

Proposal presentation

by Md Sadikur Rahman Chowdhury

Submission date: 04-Mar-2026 01:25PM (UTC+0000)

Submission ID: 276436543

File name: 67362_Md_Sadikur_Rahman_Chowdhury_Proposal_presentation_726817_1076561035.pptx (2.77M)

Word count: 1040

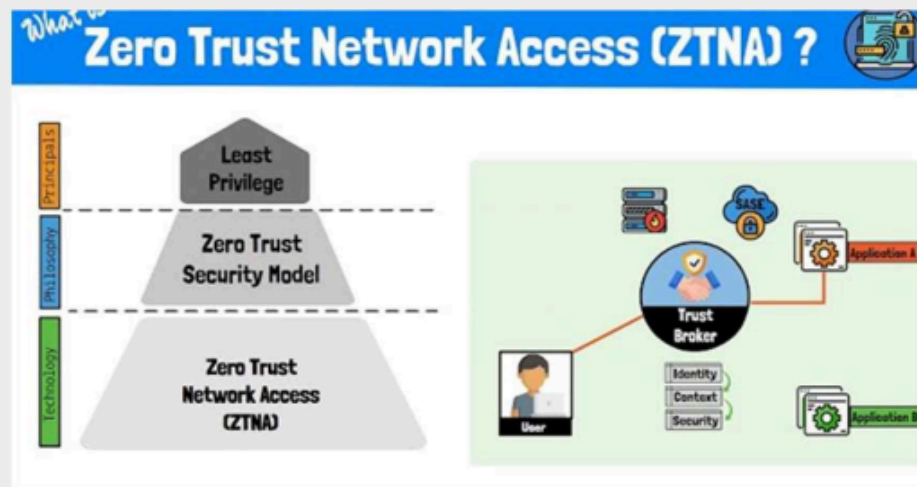
Character count: 6111

ACFA7004

Research Methods and Professional Development Presentation

Topic: The Efficacy of Adaptive Security Awareness Training (ASAT) in Reducing Social Engineering Success in Remote Enterprise Environments."

Research Background



The Modern Network Reality (2026)

- **Dissolution of the Perimeter:** The traditional "office wall" is obsolete; enterprise networking is now fully decentralized across home offices, transit hubs, and public Wi-Fi (Nahar *et al.*, 2024).
- **Technological Irony:** While high-level infrastructures like **Zero Trust (ZTA)** and **SASE** have hardened technical entry points, they have inadvertently made the "human element" the most attractive target for attackers.

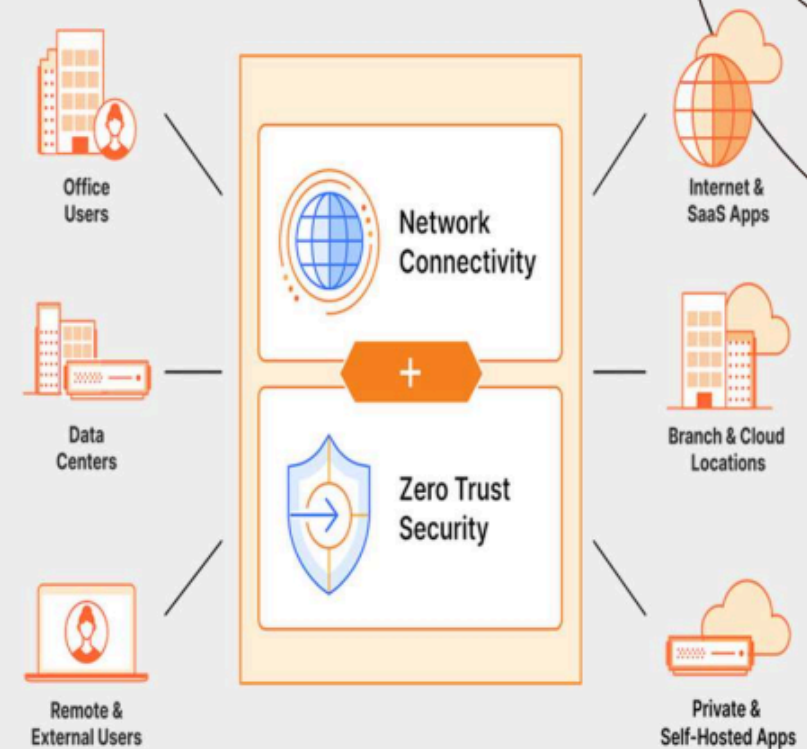
Research Problem

The Continuing "Knowledge-Action" Gap

- Existing literature notes that although workers might be able to succeed on the quiz as soon as they have viewed a training video, the defensive skills do not indicate real-life situations in three months (Hu *et al.*, 2022).

