, 2021. doi:10.3233/SHTI210248.

[19] G. Papp and P. Lovaas. Assessing Small Institutions' Cyber Security Awareness Using Human Aspects of Information Security Questionnaire (HAIS-Q). In *Intelligent Computing: Proceedings of the 2021 Computing Conference, Volume 3*, pages 933–948. Springer, 2021. ISBN 978-3-030-80128-1. doi:10.1007/978-3-030-80129-8_62.

[20] MD Gaithersburg. Security and Privacy Controls for Information Systems and Organizations. , Date Accessed: Sep. 2020.

[21] Federal Financial Institutions Examination Council. FFIEC Cybersecurity Assessment Tool. *Fed. Financ. Institutions Exam. Counc*, 3506(1557):1–59, 2015.

[22] A. Alzubaidi. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, 7(1):e06016, 2021. doi:10.1016/j.heliyon.2021.e06016.

Table 10. RSAM-E Questionnaire.

Category	Items
Email usage	1) When I open links received by email, I don't care whether the sender is known or unknown to me. Strongly agree (1) Agree (2) Neutral (3) Disagree (4) Strongly disagree (5) 2) If I receive an email requesting to enter my username and password to prevent deactivation or account blocking, I should do it or contact the sender. Strongly agree (1) Agree (2) Neutral (3) Disagree (4) Strongly disagree (5) 3) If I receive an unknown email requesting to register in the lottery, I open the received links and enter my information. Strongly agree (1) Agree (2) Neutral (3) Disagree (4) Strongly disagree (5)
Password management	1) I prefer to use a memorable password even if it is not a strong password. Strongly agree (1) Agree (2) Neutral (3) Disagree (4) Strongly disagree (5) 2) I prefer to use the same password for several systems. Strongly agree (1) Agree (2) Neutral (3) Disagree (4) Strongly disagree (5) 3) It is likely to share my password with someone else if it is needed. Strongly agree (1) Agree (2) Neutral (3) Disagree (4) Strongly disagree (5) 4) I save my username and password in browsers. Always (1) Frequently (2) Sometimes (3) Seldom (4) Never (5)
Software download	1) If I need a particular file urgently, I download it from any source regardless of source credibility. Always (1) Frequently (2) Sometimes (3) Seldom (4) Never (5) 2) I download a cracked version of the required software to access it for free. Always (1) Frequently (2) Sometimes (3) Seldom (4) Never (5)
Pop-up	1) I allow pop-ups in the browsers. Always (1) Frequently (2) Sometimes (3) Seldom (4) Never (5) 2) If I allow pop-ups, I will click and follow them. Always (1) Frequently (2) Sometimes (3) Seldom (4) Never (5)
Antivirus	1) I scan email attachments with an antivirus before opening them. Always (1) Frequently (2) Sometimes (3) Seldom (4) Never (5) 2) If the system is equipped with antivirus, there is no need to install and update anti-ransomware tools. Strongly agree (1) Agree (2) Neutral (3) Disagree (4) Strongly disagree (5)

Table 11. RSAM-E Questionnaire (Cont.).

Category	Items
System security	1) I allow connecting to my system with a remote desktop if needed. Strongly agree (1) Agree (2) Neutral (3) Disagree (4) Strongly disagree (5) 2) When I connect external storage to my system, I allow autoplay. Always (1) Frequently (2) Sometimes (3) Seldom (4) Never (5)
Preventive actions	1) I periodically back up my data on online or external storage. Always (1) Frequently (2) Sometimes (3) Seldom (4) Never (5) 2) I turn off Bluetooth and wireless when I don't use them. Always (1) Frequently (2) Sometimes (3) Seldom (4) Never (5)
User activeness	1) I should report any suspicious events and incidents. Strongly agree (1) Agree (2) Neutral (3) Disagree (4) Strongly disagree (5) 2) I follow ransomware news, technical papers, and related reports to improve my awareness of ransomware. Always (1) Frequently (2) Sometimes (3) Seldom (4) Never (5)
Attitude	1) Installing and updating antivirus is not effective for ransomware defense. Strongly agree (1) Agree (2) Neutral (3) Disagree (4) Strongly disagree (5) 2) Only systems containing sensitive and valuable data are the target of ransomware attacks. Strongly agree (1) Agree (2) Neutral (3) Disagree (4) Strongly disagree (5)

[23] R. Bitton, K. Boymgold, R. Puzis, and A. Shabtai. Evaluating the Information Security Awareness of Smartphone Users. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, page 1–13. Springer, 2020. doi:10.1145/3313831.3376385.

