



A Study of Cyber Security Knowledge and Practices among B.Ed. College Trainees of Gujarat

Research Scholar: Parmar Krunalkumar Gijubhai

Guide: Dr. Kamini Patel

Monark University

Abstract

Teachers are role models and gatekeepers of safe technology use, yet little is known about how well prospective teachers protect themselves online. This descriptive survey study examines cyber security knowledge and practices of B.Ed. college trainees in Gujarat and tests whether these vary by gender and academic stream and whether knowledge is related to practice. A knowledge test (25 items) and a practice scale (20 items, five-point) were administered to 200 trainees. Trainees obtained a mean knowledge score of 14.71 out of 25 ($SD = 3.23$); 130 trainees (65.0%) had moderate knowledge, 49 (24.5%) low and 21 (10.5%) high knowledge. The mean practice score was 3.11 out of 5 ($SD = 0.46$). Knowledge did not differ by gender, but differed significantly by stream, with science graduates scoring above arts graduates. Knowledge was positively and significantly correlated with practice ($r = 0.49$). Weak spots were data backup, two-factor authentication, public Wi-Fi use and awareness of cyber-law provisions. The paper recommends embedding cyber safety in the B.Ed. curriculum.

Keywords: cyber security awareness, digital safety, B.Ed. trainees, teacher education, knowledge and practice, Gujarat

1. Introduction

Teaching, assessment, administration and communication in schools now run on mobile phones, learning platforms and cloud storage. Teachers hold student records, share study material and increasingly guide children on safe online behaviour. A teacher who is careless about passwords, phishing messages or privacy settings exposes not only personal data but also the learners in their care. Cyber security competence is therefore part of the professional competence of a teacher, in the same way that subject knowledge and classroom management are.



Policy documents point in the same direction. India's Information Technology Act (2000) defines offences such as identity theft and cheating by impersonation using computer resources, and the National Education Policy 2020 stresses technology integration and digital literacy in education. Teacher education programmes carry the responsibility of preparing future teachers for this environment. Yet awareness of threats such as phishing and fraud in online payments does not automatically translate into safe behaviour. The human factor is widely recognised as the weakest link in information security (Furnell & Clarke, 2012).

B.Ed. trainees are an important group to study. They are young adults who are heavy users of digital services, they come from varied academic backgrounds (arts, science, commerce), and within a short time they will teach adolescents. This study therefore examines the cyber security knowledge and practices of B.Ed. college trainees of Gujarat.

1.1 Statement of the problem

Although B.Ed. trainees are future teachers and heavy digital users, there is little systematic evidence on what they know about cyber threats, how they behave online, and whether knowledge actually translates into safe practice. The study is titled: *A Study of Cyber Security Knowledge and Practices among B.Ed. College Trainees of Gujarat*.

1.2 Objectives

1. To assess the level of cyber security knowledge of B.Ed. trainees.
2. To study the cyber security practices followed by B.Ed. trainees.
3. To compare the knowledge and practices of male and female trainees.
4. To compare the knowledge of trainees from different academic streams.
5. To examine the relationship between cyber security knowledge and practices.

1.3 Hypotheses

- **H₀₁:** There is no significant difference between male and female trainees in cyber security knowledge.
- **H₀₂:** There is no significant difference in cyber security knowledge among trainees of different academic streams.



- **H₀3:** There is no significant relationship between cyber security knowledge and cyber security practices.
- **H₀4:** There is no significant difference between male and female trainees in cyber security practices.

1.4 Delimitations

The study is limited to B.Ed. trainees of selected colleges in Gujarat, to the self-reported practices of trainees, and to personal cyber security (accounts, devices, online behaviour) rather than institutional network security.

2. Review of Related Literature and Theoretical Framework

Research on information security awareness commonly uses a knowledge–attitude–behaviour structure. Kruger and Kearney (2006) proposed a prototype for assessing awareness along these three dimensions, and the Human Aspects of Information Security Questionnaire (HAIS-Q) of Parsons et al. (2014) measures knowledge, attitude and self-reported behaviour across focus areas such as password management, email use, internet use, social media use, mobile devices and information handling. The present study adopts the same logic, measuring knowledge with a test and practices with a frequency scale.