The Identified Research Gap:

- The available literature is very much on the content of training (what to teach), but does not mention the timing of the intervention (when to teach).
- It is direly needed in the field of empirical evidence of so-called Just-in-Time (JiT) learning-interventions, happening at the point when a dangerous behaviour is identified, but in this case, in the environment of widely-spread, remote enterprise networks (Hird and Sparrow, 2012).



Research Aims and Objectives

Research Aim

The aim is to compare the effectiveness of the Adaptive Security Awareness Training (ASAT), the system providing immediate behavioural-style feedback, versus the existing, periodic training tools, in the context of decreasing the success rate of social engineering attacks by remote employees.

Research Objectives

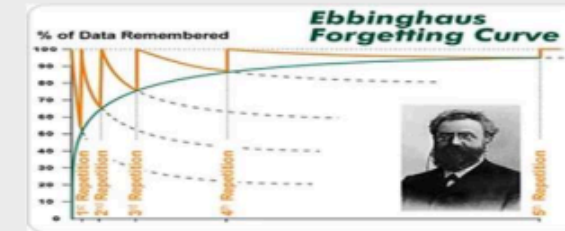
1. To determine the existing social engineering weakness in a remote workforce by conducting unannounced behaviour simulations.
2. To create a real-time (Just-in-time) feedback (JiT) system whereby micro-learning modules (less than 60 seconds long) are provided in real time when a user fails to recognise a simulated threat.
3. To assess the association of the frequency of adaptive interventions and long-term maintenance of security-first habits after 6 months.
4. To develop an enterprise HR and IT department policy roadmap to move away from static annual compliance to a dynamic, risk-based behavioural culture of security.

Literature Review

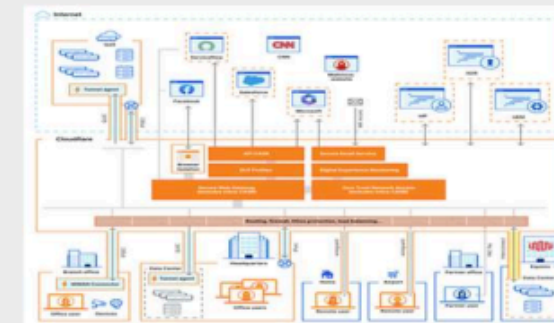
MFA Fatigue and Cognitive Load: The findings of a study done by Smith et al. (2025) indicate that remote workers who apply high-distraction conditions have higher chances of evading security measures to maintain their productivity.



The Ebbinghaus Forgetting Curve: There are psychological experiments in which psychology was applied to the field of cybersecurity that indicate that, in the case of a lack of reinforcement, 70% of security training is forgotten within the nearest 24-48 hours (Banjo, 2025).



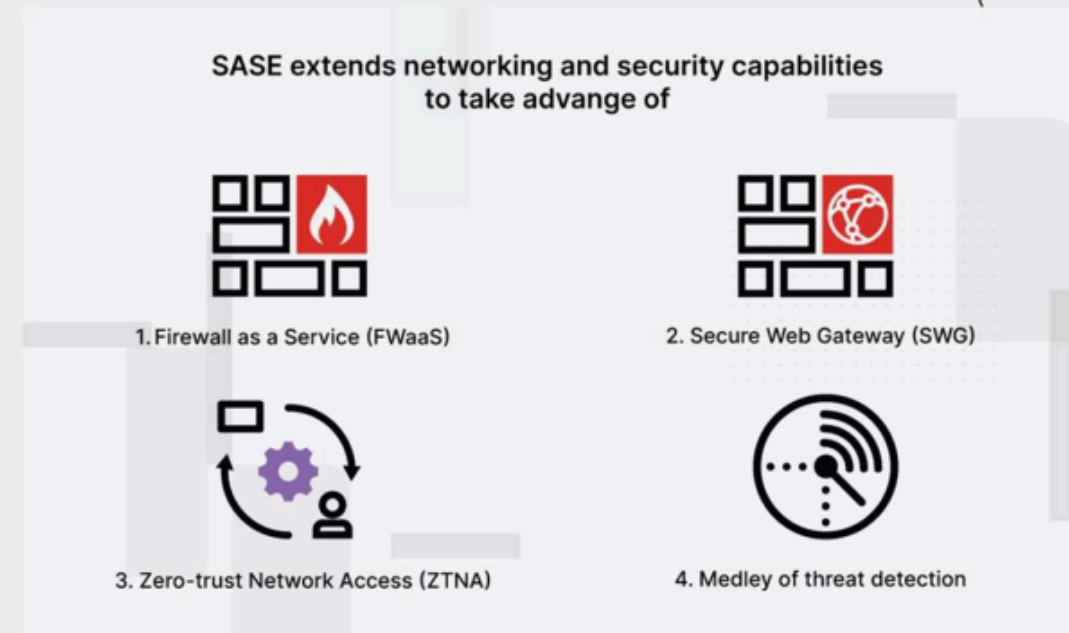
Nudge Theory in Cybersecurity: Jones (2024) discussed the concept of the so-called Security Nudges, such as small alterations to UI which influence better decision-making. This study was however, constrained to the interactions over the browsers and did not include the whole SASE/VPN setup (Konstantinou *et al.*, 2025).



