Google

Be Scam Ready

Inoculating Users Against Online Scams Using A Game Based Intervention

A Case Study from India

Abhishek Roy, Narsi G & Sujata Mukherjee

Published: February 2025 | Updated: October 2025

Acknowledgements

The authors would like to express their sincere gratitude to Prof. Sander Van der Linden for his invaluable insights and guidance on the application of inoculation theory to scam prevention. We are also deeply indebted to Prof. Monica Whitty for her expertise on scam tactics and victim vulnerabilities, which significantly informed the development of ShieldUp! We also extend our thanks to Shubham Goswami for his contributions to the research and his collaboration throughout this project.

Note

Throughout this whitepaper we refer to "Project ShieldUp!". This was the name for our pilot experiment in India in 2024. As of 13 Oct 2025, Project ShieldUp! is now available as a non-commercial web based game at `https://bescamready.withgoogle.com/`

Table of Contents

Introduction

India is experiencing an unprecedented surge in online scams, fueled by rapid digitalization and widespread adoption of mobile payments. The scale and impact of these scams are staggering. According to the Indian Cyber Crime Coordination Centre (I4C), an average of 7,000 complaints were registered daily between January and April 2024, a 113% increase over the same period in 2021–2023 [Singh, 2024]. Financial fraud accounts for three-quarters of all cybercrime in India, with approximately 47% being UPI-based [Tripathi, 2024]. A 2023 YouGov survey found that 47% of respondents said a friend or family member had lost money to an online scam [Singh, 2023].

In the first four months of 2024, Indians lost over INR 1,750 Crore (approximately USD 209 million) to cybercriminals [Tripathi, 2024].

A recent global study revealed that Indian users receive an average of 12 scam messages daily, spending an estimated 1.8 hours per week dealing with them [Dixit, 2023]. Moreover, in a 2023 McAfee survey, 60% of Indian respondents reported difficulty identifying scam messages, attributing this to scammers' increasing use of AI [Rao, 2023]. India's diverse and rapidly evolving digital landscape, while empowering millions, has also become a fertile ground for scammers. The Unified Payments Interface (UPI), a cornerstone of India's digital payment revolution, has unfortunately become a tool for fraudsters. This, coupled with the widespread use of mobile devices and varying levels of digital literacy, creates a complex challenge demanding innovative solutions.

> *"They [scams] involve the misrepresentation of facts and the deliberate intent to deceive with the promise of goods, services, or other financial benefits that in fact do not exist or that were never intended to be provided.*
>
> *[Titus et al., 1995]*

Traditional awareness campaigns, like informational videos or text based tips, have unknown or unproven efficacy in empowering users to combat online scams [Chugh and Narang, 2023, Rahman et al., 2023]. Furthermore, awareness campaigns frequently suffer from broad targeting, ill-defined success criteria, and lack of efficacy measurement (i:e change in user behavior), leading to uncertainty about their effectiveness. Research has also shown that simply providing more information or facts is unlikely to effectively change user behavior [Christiano and Neimand, 2017], particularly when scammers induce a "hot" emotional state, increasing likelihood of impulsive and error prone decision making [Loewenstein et al., 2001, Slovic et al., 2007]. Also, because scams rapidly evolve, training focused on specific scenarios risks obsolescence. Moreover, the rapidly evolving nature of online scams poses a challenge for traditional training methods that focus on specific scenarios.

To address these limitations, we explored **game-based inocula-**

tion, leveraging the psychological inoculation theory [McGuire, 1961]. This approach preemptively exposes individuals to weakened forms of persuasive messages (scam manipulation tactics) and provides preemptive refutation of these tactics so as to build resistance against future manipulation. Additionally, game-based learning offers a safe and engaging environment to experience and learn from potential threats, promoting active learning and knowledge retention [Hu et al., 2023, Breuer and Bente, 2010].

This case study presents **ShieldUp!**, a mobile game prototype developed to inoculate users against common online scams prevalent in India. We detail the game's development—guided by research on scam tactics and user behavior—and highlight key findings from a pilot study. We discuss the implications of our findings for scam-resistant products and outline future research directions.

As scammers constantly adapt their tactics and exploit new vulnerabilities, training that emphasizes recognizing static red flags may not adequately prepare users to identify novel scams, risking obsolescence and limited transferability of skills.

Figure 1: ShieldUp! has 3 increasing difficulty levels creating a skill ladder and cognitive scaffolding.

Inoculation Theory & Scam Prevention

Traditionally, scam prevention strategies include general awareness campaigns, digital / financial literacy training, technology based solutions, and scam-specific training. Additionally, governments and regulatory institutions have intervened with legal and regulatory measures. However, a recent review of real-world fraud prevention interventions highlights a lack of rigorous evaluations and an over-reliance on diagnostic studies and untested assumptions [Prenzler, 2019].

General awareness campaigns, such as UK's National Cyber Security Centre's Cyber Aware campaign and Australia's ACCC's Scamwatch, are designed to raise public awareness and serve as valuable repository of information for consumers [Ncs, , Sca, 2024]. These campaigns often use mass media, social media, and public service announcements. While they are prominently deployed as a tool by both the public [Ncp,] and private sectors [Chadha, 2022], there is limited direct evidence that they help raise awareness and are efficacious. Research consistently challenges the 'information deficit model,' showing that simply providing more information is unlikely to change behavior, particularly when other cognitive or emotional factors are at play [Christiano and Neimand, 2017]. This is particularly relevant in scam contexts, where scammers often induce a 'hot' emotional state—fear, excitement, or greed—precisely to exploit these vulnerabilities in judgment and increase impulsive de-

cisions [Loewenstein et al., 2001]. Combining these effects leads to reduced vigilance as victims fail to scrutinize information that might otherwise raise alarms. A meta-analysis of social engineering interventions found that awareness campaigns, while sometimes helpful, are generally less effective than more interactive and targeted approaches [Bullee and Junger, 2020].

Digital literacy training aims to equip individuals with critical thinking skills and knowledge to navigate the digital world safely. Organizations like MediaSmarts in Canada and Google's Be Internet Awesome program provide educational resources [Jones et al., 2023, Hoechsmann et al., 2016]. This approach acknowledges that a lack of digital literacy can increase vulnerability. However, digital literacy training is often broad, and its effectiveness for scam prevention requires further research.

