Improving Mobile Security with Visual Trust Indicators for Smishing Detection

Narges Zare, Cori Faklaris, Sarah Tabassum, Heather Richter Lipford

Department of Software and Information Systems, College of Computing and Informatics

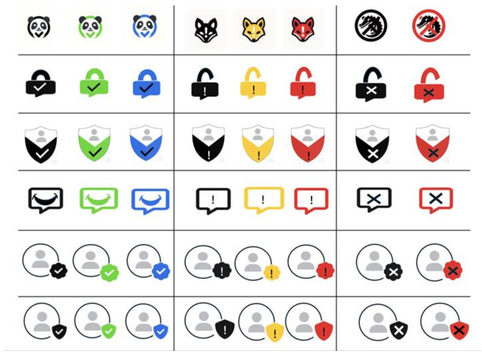
Introduction

Smishing (SMS phishing) scams are on the rise, tricking users into revealing sensitive data. Most people struggle to recognize these attacks especially on mobile devices with small screens and frequent alerts. This study focuses on **what makes mobile security icons intuitive** and **whether icons or tooltips better help users detect smishing**.

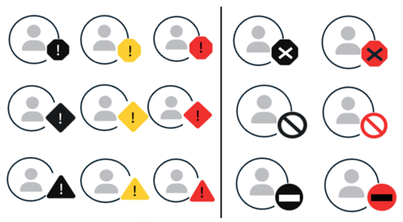
Design Process

We reviewed trust and warning icons used across platforms.

Inspired by color psychology and interface design principles, we designed **visual trust indicators** to help users make safer decisions when reading mobile messages.



Main Sets of Icons



Alternative Icons

User Evaluation

We conducted a qualitative study with 30 adult participants (ages 18–64) to explore how people interpret and use visual trust indicators in mobile messaging.

Study Format:

❖ In-person, 30–45 min sessions

❖ Activities included:

- **Pre-Survey:** Messaging habits & security concerns
- **Icon Review**: Each participant reviewed 3 random rows from the main icon sets
- **Prototype Test**: Interactive prototype session
- **Final Icon Selection**: Full icon set review + optional alternatives (16 participants)
- **Post-Survey:** Confidence and security feedback

Results

Top Selected Icons

Participants' Color, Symbol, and Icon Insights:

🟢 Green icons with ✓ ⟶ Safety, Trust

🟡 Yellow icons with ! ⟶ caution, Attention

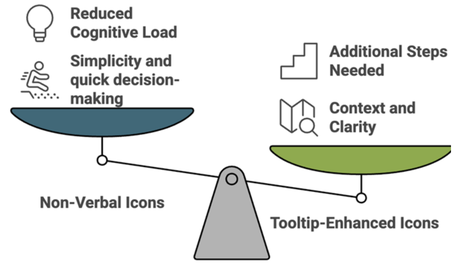
🔴 Red icons with X ⟶ Danger, Prohibition

- Non-verbal icons preferred for speed
- Tooltips added value, especially for fraud detection
- Clear color + familiar shapes improved recognition

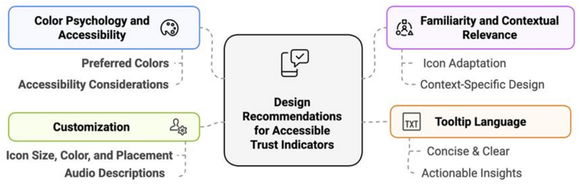
Discussion

Key Insights:

- Users favored **icons that mirrored real-world signs** (e.g., traffic signs) and **UI conventions from social apps** (e.g., verified badges).
- Inconsistent visual signals across apps caused confusion. Standardizing trust indicators could improve recognition and reduce risk.
- **Non-verbal icons** enabled rapid recognition. **Tooltips** were especially helpful when icons alone weren't clear, but vague wording (e.g., "likely safe") undermined confidence.



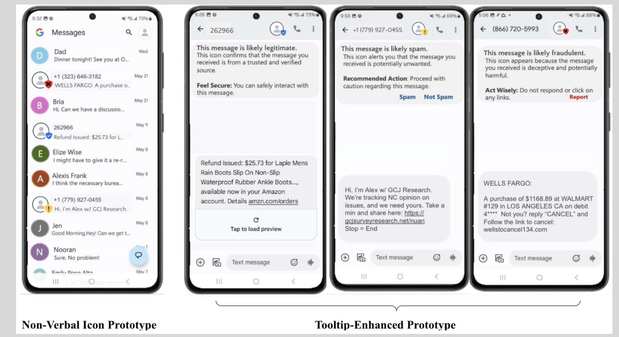
Design Recommendations:



*Four key areas—**color accessibility, contextual relevance, customization, and tooltip clarity**—guide the creation of trust indicators that are intuitive, inclusive, and effective across diverse users.*

Broader Impact:

Protecting users from fraudulent SMS also strengthens **IoT** security, as smartphones are the gateways to IoT devices. These trust indicators can also apply to **finance**, **healthcare**, and other contexts requiring quick trust decisions.



Trust indicators shown in mobile messages.

Future Work

- Conduct field studies and A/B tests to evaluate trust indicators in messaging apps.
- Measure how effectively these icons support decision-making, especially during everyday distractions.
- Explore new ways to improve security communication as smartphones evolve into IoT hubs.

Full Paper

https://spexlab.org/files/AIIOT2025_indicators.pdf

Acknowledgements

This research was supported by the NSF IU/CRC Center for Cybersecurity Analytics and Automation, award #1822150.