Three theories explain why knowing about threats may or may not lead to safe behaviour. Protection Motivation Theory (Rogers, 1975) holds that protective behaviour depends on perceived severity of and vulnerability to a threat and on confidence in the recommended response. The Health Belief Model has been applied to computer security behaviour by Ng, Kankanhalli and Xu (2009), who found that perceived susceptibility, perceived benefits and self-efficacy are associated with security behaviour. The Theory of Planned Behaviour (Ajzen, 1991) links behaviour to attitudes, social norms and perceived control. Taken together, they imply that knowledge is necessary but not sufficient, and that attitude and confidence mediate its effect on practice.

For teachers there is an added dimension: the Technological Pedagogical Content Knowledge framework (Mishra & Koehler, 2006) treats technology competence as part of professional



knowledge, and safe use of technology belongs within that competence. Figure 1 shows the conceptual framework that guides this study.

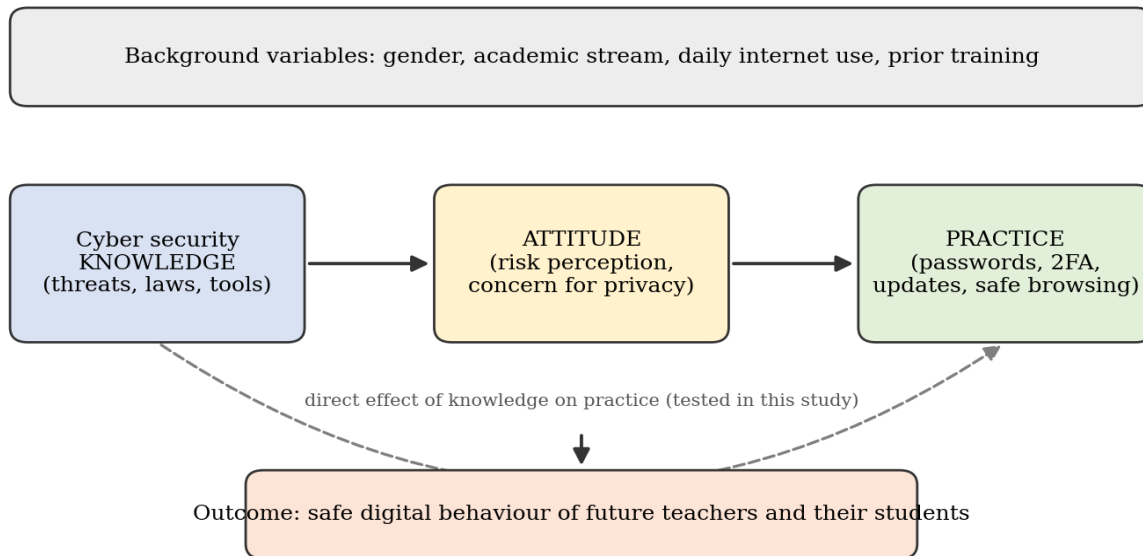


Figure 1. Conceptual framework: knowledge, attitude and practice

3. Methodology

3.1 Design, population and sample

A descriptive survey design (Creswell, 2014) was used. The population comprises B.Ed. trainees of colleges in Gujarat. A sample of 200 trainees was selected from B.Ed. colleges by stratified random sampling on gender and academic stream. Table 1 shows the profile of the sample.

Table 1. Profile of the sample

Variable	Category	n (%)
Gender	Female	124 (62.0%)
	Male	76 (38.0%)
Academic stream	Arts	82 (41.0%)
	Science	70 (35.0%)



Variable	Category	n (%)
	Commerce / other	48 (24.0%)
Daily internet use	Mean (SD), hours	3.25 (1.64)
Total		200

3.2 Tools

Two researcher-made tools were used (structure in Appendix A). The **Cyber Security Knowledge Test** has 25 multiple-choice items, scored 1 for a correct and 0 for an incorrect answer (range 0–25), covering threats, safe online behaviour, tools and basic cyber-law awareness. The **Cyber Security Practice Scale** has 20 statements rated on a five-point frequency scale (1 = never to 5 = always), covering password management, device security, safe browsing and privacy, with higher scores indicating safer practice. Content validity is established through review by subject experts, and reliability is established through a pilot study with Cronbach's alpha (Cronbach, 1951), with a coefficient of .70 or above taken as acceptable.