Technology-based interventions are crucial. Anti-phishing tools, spam filters, and multi-factor authentication prevent scams and protect accounts. For example, the Singaporean government developed ScamShield that provides a product suite to help users check suspicious calls, websites, and messages [Sca,]. While these offer a first line of defense, they cannot fully address the human element of scams, which often uses social engineering and psychological manipulation to bypass technological safeguards. Over-reliance on technology can create a false sense of security, discouraging critical thinking.

Financial literacy education can indirectly help prevent financial scams by empowering individuals to make informed decisions. [Lusardi and Mitchell, 2014] This approach emphasizes that financial knowledge can be a protective factor. For example, understanding the concept of compound interest and legitimate investment returns can help individuals spot unrealistic promises of quick riches, a common tactic in many scams. Burke et al. (2022) explored educational interventions, finding some positive effects [Burke et al., 2022]. However, maintaining and scaling this approach is challenging, and its impact on broader scam recognition is uncertain.

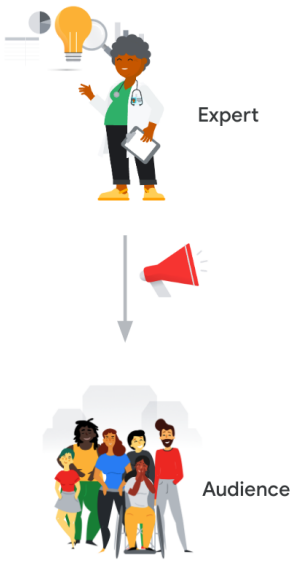

Figure 2: General Awareness Campaigns are based on Miller's 'information deficit model,' which assumes that users lack knowledge and that simply providing more information will change their behavior. [Miller, 1983]

Our Approach: Inoculation Against Manipulation Techniques

Manipulation techniques, a perversion of persuasion techniques, are central to scams. While persuasion involves ethically influencing

for mutual benefit; manipulation exploits victim's psychological vulnerabilities. Robert Cialdini's *The Psychology of Persuasion* outlines six core principles: reciprocity, scarcity, authority, consistency, liking, and social proof [Cialdini, 1984]. These principles leverage our natural tendencies for trust, social conformity, and reciprocation to increase compliance with requests, even when those requests are deceptive or harmful. For example, scammers often create a false sense of scarcity or urgency to pressure victims into making quick decisions without careful consideration [Ariely and Zakay, 2001].

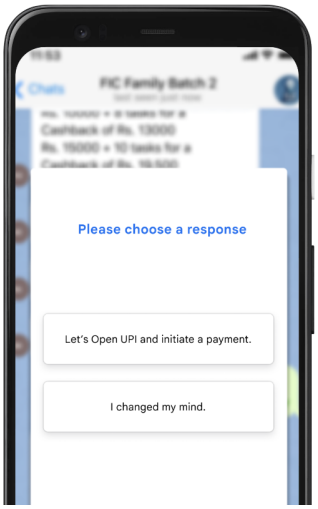

Figure 3: ShieldUp! confronts users to make choices simulating real-world scam scenarios

Since emotional appeals and psychological manipulation techniques often bypass rational decision-making [Petty, 1977], an approach that preemptively addresses these emotional vulnerabilities is crucial for effective scam prevention. Ergo, Psychological Inoculation, introducing users to weakened threats to increase resilience, is an approach worth exploring.

Introduced by McGuire (1961), inoculation theory posits that resilience can be built by introducing weakened attacks and then refuting them [McGuire, 1961]. An inoculation treatment includes a forewarning and preemptive refutation [Compton and Pfau, 2005]. Thus, pre-exposing users to weakened scams and providing counterarguments could build future immunity. Recent studies have shown inoculation improves scam detection without harming trust [Robb and Wendel, 2023, DeLiema et al., 2024].

Inoculation theory has demonstrated efficacy in bolstering attitudinal resilience against misinformation [Roozenbeek and van der Linden, 2019, McPhedran et al., 2023], extremist narratives [Saleh et al., 2023], and even in smoking prevention [Pfau et al., 1992]. Inoculation theory, therefore, offers a robust framework for building resistance against persuasion and manipulation.

To summarize, therefore, our thesis was that inoculating users against common *manipulation techniques* rather than specific scenarios might be a robust alternative to traditional methods of interventions against scams. We posit that this approach has the following advantages:

- **Scalability:** Focusing on core techniques covers a wide array of scams.
- **Adaptability:** New techniques can be added easily.
- **Cross-protection:** Recognizing techniques in one context aids identification in new scenarios.

- **Cognitive Efficiency:** Teaching principles is more effective than teaching about specific instances.
- **Long-term Relevance:** Techniques persist even as specific scams evolve.
- **Empowerment:** Critical thinking skills extend beyond scams.

Developing ShieldUp!: A Game-Based Approach to Scam Prevention

Building upon the principles of inoculation theory and a deep understanding of the Indian scam landscape, we developed ShieldUp!, a mobile game designed to empower users with the knowledge and skills to identify and avoid online scams.

Understanding Victim User Journeys

Broadly, most scams follow a three phase trajectory: hook, interaction and closure. Hooks are designed to capture attention, followed by manipulation tactics to gain trust and exploit vulnerabilities, ultimately leading to loss of utility (monetary/information) for the victim. For example, a common tactic employed by scammers is to impersonate legitimate entities such as banks, courier services, or government agencies to gain the victim's trust [Tripathi, 2024]. They may also leverage social pressure, using fake testimonials or creating a sense of urgency to coerce individuals into making hasty decisions.

Our preliminary analysis of India's scam landscape revealed that UPI scams, customer care scams, job scams, loan scams, marketplace scams, and crypto scams are among the most prevalent in India [Tripathi, 2024, Singh, 2024].

We used Google advanced search features to search for a combination of keywords and identify user journey stories that were reported by 3rd party agencies like news and watchdog agencies or were self-reported by users on social media (Reddit, Twitter, Facebook etc.). We scanned and filtered through the first 5 pages of Google Search Results. In total, we collected 31 victim stories for 8 scam schemes, a full breakdown of which is available in *Appendix A*.