[24] L. C. Miller. *Ransomware Defense For Dummiess*. 1st ed. For Dummies, 2020.

[25] N. A. Hassan. *Ransomware Revealed: A Beginner's Guide to Protecting and Recovering from Ransomware Attacks*. Apress, 2019.

[26] R. A. Grimes. *Ransomware Protection Playbook*. Wiley, 2021.

[27] N. A. Hassan. Enterprise Defense Strategies Against Ransomware Attacks. *Ransomware Revealed: A Beginner's Guide to Protecting and Recovering from Ransomware Attacks*, page 115–154, 2019. ISSN 978-1-4842-4254-4. doi:10.1007/978-1-4842-4255-1_5.

[28] Z. Manjezi and R. A. Botha. Preventing and Mitigating Ransomware. *Information Security*, page 149–162, 2017.

[29] I. A. Chesti, M. Humayun, N. U. Sama, and N. Jhanjhi. Evolution, Mitigation, and Prevention of Ransomware. In *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, pages 1–6. IEEE, 2020. ISBN 978-1-7281-5468-8. doi:10.1109/ICCIS49240.2020.9257708.

[30] J. Jansen van Vuuren, L. Leenen, and Jansen A. van Vuuren. Don't be Caught Unaware: A Ransomware Primer with a Specific Focus on Africa. In *Human Choice and Digital by Default: Autonomy vs Digital Determination: 15th IFIP International Conference on Human Choice and Computers, HCC 2022, Tokyo, Japan, September 8–9, 2022, Proceedings*, pages 115–131. Springer, 2022. ISBN 978-3-031-15687-8. doi:10.1007/978-3-031-15688-5_11.

[31] O. A. Bolarinwa. Principles and methods of validity and reliability testing of questionnaires used in social and health science researches. *Nigerian Postgraduate Medical Journal*, 22(4):195–201, 2015. doi:https://www.npmj.org/text.asp?2015/22/4/195/173959.

[32] J. M. Cortina. What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology*, 78(1):98–104, 1993. doi:10.1037/0021-9010.78.1.98.

[33] D. T. Shek and L. Yu. Use of structural equation modeling in human development research. *International Journal on Disability and Human Development*, 13(2):157–167, 2014. doi:10.1515/ijdhd-2014-0302.

[34] D. T. Shek and L. Yu. Confirmatory factor analysis using AMOS: a demonstration. *International Journal on Disability and Human Development*, 13(2):191–204, 2014. doi:10.1515/ijdhd-2014-0305.

[35] D. E. Beaton, C. Bombardier, F. Guillemin, and M. B. Ferraz. Guidelines for the process of cross-cultural adaptation of self-report measures. *Spine*, 25(24):3186–3191, 2000.

Fakhroddin Noorbehbahani is an assistant professor of computer engineering at the University of Isfahan. He received his B.Sc. and M.Sc. in computer and IT engineering from the Isfahan University of Technology and Amirkabir University of Technology, Iran, in 2007 and 2010, respectively. He obtained his Ph.D. degree in computer engineering from Isfahan University of Technology, Iran, in 2016. His research interests include Human-Computer Interaction, E-business, Machine Learning, and Data Science.

Anahita Taghiyar studied IT Engineering and received her M.Sc. from Sheikh Baha'i University, Isfahan, Iran, in 2021. Her current research interests include Data mining and Information Security.

Azadeh Rezvani studied IT Engineering and received her M.Sc. from Sheikh Baha'i University, Isfahan, Iran, in 2021. Her current research interests include E-commerce and Information Security.