Literature Review

Summary leading to the Gap:

- Although literature is affirmative that human beings are the weakest links and that nudges do act alone (Nahar *et al.*, 2024).
- no detailed research is found on using such nudges as part of an ongoing,
- adaptive feedback loop that reacts to live network behaviour in a remote enterprise environment.



Research Methodology

The project will involve a Mixed-Methods Quasi-Experimental Design.

Phase 1: Quantitative Simulation.

There will be two groups of remote employees of 100 each:

Control Group: Undergoes regular annual training of videos.

Experimental Group: The victim under ASAT. On clicking a fake phishing link, they are soon met with an instantaneous Teachable Moment pop-up indicating the red flags they overlooked.

Phase 2: Data Collection

Measures: Click rates, rates reporting (reporting via a button called Report Phishing), and time-to-report.

Frequency: Simulations will be held every two weeks with some degree of complexity.

Phase 3: Qualitative Evaluation

Semi-structured interviews were conducted on 15 participants of each group in order to comprehend the levels of "Security Frustration" and Self-Efficacy. This assists in deciding whether there is so-called Security Fatigue because of frequent training

Project Resources and Planning

Timeline (6 Months)

Month 1: Preparation & IRB approval

Month 2: Baseline assessment (phishing & social engineering)

Month 3: ASAT Framework deployment (JIT feedback)

Month 4: Data maturation (behavior retention)

Months 5-6: Analysis & ERP formulation

Task	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6
Preparation and Literature Review						
Baseline Assessment						
Intervention						
Data Maturation/Retention Tests						
Analysis and Policy Formulation						

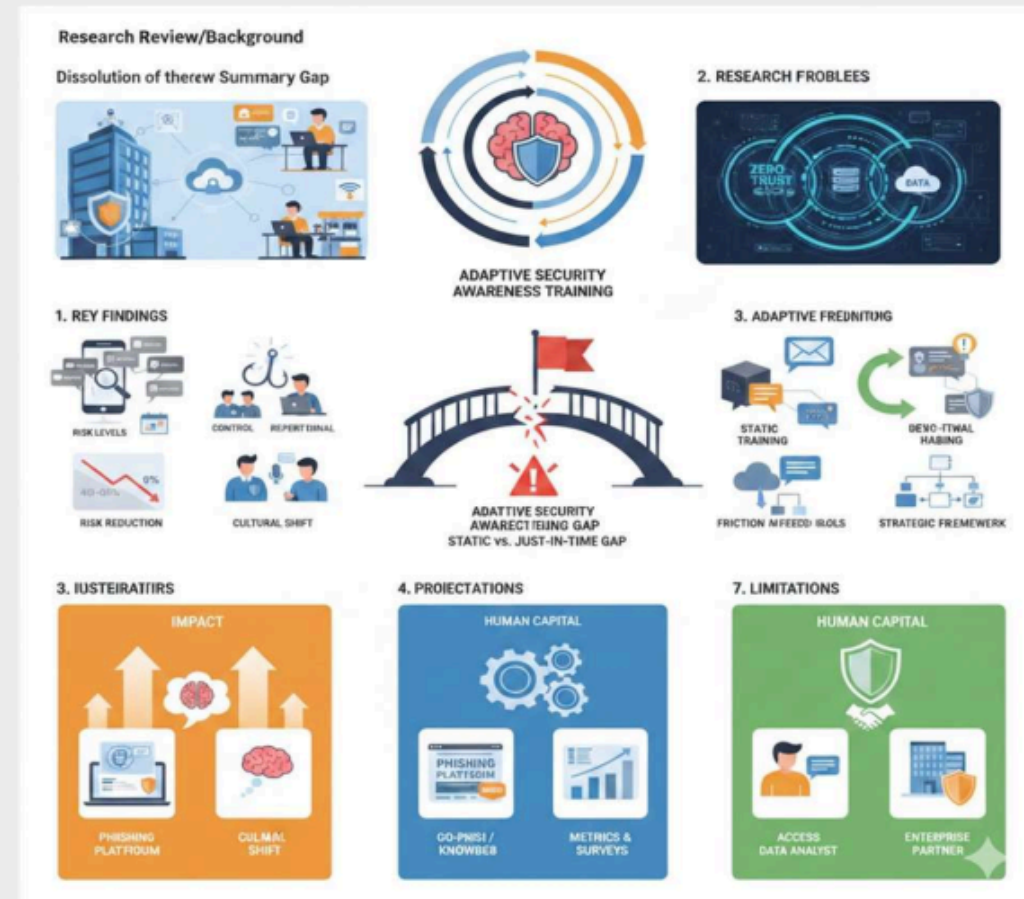
Project Resources and Planning

Resources Required

Software: A phishing simulation device (e.g., KnowBe4 or an open-source alternative such as Gophish) adapted to JiT redirects.