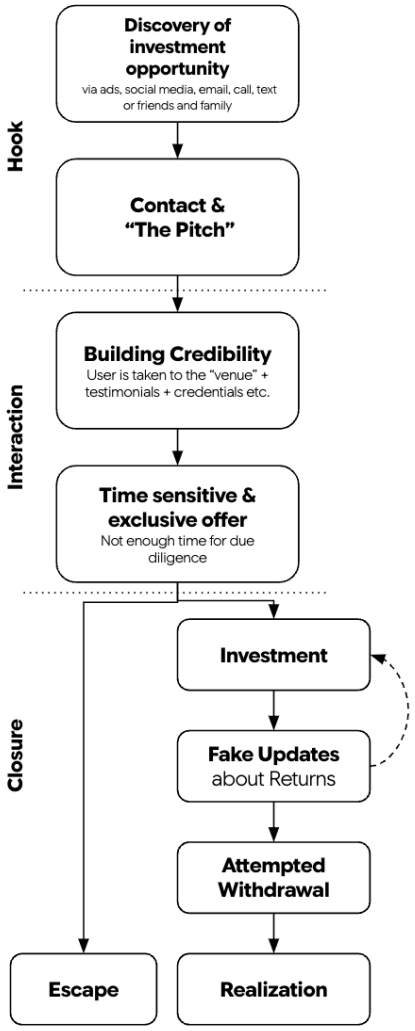

Figure 4: Example of a user journey mapping exercise used to design a game scenario, illustrating the flow of interactions and decision points involved in a typical Investment Scam

We captured the following aspects of the Victim User Journeys (VUJs):

1. Key aspects of a typical victim's user journey (Hook, Interaction & Closure)
2. Manipulation techniques and other tactics used by scammers in different parts of the VUJ.
3. Victim vulnerabilities targeted
4. Mental state and emotions felt by the victim (before, during and after the end of the VUJ).

This analysis allowed us to identify common scam narratives, manipulation techniques employed by scammers, and vulnerabilities targeted in victims.

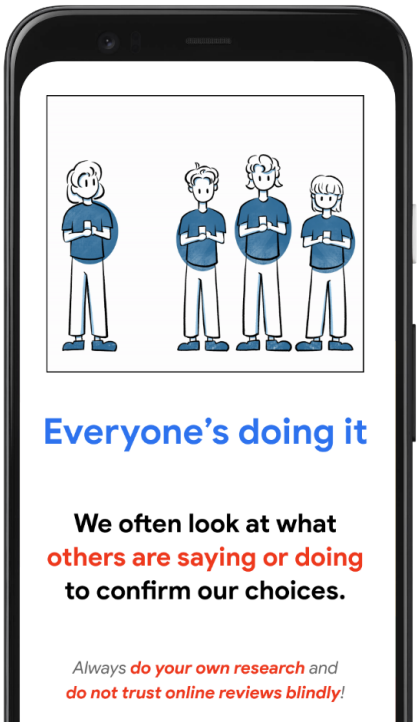

Figure 5: ShieldUp! has animated figures helping users understand manipulation techniques.

Identifying Target Vulnerabilities

Our analysis revealed a range of emotional and cognitive vulnerabilities that scammers frequently exploit:

- **Trust in Authority:** Scammers often impersonate authority figures or well-known companies to leverage pre-existing trust.
- **Desire for Quick Rewards:** Promises of easy money, high returns on investments, or quick solutions to problems often cloud judgment.
- **Lack of Awareness:** Limited knowledge of common scam tactics, digital security measures, or the workings of specific online platforms can increase vulnerability.
- **Emotional Reasoning:** Scammers often induce fear, excitement, or a sense of urgency to trigger impulsive decision-making.

Design Principles for Developing ShieldUp!

Informed by the aforementioned research, we designed ShieldUp! as an interactive mobile game prototype that simulates real-world scam scenarios, allowing users to safely experience and learn from potential threats.

Key design features of ShieldUp! include:

- **Realistic Scenarios:** The game features a variety of scam scenarios based on real-world examples collected through our research, ensuring relevance and familiarity for Indian users.
- **Gradual Difficulty Progression (Skill Ladder):** ShieldUp! utilizes a "skill ladder" approach, gradually increasing the complexity of scams as players progress through the levels. This allows users to build confidence and apply their growing knowledge to increasingly challenging situations. This approach incorporates principles of *cognitive scaffolding*, where users are initially provided with more support and guidance, which is gradually reduced as their skills and understanding develop.
- **Interactive Storytelling:** The game utilizes an engaging narrative format, presenting players with choices that determine the course of the interaction. This interactive approach fosters active learning and allows users to experience the consequences of their decisions in a safe environment.
- **Explicit Teaching of Manipulation Tactics:** After each scenario, the game provides clear explanations of the manipulation tactics used by the scammer, using simple language and memorable visuals. This equips users with the knowledge and vocabulary to identify these tactics in real-world settings.
- **Active Recall and Reinforcement:** ShieldUp! incorporates quizzes and interactive elements throughout the game play to reinforce learning and promote knowledge retention.

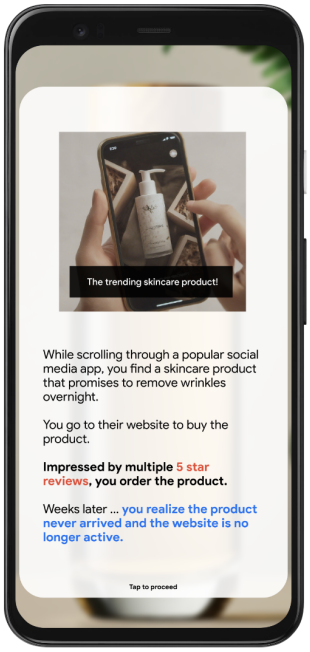

Figure 6: The game ends up with a short interactive quiz as an active recall exercise.

Targeting Specific Manipulation Tactics To ensure ShieldUp! effectively builds user resilience, we focused on incorporating the most prevalent and potent manipulation tactics identified in our research. These include:

- **Social Proof (Conformity):** ShieldUp! presents scenarios where scammers leverage fake testimonials, inflated user numbers, or group chat dynamics to create a false sense of legitimacy and urgency. The game then teaches players to recognize and question such attempts to manipulate their behavior through social pressure. [Cialdini et al., 1999]
- **Appeal to Authority:** The game features situations where scammers impersonate authority figures, such as bank officials or government representatives, to gain trust and coerce action. ShieldUp! trains users to be wary of such authority claims and verify information through official channels. [Milgram, 1965]

- **Foot in the Door:** ShieldUp! incorporates scenarios where scammers start with small, seemingly harmless requests that gradually escalate into larger demands. Players learn to recognize this pattern and set boundaries to prevent being drawn into exploitative situations. [Freedman and Fraser, 1966]
- **Urgency/Scarcity:** The game simulates scenarios where scammers use time pressure, limited-time offers, or impending deadlines to trigger impulsive decision-making. ShieldUp! trains players to resist this pressure, step back, and assess situations rationally before taking any action. [Ariely and Zakay, 2001]
- **Appeal to Emotions:** ShieldUp! includes scenarios designed to evoke strong emotions like fear, excitement, or greed, mirroring real-world tactics used to cloud judgment. The game teaches players to recognize these emotional triggers and seek alternative sources of information before making any decisions. [Loewenstein et al., 2001]
- **Norm Activation:** Activation of personal or social norms (what one believes they should do) can significantly motivate behavior, especially in contexts where these norms are made salient. The game simulates scenarios which try to trigger and help users recognize how norm activation is used in by scammers to manipulate them into their schemes. [Schwartz, 1977]

By directly addressing these specific manipulation tactics within the game's scenarios, ShieldUp! equips players with the knowledge and skills to recognize and resist such tactics in real-world settings. Combining realistic scenarios, interactive gameplay, and explicit teaching of manipulation tactics, ShieldUp! aims to empower users with the critical thinking skills and behavioral strategies needed to navigate the digital landscape safely and confidently.