3.3 Data collection and analysis

The tools were administered in college during the academic session after obtaining permission and informed consent, with anonymity assured. The data were analysed with descriptive statistics (mean, SD, percentages), the independent-samples t-test, one-way analysis of variance with Bonferroni-adjusted pairwise comparisons, and Pearson's correlation, at the .05 level of significance. Effect sizes were reported as Cohen's d and eta-squared (Cohen, 1988).

4. Results and Interpretation

4.1 Level of cyber security knowledge (Objective 1)

The mean knowledge score of the 200 trainees was 14.71 out of 25 (58.8%; SD = 3.23). Taking scores below 50% as low, 50–74% as moderate and 75% or above as high, 65.0% of trainees had moderate knowledge, 24.5% low knowledge and only 10.5% high knowledge (Figure 2).

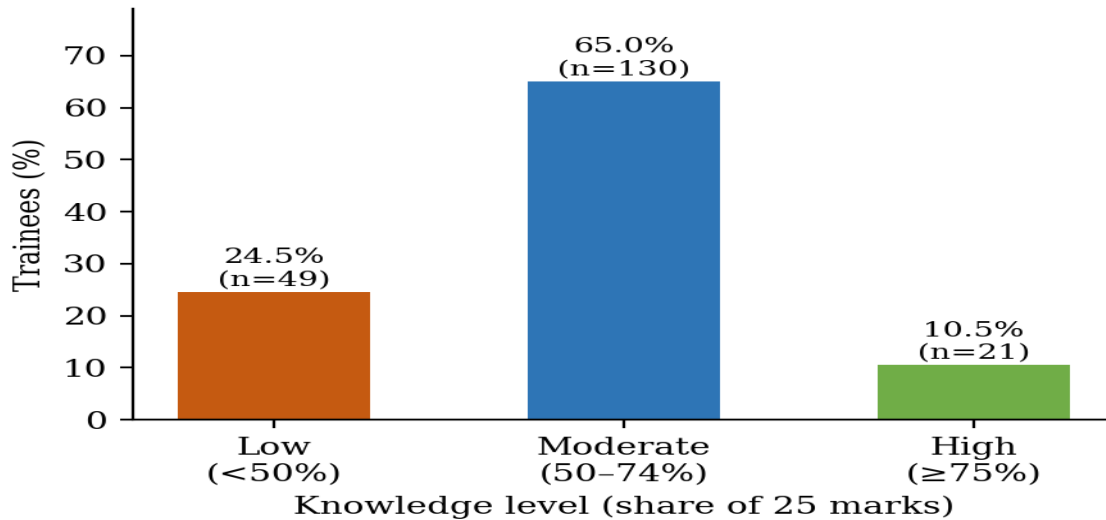


Figure 2. Distribution of trainees by knowledge level

Awareness varied by topic (Figure 3). Most trainees correctly identified cyberbullying, phishing and online payment fraud. Fewer answered correctly on ransomware and only a minority on cyber-law provisions, which suggests that familiar, everyday threats are better understood than technical and legal aspects.

