Understanding and Supporting Information Privacy/Security Behaviors
Faculty supervisor: Florian Schaub

Why do people fall prey to phishing attacks and identity theft? Why do we have to rely on passwords? Why are people concerned about privacy yet share lots of personal information on social media or with companies by using their services and devices? The Security Privacy Interaction lab (spilab), directed by UMSI Assistant Professor Florian Schaub, conducts research to understand individuals’ decisions and behavior with respect to privacy and security. We further design, build and evaluate usable privacy and security mechanisms that help individuals make better privacy and security decisions without getting in the way of their primary activities.

We conduct mixed-methods research and combine user studies with user experience design and the design of privacy-friendly and secure systems. Interested candidates should either have experience in HCI with an interest in privacy/security, or experience in privacy/security with an interest in HCI. Technical and programming experience is a plus.

We’re looking for highly motivated students to work with us on the following projects:

- **Nudging People Towards Protective Action After a Data Breach**
  Data breaches pose substantial risks to affected individuals, including identity theft and financial loss. Yet, many people do not take protective or remedial action when they become the victim of a data breach. This project investigates what prevents people from taking action and, in particular, the role of data breach notifications in this process. Under the mentorship of UMSI assistant professor Florian Schaub, the student will conduct a mixed-method user study to identify patterns and issues with data breach notifications that affect people’s understanding of the data breach and available recovery options. The findings will provide insights for improving communication after a data breach occurs and, depending on the students’ interest, could be complemented with the design and evaluation of enhanced user experiences.

- **Intuitive Privacy Controls for Smart Speakers**
  Smart speakers, such as Amazon Echo, require a live microphone that continuously listens for activation keywords and commands. Based on prior work in Prof. Schaub’s group, this project will contribute to the design of intuitive smart speaker privacy controls that leverage additional context cues to determine when the microphone is needed and can be switched off otherwise. The student is expected to build prototypes with Raspberry Pi and Arduino and carry out a field study to evaluate the privacy control’s effectiveness and usability. Programming experience is required.

- **Understanding Privacy Needs and Behaviors of At-Risk Populations**
  Privacy needs and concerns are personal and contextual, yet many privacy settings and options are generic. Through semi-structured interviews and potentially surveys, this project will study technology-related privacy needs and behaviors of individuals with an objectively higher privacy risk, due to their status, background or past experience. The goal of this study is to understand needs of a specific at-risk population in order to inform the design of tailored support and interventions. At-risk populations Prof. Schaub’s group has worked with include undocumented immigrants, older adults, and sex workers. Prof.
Schaub and the student will define this study’s specific focus and research questions together.

- **Managing Information Needs and Privacy in Memory Work**
  Memory workers are human rights advocates who raise public awareness about past regimes’ human rights violations. Such memory work contributes to reconciliation and accountability in post-conflict societies. The information gathered by memory workers is often at risk of being destroyed, hidden, or breached. The goal of this qualitative research study is to gain a deeper understanding of information management practices among memory workers, in particular their strategies and approaches for managing and protecting information about victims and survivors of human rights violations.

- **Designing Effective Phishing Warnings**
  Phishing emails often disguise a link's actual URL. Thus, common anti-phishing advice is to check a link's URL before clicking, but email clients do not support this well. Automated phishing detection enables email clients to warn users that an email is suspicious, but current warnings are often not specific. In prior work, we showed that moving phishing warnings close to the suspicious link in an email is effective at reducing phishing susceptibility. This project aims to conduct a field experiment to investigate in more detail the effects of exposing a link’s URL for preventing users from clicking on phishing links. The student is expected to contribute to planning and conducting the experiment, and is expected to design phishing warnings and implement them for the study. Web development experience is required.