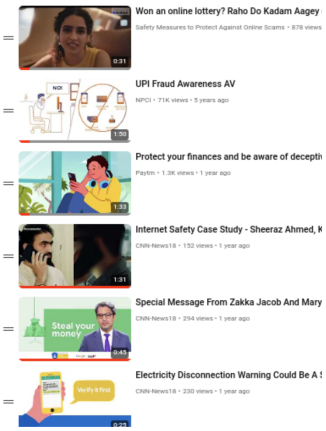

Figure 7: Active control group watched 5 short scam awareness campaign advertisements

Pilot Study and Key Findings

To evaluate the efficacy of ShieldUp! in improving scam identification, we conducted a randomized controlled trial with 3,000 participants in India.

Experimental Design

The experiment had 4 parts: a pre-test to establish baseline scam and not scam identification abilities, the intervention, a post test to measure any change in abilities and a 21 day follow up assessment of ability. Participants were randomly assigned to one of three groups:

1. **ShieldUp! Group (Treatment):** Participants in this group played ShieldUp! for approximately 15 minutes.
2. **General Awareness Group (Active Control):** Participants in this group watched a series of scam awareness videos and read safety tips for approximately 10 minutes. The content for this group was curated from reputable sources, including government agencies, news channels and technology companies and can be found here and the safety tips can be found in *Appendix B*.
3. **Chrome Dino Group (Control):** Participants in this group played the Chrome Dino game for approximately 8 minutes. This group served as a baseline to control for the effects of simply engaging with a digital activity.

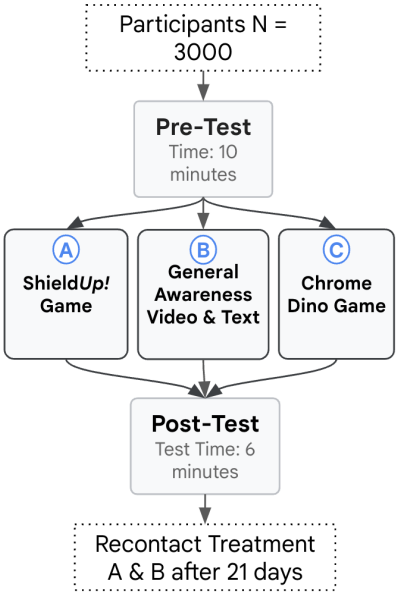

Figure 8: Experiment Design for the Randomized Controlled Trial

Measuring Scam Discernment Ability

To assess a user's scam discernment ability, we developed the Scam Discernment Ability Test (SDAT-10), a 10-item test designed to measure an individual's capacity to identify and differentiate between scam and non-scam scenarios. The development of SDAT-10 involved a rigorous three-stage process: item generation, item condensation, and scale construction.

Item Generation Drawing on I4C data, we identified the most prevalent scam types in India: Customer Care, Courier, Refund, Jobs, Friends/Family Impersonation, Online Shopping & P2P Marketplace, and Crypto & Investment scams [Singh, 2024]. We then conducted a thematic analysis of 31 real-world scam victim user journeys reported in news media, social media, and civil society reports. This analysis allowed us to identify common scam narratives, manipulation techniques employed by scammers, and vulnerabilities targeted in victims.

Based on this analysis, we generated over 40 storylines, each with

both scam and non-scam variants, resulting in a pool of over 80 potential test items.

Item Condensation An expert committee reviewed the initial pool of items for content validity, resulting in the selection of 23 items for further testing. We tested these 23 items with a random sample of 360 users in India via an online survey. Based on Exploratory Factor Analysis (EFA), Item Response Theory (IRT) analysis, reliability analysis, and validity assessments, we shortlisted the 10 best performing items.

Scale Construction To mitigate memorization effects between pre- and post-tests, we created a second version (replica) of the SDAT-10 by making aesthetic changes to each item while maintaining the core storyline. Both versions were then tested again with a random sample of 600 users in India (300 per version) to confirm the 2 factor structure (one for scam identification ability and one for not scam identification ability) and to ensure that both the test sets were balanced.

The final SDAT-10 comprises five scam scenarios and five non-scam scenarios, each presented as a medium-fidelity interactive prototype depicting a typical scam user journey. Each scenario is accompanied by three questions assessing:

1. **Scam Compliance:** Likelihood of continuing engagement with the scenario.
2. **Discernment:** Categorization of the interaction as "Scam" or "Not Scam."
3. **Confidence:** Level of confidence in their assessment.

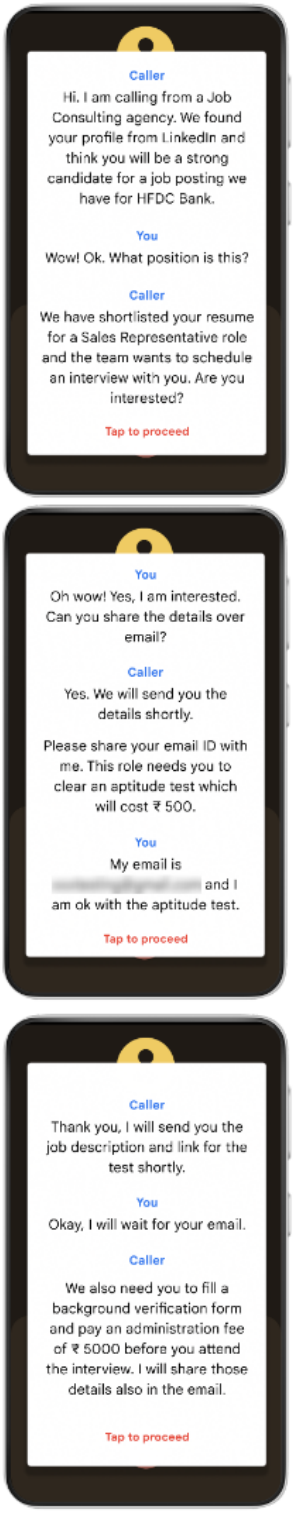

Figure 9: A SDAT-10 question item depicting a Job Scam

Key Findings

Using an ANCOVA model, we tested if there was an increase in user ability to correctly identify Scam and Not Scam scenarios post-intervention while controlling for their demographic profile (age, gender, income level, education level) and their pre-intervention ability of correctly identifying these scenarios. Since there were 5 scam and 5 not scam scenarios, their scam scores (1-5) denote their ability to identify scam scenarios correctly and their not scam scores denote their ability to identify not scam scenarios correctly.