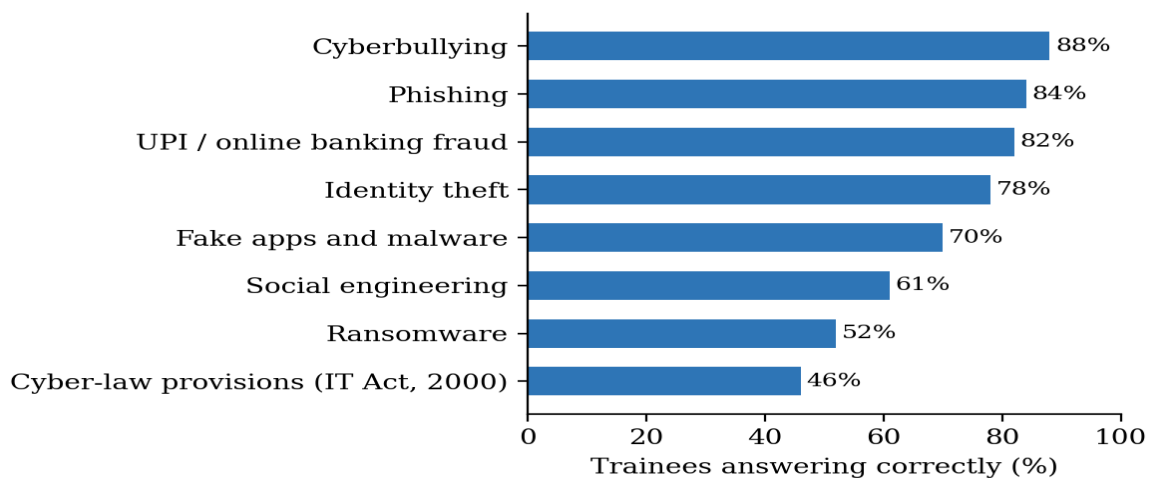


Figure 3. Awareness of cyber threats and cyber law



4.2 Cyber security practices (Objective 2)

The mean practice score was 3.11 out of 5 (SD = 0.46), indicating that trainees follow the recommended practices “sometimes” on average. Figure 4 shows the practices item by item. Checking links before clicking and using a security app were the most frequent, whereas data backup and avoiding public Wi-Fi for banking were the least frequent. Only 48% always or often used two-factor authentication.

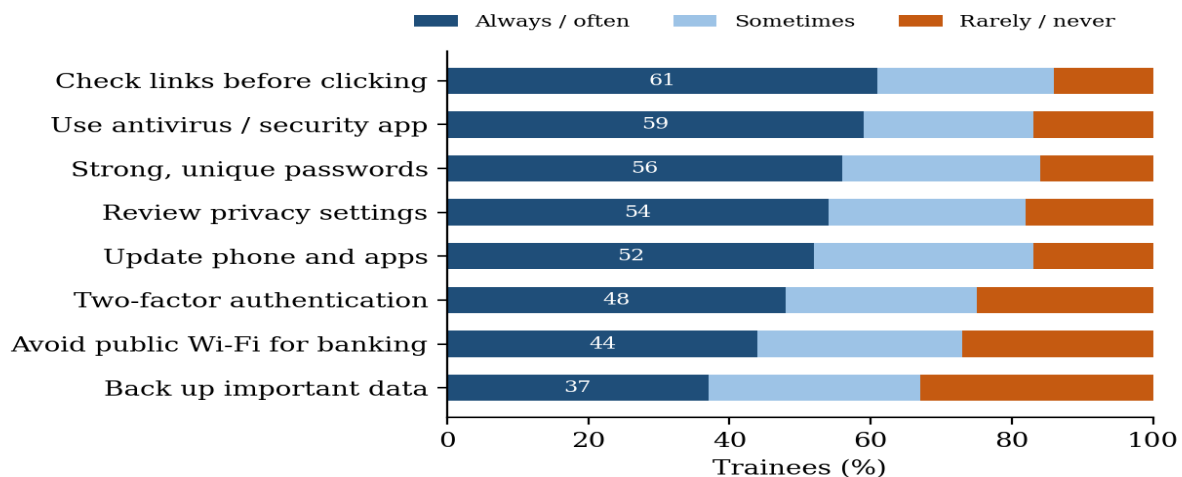


Figure 4. Frequency of cyber security practices among trainees

4.3 Gender differences (Objective 3; H_{01} and H_{04})

Table 2. Gender comparison of knowledge and practices (illustrative)

Variable	Female M (SD)	Male M (SD)	t	p	d
Knowledge (max 25)	14.61 (3.49)	14.88 (2.77)	-0.6	.548	-0.08
Practices (1–5)	3.14 (0.45)	3.06 (0.49)	1.24	.216	0.19

Note. Welch *t*-tests; female *n* = 124, male *n* = 76.

Male and female trainees did not differ significantly in knowledge ($t = -0.6$, $p = .548$) or in practices ($t = 1.24$, $p = .216$); effect sizes were negligible to small. H_{01} and H_{04} are retained.



