A Framework for Reasoning about Social Influences on Security and Privacy Adoption

Cori Faklaris, University of North Carolina at Charlotte
Laura Dabbish and **Jason I. Hong**, Carnegie Mellon University

CHI 2024
Surfing the World

SUMMARY

Many usable security solutions exist (such as using password managers or reporting phishing scams), but people often are not fully aware of what they do or use them regularly. A **conceptual model** of the adoption process will help us to **identify where people get stuck** and **how to leverage social influences** to encourage secure behaviors. We will be able to **form and test hypotheses** and improve our designs.

Toward this goal, we have developed a framework that synthesizes our design ideation, expertise, prior work, and new interview data (*N*=17) into a **six-step adoption process** with path relationships (**Figure 1**), associated social influences, and obstacles (**Table 1**).

This work contributes a prototype framework that accounts for social influences by step. It adds to what is known in the literature and the SIGCHI community about the **social-psychological drivers of security adoption**.

Future work should establish whether this process is the same regardless of **culture**, **demographic variation**, or **work vs. home** context, and whether it is a reliable theoretical basis and method for **designing experiments** and **focusing efforts** where they are likely to be most productive.

KEY CONCEPTS

Process Models of Behavior: These account for the progress of time, roughly following the Lewin Change Model of "unfreeze," "move," and "refreeze", as people reason about what actions they should take and continue taking. While the process they describe is continuous, the segmentation of the process into stages helps describe people's journey and distinguish the characteristics of one point in time from another. Other relevant models for security and privacy include *Protection Motivation Theory* and *Innovation-Diffusion Theory*.

Usable Security Practices: Methods of either dealing with or preventing a security and privacy concern, whether cyber/virtual or physical, that are simple to use, useful, and satisfying. These can be categorized as (1) using strong and unique authentication, (2) staying alert for phishing, scams and misinformation, (3) keeping systems up to date; and (4) securing devices.

LEARN MORE

Go to https://corifaklaris.com for a copy of this short paper or scan this QR code.