Our analysis revealed the following key findings:

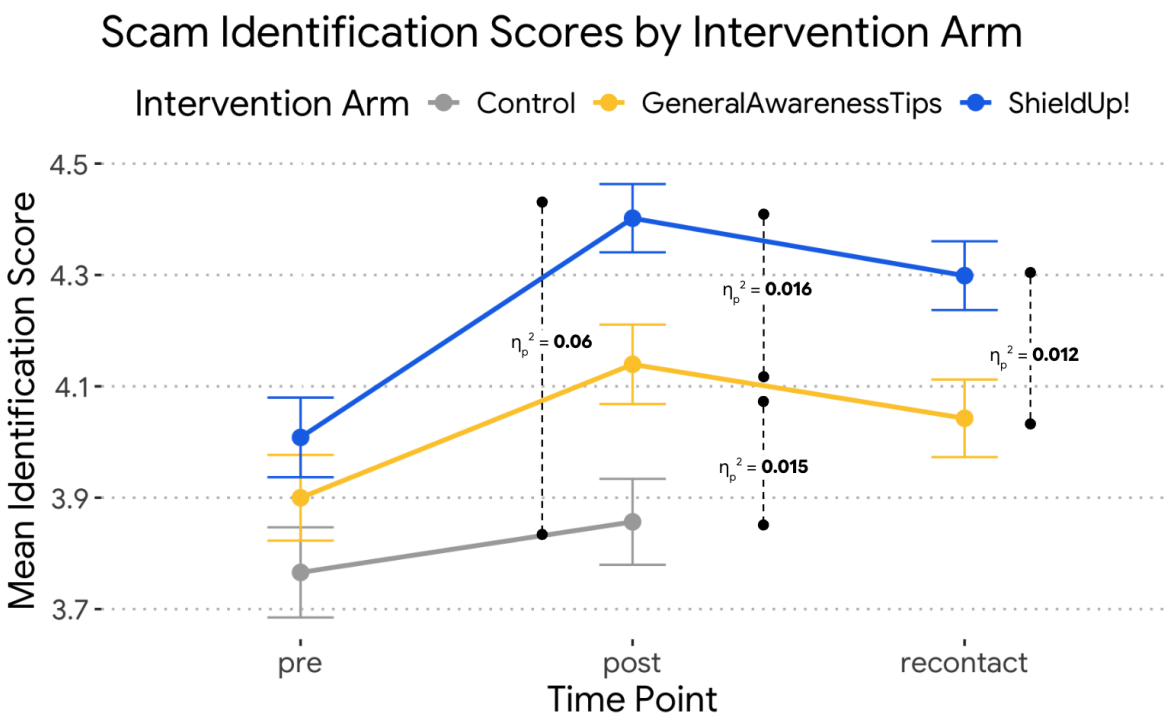

Figure 10: Mean Scam Identification scores by intervention arm at pre-test, post-test, and 21-day follow-up. Error bars represent standard errors.

1. **ShieldUp! Improved Scam Identification Ability:** Participants who played ShieldUp! demonstrated a statistically significant improvement in their ability to discern scam scenarios compared to both the general awareness and control groups. This effect was observed immediately after the intervention and persisted at a follow-up assessment conducted 21 days later.
2. **Users have increased skepticism towards genuine offers following interventions, but this dissipates over time:** Immediately following both the ShieldUp! and general awareness interventions, participants exhibited heightened skepticism towards certain genuine online offers, such as cashback rewards and shopping discounts. This is similar to what Kubilay et al. observed in their intervention as well [Kubilay et al., 2023]. However, we observe that this initial increase in skepticism dissipated after 21 days for both ShieldUp! and General Awareness arms, suggesting that the interventions did not negatively impact trust in legitimate online interactions in the long term.
3. **Effect Sizes:** The ShieldUp! intervention demonstrated a mod-

Players experience an increased reluctance towards genuine offers after playing ShieldUp!, but this dissipates over time.