4.4 Differences by academic stream (Objective 4; H_02)

Table 3. One-way ANOVA of knowledge by academic stream (illustrative)

Stream	n	M (SD)	F	p	η^2
Arts	82	14.07 (3.35)			
Science	70	15.59 (2.79)	4.37	.014	0.042
Commerce / other	48	14.54 (3.39)			

Note. $F(2, 197)$. The F , p and η^2 values apply to the whole comparison.

Knowledge differed significantly by stream, $F(2, 197) = 4.37$, $p = .014$, $\eta^2 = 0.042$, a small effect. Bonferroni-adjusted pairwise tests showed that science graduates scored significantly above arts graduates ($p = .009$), while the other two pairs did not differ (commerce/other vs arts $p = 1.000$; science vs commerce/other $p = .244$). H_02 is rejected (Figure 5).

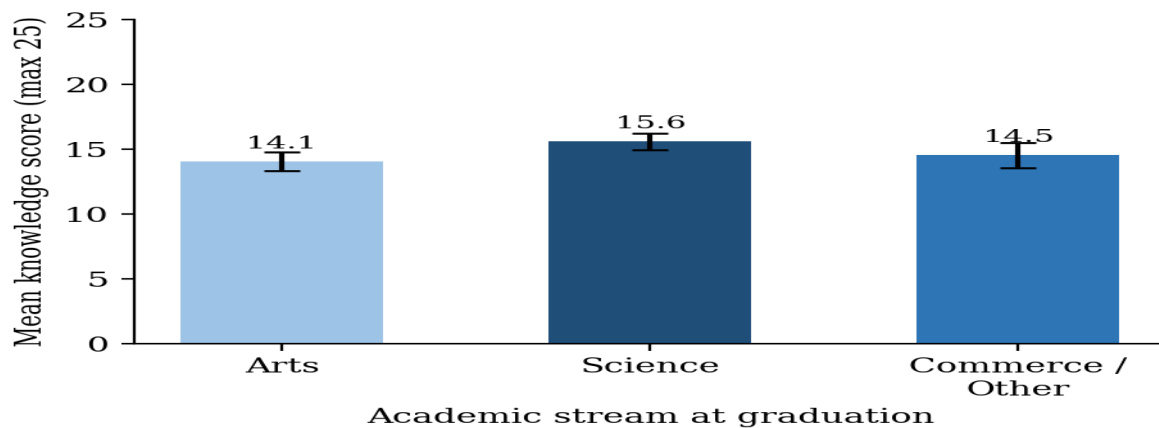


Figure 5. Mean knowledge score by academic stream (error bars show 95% confidence intervals)

4.5 Relationship between knowledge and practices (Objective 5; H_03)

Knowledge and practice scores were positively and significantly correlated, $r(198) = 0.49$, $p < .001$, a medium-to-large association: trainees who knew more tended to follow safer practices (Figure 6). Knowledge explains about 24% of the variance in practice, so most of the variation in practice is related to other factors such as attitude, habit and confidence. H_03 is rejected.