FRAMEWORK RESULTING FROM OUR RESEARCH

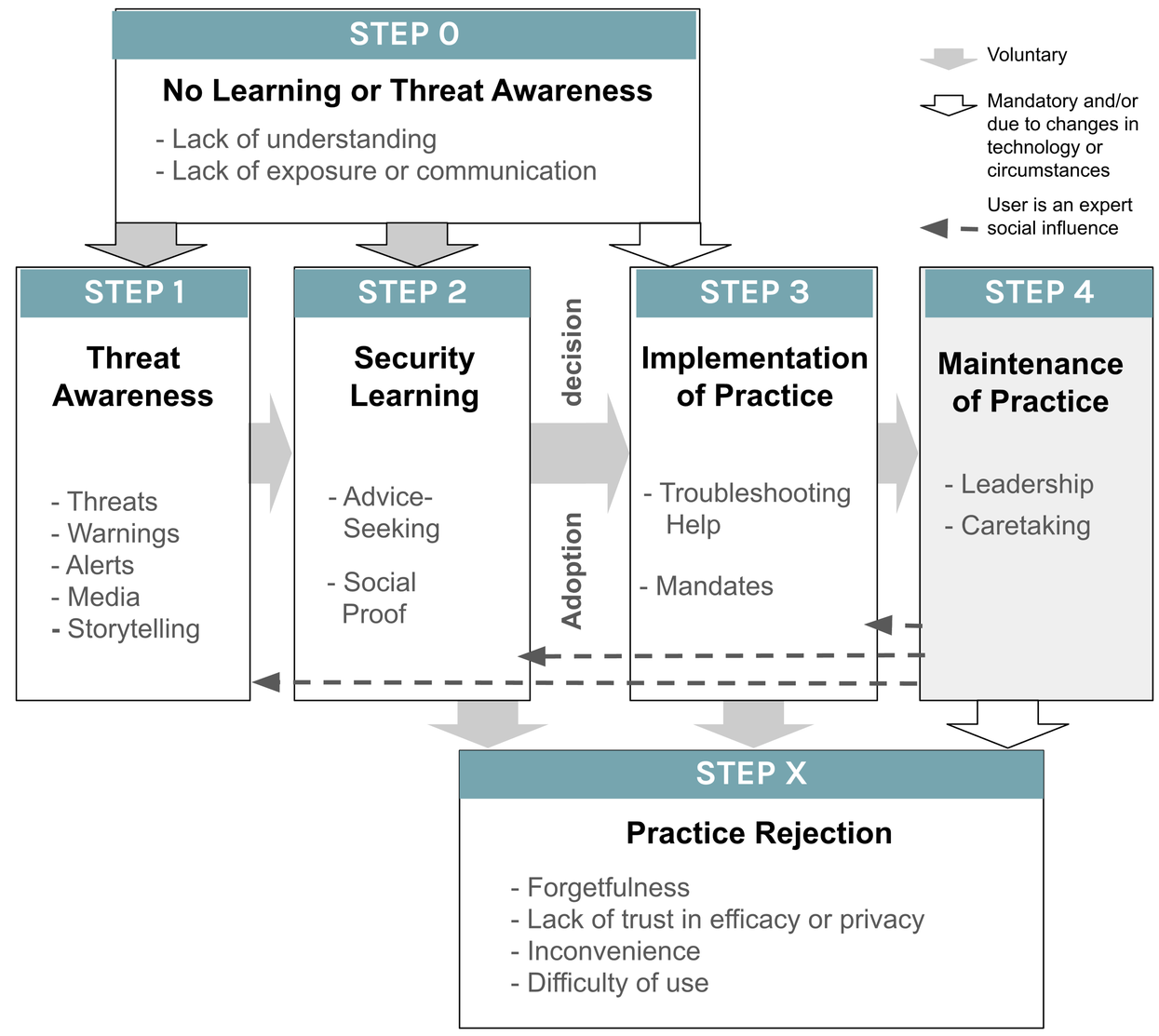

Figure 1: People start at Step 0, then move to either Steps 1, 2, or 3 based on messaging and mandates.

Table 1: How to identify a person's step, and which social influences and obstacles are associated with each.

Step	Description	Associated Social Influences	Obstacle(s) to Moving Forward
No Learning or Threat Awareness (Step 0)	- Lack of understanding about a recommended security practice or the importance of guarding against the specific threats it protects against. - Examples: No knowledge of where to go for advice, ignorance that software updates are for security.	- No person or source to help them with security. - No authority mandating training.	- Cultural differences. - Fear of creating tech headaches. - Lack of interest.
Threat Awareness (Step 1)	- Mention of threat, risk, harm, or potential harm; perception that event has implications for security. - Examples: Receiving a threatening email, reacting to media, suspecting your smartphone was hacked.	- Threats. - Warnings. - Media. - Storytelling.	- No awareness of a given security practice or other technology.
Security Learning (Step 2)	- Knowledge of existence of a given security practice or other technology, but no enactment. - Examples: Hearing about secure messaging, finding out how to verify a post, being told to update.	- Advice-seeking. - Social proof.	- Not feeling threat (skipped Step 1). - Rejecting adoption before it is tried.
Security Practice Implementation (Step 3)	- Acting to test the security practice to evaluate its usefulness; acting to put the decision into effect. - Examples: Using a trial offer, playing around with a practice; acquiescing to a policy.	- Troubleshooting help. - Mandates.	- Discontinuing adoption after the practice has been used at least once.
Security Practice Maintenance (Step 4)	- Acting to finalize the decision to use a practice; expanding use; mention of past implementation. - Examples: Stepping up frequency of use; making statements like "I still use this" or "I currently use it."	- Leadership. - Caretaking.	- The context becomes obsolete. - Waning effectiveness.
Security Practice Rejection (Step X)	- Either discontinuing adoption of a security practice or deciding not to implement the security practice. - Examples: Stopping after a few uses; making statements like "It felt like overkill" or "Effort is too much for the benefit."	- Receiving advice not to use it. - Lack of help with troubleshooting. - Lack of mandates.	- Forgetfulness. - Lack of trust in efficacy or privacy. - Inconvenience - Difficulty of use.