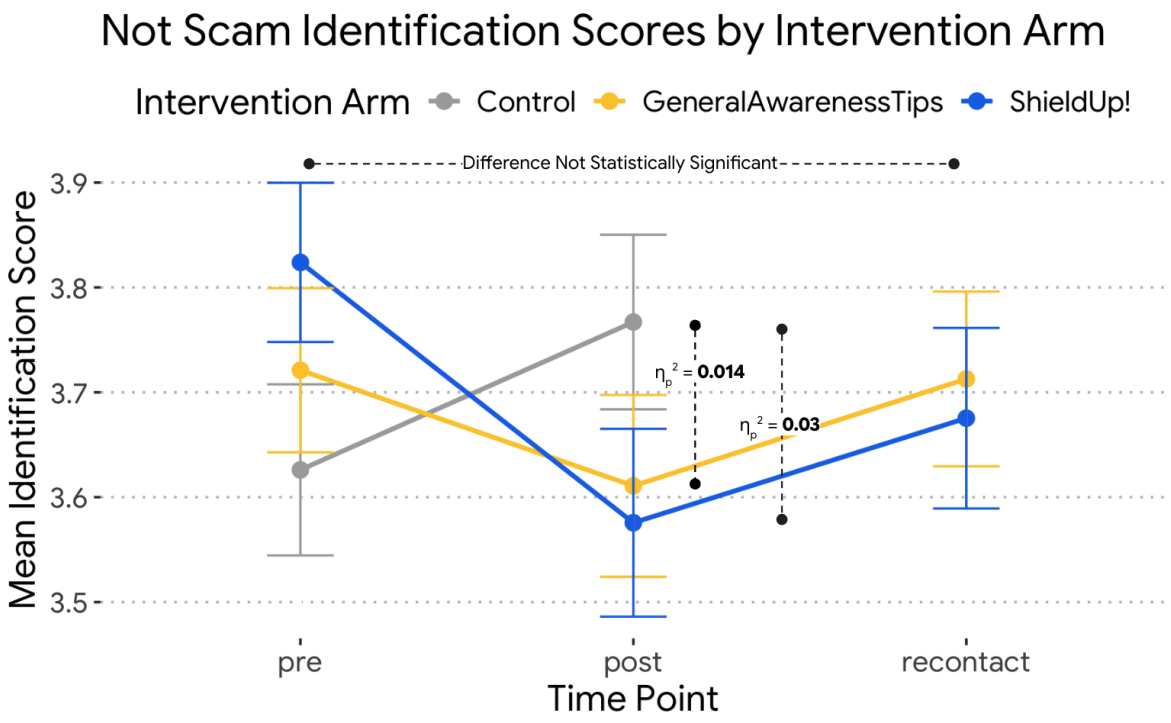

Figure 11: Mean Not Scam Identification scores by intervention arm at pre-test, post-test, and 21-day follow-up. Error bars represent standard errors.

erate effect size compared to the control group in improving scam identification. The general awareness intervention showed a smaller effect size compared to both the control and ShieldUp! groups. This suggests that the active, game-based approach of ShieldUp! was more effective in enhancing scam identification than passive exposure to awareness materials.

The findings of our pilot study provide promising evidence for the effectiveness of ShieldUp! as a game-based intervention for improving scam identification. The game's ability to engage users, simulate realistic scenarios, and explicitly teach manipulation tactics appears to translate into tangible improvements in users' ability to identify and avoid potential scams. Moreover, the observed increase in skepticism towards genuine offers was temporary, suggesting that the game does not promote undue distrust in legitimate online interactions over longer periods of time while the improvements in scam identification abilities stay at an elevated level after 21 days.

Implications and Recommendations

The ShieldUp! pilot study demonstrated the effectiveness of inoculation-based gamified training in improving users' scam identification skills. This has significant implications for product design, policy, and future research in combating online scams.

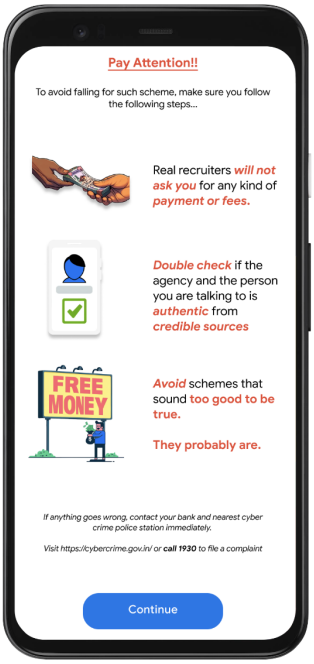

Figure 12: A safety advisory messages relevant to the scam scenario were shown after each level in the game

Implications for Product Design

1. **Integrate Inoculation-Based Training:**
    - **Interactive Learning Modules:** Introduce users to common manipulation techniques and provide opportunities to practice identifying scams in a safe environment. This can be achieved through engaging tutorials and interactive simulations that mimic real-world scam encounters, offering immediate feedback and guidance. These modules could be triggered at key moments in the user journey, such as when setting up a new account or making a transaction.
    - **Just In Time Interventions:** Implement real-time warnings that alert users to potential red flags when engaging in risky online activities. These alerts should be context-specific and provide concise explanations of the manipulation tactics being employed. For instance, if a user receives a message containing a shortened link or a request for personal information, an alert could pop up explaining the potential risks.
2. **Context-Specific Interventions:** The effectiveness of inoculation interventions can be further enhanced by tailoring them to specific contexts, platforms, and demographics.
    - **Platform Specificity:** Design interventions tailored to the specific platform where scams are prevalent. E-commerce sites could incorporate scam prevention modules during checkout, while social media platforms could provide tailored tips based on users' interaction patterns or offer warnings about suspicious profiles or messages.
    - **Demographic Targeting:** Customize interventions based on user demographics, literacy levels, and risk profiles.
3. **Gamification for Enhanced Engagement:** ShieldUp!'s success highlights the value of gamified learning. Some best practices

learnt from this experiment indicate that future efforts could benefit from incorporating design elements such as interactive narratives, effective sound design, reward mechanisms, cognitive scaffolding and active recall based quizzes to enhance user engagement and longer term knowledge retention.

Policy Recommendations

1. **Promote Digital Literacy and Scam Prevention Education:** Policymakers can play a vital role in fostering a safer digital environment.
    - **Curriculum Integration:** Integrate digital literacy and scam prevention education into school curricula at all levels.
    - **Public Awareness Campaigns:** Develop targeted public awareness campaigns using various channels to disseminate information about common scam tactics and prevention strategies.
    - **Financial Literacy Programs:** Incorporate scam prevention education into financial literacy programs to help individuals understand the link between financial knowledge and scam susceptibility.
2. **Support Research and Evaluation:** Continued research is crucial. This includes investing in data collection and analysis to understand scam trends and evaluating intervention effectiveness. Further research should focus on developing and refining scam prevention strategies, particularly those addressing the psychological aspects of scam susceptibility.

Future Research Directions

1. **Longitudinal Studies:** Conducting longer time horizon (1-3 months) longitudinal studies can provide insights into the long-term effectiveness of interventions like ShieldUp! and determine whether booster interventions are needed to maintain heightened scam identification over time.
2. **Cross-Cultural Adaptations:** Given the global nature of online scams, adapting ShieldUp! and similar interventions for diverse cultural and linguistic contexts is essential. Research should explore how to tailor game narratives, characters, and scenarios to resonate with different cultural values and beliefs.

3. **Personalized Interventions:** To maximize effectiveness, future research should explore the development of personalized scam prevention interventions that take into account individual user characteristics, such as cognitive abilities, learning styles, risk preferences, and previous experience with scams. Personalized interventions can improve effectiveness by accounting for individual needs [DeLiema et al., 2024].

The exploration of personalized interventions holds great promise for optimizing scam prevention efforts. By tailoring interventions to individual needs and learning styles, we can potentially maximize their effectiveness and impact.

Conclusion

Traditional awareness campaigns, while important, often fail to equip users with the skills and knowledge needed to effectively identify and avoid sophisticated scam tactics. This case study presents ShieldUp!, a mobile game prototype developed specifically for the Indian market, leveraging the principles of inoculation theory to provide users with a fun, engaging, and effective way to learn about online scams. By simulating real-world scenarios, gradually increasing difficulty, and explicitly teaching manipulation tactics, we can empowers users to develop cognitive resistance and make safer choices online.