Human Resources: A behavioural psychologist (consultant) to review the content of training and a data analyst.

Access: The involvement of a partner with a mid-sized enterprise to facilitate a realistic remote-working environment.



Impact and Limitations of the Project

Anticipated Impact

Minimisation of Risk: The experimental group will record a reduction in the risk by almost 40-60% in the rate of clicks.

Cultural Shift: Making security a matter of habit - remote workers.

Cost Efficiency: Showing that brevity and targeting make short interventions more cost-efficient compared to lengthy and ineffective training seminars.

Limitations

- Sample Bias
- Technical Constraints
- Privacy Issues


$$\text{Relative Risk Reduction (RRR) Formula} = \frac{(\text{Control Event Rate (CER)} - \text{Experimental Event Rate (EER)})}{\text{Control Event Rate (CER)}}$$




References

- Banjo, O. O. (2025). Enhancing Cybersecurity through Comprehensive User Training Programs: A Study on Mitigating Social Engineering Threats (Doctoral dissertation, Dublin, National College of Ireland).
- Hird, M., and Sparrow, P. (2012). Learning & Development: Seeking a Renewed Focus?. Lancaster University Management School.
- Hughes-Lartey, K., Li, M., Botchey, F. E., and Qin, Z. (2021). Human factor is a critical weak point in the information security of an organisation's Internet of Things. *Heliyon*, 7(3).
- Hu, S., Hsu, C., and Zhou, Z. (2022). Security education, training, and awareness programs: Literature review. *Journal of Computer Information Systems*, 62(4), 752-764.
- Jones, M. L. (2024). The nudge trap: Why passive security alerts fail in remote enterprise environments. *Journal of Cybersecurity and Behavioural Science*, 12(3), 145–162.
<https://doi.org/10.1016/j.jcyber.2024.05.012>
- Konstantinou, L., Panos, D., and Karapanos, E. (2025). Exploring the design of technology-mediated nudges for online misinformation. *International Journal of Human–Computer Interaction*, 41(1), 515-542.
- Nahar, N., Andersson, K., Schelén, O., and Saguna, S. (2024). A survey on zero trust architecture: Applications and challenges of 6 G networks. *IEEE Access*, 12, 94753-94764.



Thanks!

CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon** and infographics & images by **Freepik**

Please keep this slide for attribution

Proposal presentation

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

21 /100

Further to the comments provided during the presentation, please follow the feedback provided for each category in the rubric.

Also, an artefact needs to be developed as part of the project.

As discussed the proposed topic is not acceptable considering the ethical issues.

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

GRADING FORM: ACFA7004 PROPOSAL PRES 2026

MD SADIKUR RAHMAN CHOWDHURY

21

ENGAGEMENT WITH LIT.SKILL [20]

Relevant and recent Literature support for Research background/context [7 Marks] Recent Literature support for the identified research problem [7 Marks] Recent and Relevant in-text citations and reference list [6 Marks]

 The relevant and recent literature is provided, however as discussed during the presentation the topic needs to be changed. Incorrect citation and reference style. **6**

KNOWLEDGE _ UNDER.. SKILLS[15]

Brief overview and current developments in the proposed research area [10 Marks] Research problem statement [5 Marks]

 The background is not clearly stated as per the given research problem. **4**

COGNITIVE&INTELL. SKILLS[20]

Formulation of research aim and objective based on the identified research problem [20 Marks]

 During the presentation, the it is indicated that the research will be done in Bangladesh and considering the ethical issues, this is not acceptable. The topic needs to be changed. **4**

PRACTICAL APPN SKILLS[25]

Selection of appropriate research methods and materials to achieve the research objectives, with justification [15 Marks]
Details of the data collection and evaluation process [10 Marks]

 as discussed, please change the topic and consider a project that can be implemented here in UK. Formulate the research aim and objectives clearly and follow a propose research methods to achieve the objectives.

2

TRANSF. SKILL & PROF.PRAC [20]

Project planning and resource management [10 Marks] Description of the project's potential impact and limitations [5 Marks] Presentation style [5 Marks]

 Project planning and resources are need to be revisited. Understand the requirements of the assessment and prepare them accordingly. Presentation was good.

5