T1: Scambaiting Community Studies

Methods

- Interview studies with scambaiters
- Controlled observational studies of live ISE attack engagements
- Passive analysis of coordination platform data
- Co-design workshops for tooling

Expected Results

- Taxonomy and behavioral models of ISE attacks
- Real-world scambaiting setups and workflows
- Design blueprint for a general-purpose scambaiting tool
- Grounded insights to inform automated defenses

T2: Automated ISE Attack Engagement

System Development

- Verbal agent for real-time scam conversations
- Action agent to perform scammer-directed tasks
- Infrastructure: VMs, VOIP, voice synthesis, fake banking interfaces

Goals

- Build and evaluate an autonomous ISE engagement pipeline
- Collect fine-grained, attacker-driven multi-modal data
- A deployable tool that can waste scammer time

EDU: Education Against ISE attacks

Methods

- Interactive multi-modal simulation tool leveraging real-world ISE attack data
- Evaluation via summer workshops for older adults
- Short-form educational video development
- Dissemination through law enforcement and AARP

Expected Results

- Effective education tool for ISE attack awareness
- Extensible framework to adapt to future ISE attacks
- Broader public access to in-depth ISE attack knowledge

T3: Detecting ISE Attacks

Methods

- Fine-tuning LLMs on ISE transcripts
- Audio signal analysis
- Behavioral analysis of system and network events
- Brand-specific allowlist construction

Expected Results

- Deployable, multi-modal defensive tools for real-time ISE mitigation
- Early-stage detection of ISE attacks across modalities