Our pilot study findings provide promising evidence that a game-based inoculation approach can significantly improve scam identification and potentially mitigate the growing threat of online scams. The observed improvements in scam identification, coupled with the dissipation of increased skepticism towards genuine offers over time, suggest that ShieldUp! can enhance user resilience without fostering undue distrust in legitimate online interactions. By embracing a proactive, evidence-based approach and fostering a culture of digital literacy and critical thinking, we can create a safer and more trustworthy digital world for everyone.

References

[Ncs,] National cyber security centre uk. https://www.ncsc.gov.uk/. Accessed: 2024-10-15.

[Ncp,] Ncpi fraud awareness program. https://www.npci.org.in/npci-in-news/knowledge-centre/fraud-awareness. Accessed: 2024-10-15.

[Sca,] ScamShield website. https://scamshield.gov.sg/. Accessed: 2024-10-15.

[Sca, 2024] (2024). Scamwatch australia. https://www.scamwatch.gov.au/. Accessed: 2024-10-15.

[Ariely and Zakay, 2001] Ariely, D. and Zakay, D. (2001). A timely account of the role of duration in decision making. *Acta Psychol. (Amst.)*, 108(2):187–207.

[Breuer and Bente, 2010] Breuer, J. S. and Bente, G. (2010). Why so serious? on the relation of serious games and learning. *Eludamos: Journal for Computer Game Culture*, 4(1):7–24.

[Bullee and Junger, 2020] Bullee, J.-W. and Junger, M. (2020). How effective are social engineering interventions? a meta-analysis. *Information and Computer Security*, ahead-of-print(ahead-of-print).

[Burke et al., 2022] Burke, J., Kieffer, C., Mottola, G., and Perez-Arce, F. (2022). Can educational interventions reduce susceptibility to financial fraud? *J. Econ. Behav. Organ.*, 198:250–266.

[Chadha, 2022] Chadha, S. (2022). Inside google marketing: How we mobilized an industry-wide alliance in india to keep people safe online. https://www.thinkwithgoogle.com/intl/en-apac/future-of-marketing/management-and-culture/raising-cybersecurity-awareness-india/. Accessed: 2024-10-15.

[Christiano and Neimand, 2017] Christiano, A. and Neimand, A. (2017). Stop raising awareness already.

[Chugh and Narang, 2023] Chugh, B. and Narang, L. (2023). Are fraud awareness campaigns effective. Technical report, Dvara Research.

[Cialdini, 1984] Cialdini, R. (1984). Influence: Science and practice.

[Cialdini et al., 1999] Cialdini, R. B., Wosinska, W., Barrett, D. W., Butner, J., and Gornik-Durose, M. (1999). Compliance with a request in two cultures: The differential influence of social proof and commitment/consistency on collectivists and individualists. *Pers. Soc. Psychol. Bull.*, 25(10):1242–1253.

[Compton and Pfau, 2005] Compton, J. A. and Pfau, M. W. (2005). Inoculation theory of resistance to influence at maturity: Recent progress in theory development and application and suggestions for future research. *Communication yearbook 29*.

[DeLiema et al., 2024] DeLiema, M., Robb, C. A., and Wendel, S. (2024). What *does* trust *have* to do with it? training consumers to detect digital imposter scams. *J. Financ. Crime*.

[Dixit, 2023] Dixit, P. (2023). An average indian gets 12 fake messages daily and these are the most common ones they fall prey to: Study. https://www.businesstoday.in/technology/news/story/an-average-indian-gets-12-fake-messages-daily-and-these-are-the-most-common-ones-they-fall-prey-to-study-405067-2023-11-08. Accessed: 2024-10-14.

[Freedman and Fraser, 1966] Freedman, J. L. and Fraser, S. C. (1966). Compliance without pressure: the foot-in-the-door technique. *J. Pers. Soc. Psychol.*, 4(2):195–202.

[Hoechsmann et al., 2016] Hoechsmann, M., DeWaard, H., and Lakehead University / MediaSMarts (2016). MAPPING DIGITAL LITERACY POLICY AND PRACTICE IN THE CANADIAN EDUCATION LANDSCAPE.

[Hu et al., 2023] Hu, B., Ju, X.-D., Liu, H.-H., Wu, H.-Q., Bi, C., and Lu, C. (2023). Game-based inoculation versus graphic-based inoculation to combat misinformation: a randomized controlled trial. *Cogn Res Princ Implic*, 8(1):49.

[Jones et al., 2023] Jones, L. M., Mitchell, K. J., and Beseler, C. L. (2023). The impact of youth digital citizenship education: Insights from a cluster randomized controlled trial outcome evaluation of the be internet awesome (BIA) curriculum. *Contemp School Psychol*, pages 1–15.

[Kubilay et al., 2023] Kubilay, E., Raiber, E., Spantig, L., Cahlíková, J., and Kaaria, L. (2023). Can you spot a scam? measuring and improving scam identification ability. *SSRN Electron. J.*

[Loewenstein et al., 2001] Loewenstein, G. F., Weber, E. U., Hsee, C. K., and Welch, N. (2001). Risk as feelings. *Psychol. Bull.*, 127(2):267–286.

[Lusardi and Mitchell, 2014] Lusardi, A. and Mitchell, O. S. (2014). The economic importance of financial literacy: Theory and evidence. *J. Econ. Lit.*, 52(1):5–44.

[McGuire, 1961] McGuire, W. J. (1961). The effectiveness of supportive and refutational defenses in immunizing and restoring beliefs against persuasion. *Sociometry*, 24(2):184–197.

[McPhedran et al., 2023] McPhedran, R., Ratajczak, M., Mawby, M., King, E., Yang, Y., and Gold, N. (2023). Psychological inoculation protects against the social media infodemic. *Sci. Rep.*, 13(1):5780.

[Milgram, 1965] Milgram, S. (1965). Some conditions of obedience and disobedience to authority. *Hum. Relat.*, 18(1):57–76.

[Miller, 1983] Miller, J. D. (1983). Scientific literacy: A conceptual and empirical review. *Daedalus*, 112(2):29–48.

[Petty, 1977] Petty, R. E. A. D. (1977). *A COGNITIVE RESPONSE ANALYSIS OF THE TEMPORAL PERSISTENCE OF ATTITUDE CHANGES INDUCED BY PERSUASIVE COMMUNICATIONS*. PhD thesis.