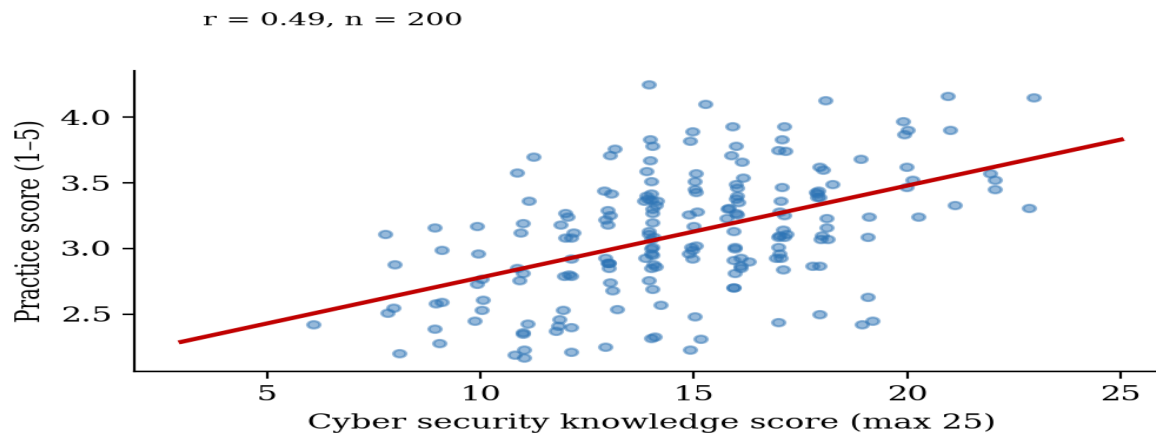


Figure 6. Relationship between knowledge and practice scores

As a supplementary check, daily internet use was weakly correlated with knowledge ($r = 0.18, p = .011$) and was not significantly correlated with practice ($r = 0.12, p = .104$), so more time online does not by itself make trainees safer.

Table 4. Summary of hypothesis decisions

Hypothesis	Content	Decision	Statistic
Ho1	Gender, knowledge	Retained	$p = .548$
Ho2	Stream, knowledge	Rejected	$p = .014$
Ho3	Knowledge–practice relationship	Rejected	$r = 0.49$
Ho4	Gender, practices	Retained	$p = .216$

5. Discussion

The pattern of results, moderate knowledge with moderate practice, is consistent with the view that awareness programmes reach the basics but leave gaps in technical and legal knowledge. Familiar threats (cyberbullying, phishing, payment fraud) were recognised by most trainees, while ransomware and cyber-law provisions were not. The positive relationship between knowledge and practice supports the knowledge–attitude–behaviour logic used in the awareness literature (Kruger & Kearney, 2006; Parsons et al., 2014), but the modest share of variance explained fits Protection



Motivation Theory and the Theory of Planned Behaviour: knowing is necessary but not sufficient, and risk perception, self-efficacy and habit also shape behaviour (Rogers, 1975; Ajzen, 1991; Ng et al., 2009).

The absence of a gender difference suggests that safe-practice education is needed equally for male and female trainees. The stream difference, with science graduates scoring higher, is plausible because science programmes involve more exposure to computing, but the effect is small and should not be over-interpreted. The weakest practices (backups, two-factor authentication, public Wi-Fi) are low-effort habits that are easily taught, which makes them good targets for training.

6. Educational Implications and Recommendations

1. Include a compulsory unit on cyber safety and digital citizenship in the B.Ed. programme, linked to the ICT course.
2. Teach and assess practical habits (password managers, two-factor authentication, updates, backups, safe use of public Wi-Fi), not only definitions.
3. Give trainees basic awareness of cyber-law provisions, reporting channels and how to handle cyberbullying involving students.
4. Use simulated phishing exercises and case studies from everyday situations such as UPI fraud.
5. Arrange orientation for arts and commerce graduates who may have had less exposure to computing.
6. Prepare trainees to teach cyber safety to school students during their teaching practice.

7. Limitations and Scope for Further Research

The sample is limited to selected colleges in one state, and practices are self-reported, so social desirability may inflate scores. The design is cross-sectional and correlational, so the knowledge–practice relationship does not establish that knowledge causes practice. Future studies could use a larger multi-district sample, add attitude and self-efficacy measures, compare trainees with in-service teachers, and test an intervention programme with a pre-test and post-test design.



8. Conclusion

This study set out to describe the cyber security knowledge and practices of B.Ed. trainees of Gujarat and to test their relationships with gender, stream and each other. The analysis shows moderate knowledge, moderate practice, no gender difference, a small stream difference and a positive relationship between knowledge and practice. The findings point to a clear role for teacher education: building practical, habit-oriented cyber safety competence in future teachers so that they can protect themselves and guide their students.

References

- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211.
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum Associates.
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.
- Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), 297–334.
- Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31(8), 983–988.
- Government of India. (2000). *The Information Technology Act, 2000*. Ministry of Law and Justice.
- Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289–296.
- Ministry of Education, Government of India. (2020). *National Education Policy 2020*.
- Mishra, P., & Koehler, M. J. (2006). Technological pedagogical content knowledge: A framework for teacher knowledge. *Teachers College Record*, 108(6), 1017–1054.
- Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4), 815–825.



Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114.

