Title: Improving Mobile Security with Visual Trust Indicators for Smishing Detection

Authors: Narges Zare, Cori Faklaris, Sarah Tabassum, and Heather Richter Lipford *(University of North Carolina at Charlotte)*

Venue: 2025 IEEE 6th Annual World AI IoT Congress (IEEE AIIoT)

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

This paper has been **peer-reviewed and accepted** for publication at the *2025 IEEE 6th Annual World AI IoT Congress (IEEE AIIoT)*. It will appear in the IEEE Xplore Digital Library upon official release. (*Acceptance confirmation shown below.)*

Abstract: Smishing (SMS phishing) is a growing cyber threat that exploits user trust in text messages. Many users struggle to distinguish between legitimate and fraudulent messages, increasing their risk. To address this problem, we researched and developed options for visual trust indicators that can be displayed to guide mobile phone users in judging messages. We evaluated the indicator options with 30 participants. Participants preferred intuitive, color-coded icons, especially when familiar and contextually clear. Non-verbal icons enabled low-effort recognition, while tooltips were valuable when they provided clear, actionable options like one-click reporting. Profile with shield icons and triangle road signs were most effective. Our findings highlight how visual indicators enhance user security and confidence, while also supporting more informed decision-making. We recommend accessible and customizable designs that align with user expectations. These insights have broader relevance for improving mobile messaging and securing IoT environments where compromised phones can trigger downstream risks.

Future Work: To build on our findings, future research will evaluate these trust icons in real-world settings where people naturally receive messages. We plan to conduct field studies and A/B tests within messaging apps to observe how users interact with icons during everyday routines, rather than in controlled environments. This will help determine whether visual cues—such as color-coded icons—effectively assist users in recognizing spam, scams, or legitimate messages, especially when distracted or multitasking. A key question is whether trust indicators improve users' ability to make informed safety decisions in high-pressure scenarios. Future work may also explore similar indicators in other domains like finance, health, or smart devices. As smartphones increasingly act as hubs for IoT devices, clearly communicating security threats is more critical than ever.

Screenshot from EDAS showing accepted status for IEEE AIIoT 2025.