[Pfau et al., 1992] Pfau, M., Van Bockern, S., and Kang, J. G. (1992). Use of inoculation to promote resistance to smoking initiation among adolescents. *Commun. Monogr.*, 59(3):213–230.

[Prenzler, 2019] Prenzler, T. (2019). What works in fraud prevention: a review of real-world intervention projects. *Journal of Criminological Research, Policy and Practice*, 6(1):83–96.

[Rahman et al., 2023] Rahman, N. A. A., Chong, C. C., and Hisham, R. R. I. R. (2023). Money mule scams: Patterns of involvement and awareness campaign. In *The European Proceedings of Social and Behavioural Sciences*, volume 132, pages 802–808. European Publisher.

[Rao, 2023] Rao, A. K. (2023). People in india are exposed to nearly 12 fake messages daily, reveals McAfee's scam message study. `https://www.thefinancialworld.com/people-in-india-are-exposed-to-nearly-12-fake-messages-daily-reveals-mcafees-scam-message-study/`. Accessed: 2024-10-14.

[Robb and Wendel, 2023] Robb, C. A. and Wendel, S. (2023). Who can you trust? assessing vulnerability to digital imposter scams. *J Consum Policy (Dordr)*, 46(1):27–51.

[Roozenbeek and van der Linden, 2019] Roozenbeek, J. and van der Linden, S. (2019). Fake news game confers psychological resistance against online misinformation. *Palgrave Communications*, 5(1):1–10.

[Saleh et al., 2023] Saleh, N., Makki, F., van der Linden, S., and Roozenbeek, J. (2023). Inoculating against extremist persuasion techniques – results from a randomised controlled trial in post-conflict areas in iraq. *adv.in/psych*, 1(1).

[Schwartz, 1977] Schwartz, S. H. (1977). Normative influences on altruism. In *Advances in Experimental Social Psychology*, volume 10 of *Advances in experimental social psychology*, pages 221–279. Elsevier.

[Singh, 2023] Singh, B. (2023). A fifth of urban indians claim they have lost money due to a scam. `https://business.yougov.com/content/48051-a-fifth-of-urban-indians-claim-they-have-lost-money-due-to-a-scam`. Accessed: 2024-10-14.

[Singh, 2024] Singh, R. (2024). Here is how much indians lost to cyber frauds between jan and apr of 2024. `https://www.business-standard.com/india-news/here-is-how-much-indians-lost-to-cyber-frauds-between-jan-and-apr-of-2024-124052700151_1.html`. Accessed: 2024-10-14.

[Slovic et al., 2007] Slovic, P., Finucane, M. L., Peters, E., and MacGregor, D. G. (2007). The affect heuristic. *Eur. J. Oper. Res.*, 177(3):1333–1352.

[Titus et al., 1995] Titus, R. M., Heinzelmann, F., and Boyle, J. M. (1995). Victimization of persons by fraud. *Crime Delinq.*, 41(1):54–72.

[Tripathi, 2024] Tripathi, R. (2024). Indians lost over inr 1,750 crore to cyber fraud in first four months of 2024. https://economictimes.indiatimes.com/news/india/indians-lost-over-1750-crore-to-cyber-fraud-in-first-four-months-of-2024/articleshow/110444616.cms. Accessed: 2024-10-14.

Appendices

Appendix A: Thematic Analysis of Victim User Journeys

Table 1: Search Strategy and Results for Scam User Journey Artifacts

Scam Type	Search Keywords	Stories Analyzed	Example Story Link
Courier Scams	(“courier” OR “parcel” OR “fedex”) AND “scam” AND “india”	5	https://tinyurl.com/fedex-scam-story
Customer Care Scams	(“customer care” OR “refund”) AND “scam” AND “india”	5	https://tinyurl.com/customer-care-scam-story
Jobs Scams	(“jobs” OR “recruitment”) AND “scam” AND “india”	5	https://tinyurl.com/jobs-scam-story
Friends/Family Impersonation Scams	(“friend” OR “family” OR “impersonat*”) AND “scam” AND “india”	3	https://tinyurl.com/friends-scam-story
Online Shopping & P2P Marketplace Scams	((“shopping” AND “online”) OR (“olx” OR “facebook marketplace” OR “quickr”)) AND “scam” AND “india”	3	https://tinyurl.com/marketplace-scam-story
Crypto/Investment Scams	“online” AND (“investment” OR “crypto” OR “cryptocurrency”) AND “scam” AND “india”	4	https://tinyurl.com/inv-scam-story
Loan Scams	("loan" OR "quick loan" OR "payday") AND ("scam" OR "fraud") AND "india"	4	https://tinyurl.com/loan-scam-story
Other UPI Scams	("qr code scam" OR "upi pin scam" OR "fake payment" OR "money transfer scam") AND "upi" AND "india"	2	https://tinyurl.com/upi-scam-story
Total		**31**	

Appendix B: Safety Tips Infographic for the Active Control Group

Safety Tips for Online Transaction per RBI

	DOs	DON'Ts
General Precautions	✅ Check for a **secure payment gateway** (https:// - URL with a padlock symbol) before making online payments / transactions. ✅ Turn on **two-factor authentication** where such facility is available.	❌ Do not share **confidential financial information** (PIN, password, debit or credit card number, CVV etc.) with banks/ financial institutions, friends or even family members. ❌ Avoid **saving card details** on websites / devices / public laptop / desktops.
Device / Computer Security	✅ Change passwords at **regular intervals.** ✅ Install **antivirus** on your devices and install updates whenever available. ✅ Always **scan unknown Universal Serial Bus (USB) drives / devices** before usage.	❌ Do not leave your **device unlocked.** ❌ Do not install any **unknown applications or software** on your phone / laptop. ❌ Do not **store passwords or confidential information** on devices.
Safe Online Banking	✅ Always use **virtual keyboard** on public devices since the keystrokes can also be captured through compromised devices, keyboard, etc. ✅ **Log out** of the internet banking session immediately after usage.	❌ Do not use **same passwords** for your email and internet banking. ❌ Avoid using **public terminals** (viz. cyber cafe, etc.) for financial transactions.
Email and Password Security	✅ Use a **combination of alphanumeric and special characters** in your password.	❌ Do not click on **links sent from unknown addresses / names.** ❌ Avoid opening emails on **public or free networks.**

Reference: Office of RBI Ombudsman. "BE(A)WARE: A Booklet on Modus Operandi of Financial Fraudsters". Reserve Bank of India. https://rbi.org.in/commonman/english/Scripts/BEAWARE.aspx