Abstract Deutsch

Heutzutage ist es möglich, mit web-basierten Lösungen Texte zu editieren, Filme anzusehen, oder seine persönlichen Finanzen zu verwalten. Die Anbieter müssen hierbei Sicherheit und Vertraulichkeit von Nutzerdaten sicherstellen. Dazu sind Passwörter weiterhin die geläufigste Authentifizierungsmethode im Internet. Sie sind kostengünstig und einfach zu implementieren. NutzerInnen sind bereits im Umgang mit diesem Verfahren vertraut jedoch stellen Passwörter ein beträchtliches Ärgernis dar, weil sie mühsam zu erstellen, einzuprägen, und verwalten sind. Oft werden Usabilityfragen zu Sicherheitsproblemen, weil NutzerInnen Herausforderungen umschiffen und sich einfach zu erratende Zugangsdaten ausdenken. Daneben verwenden sie Passwörter für viele Zwecke wieder, was das Risiko eines Identitätsdiebstals weiter erhöht. Es gibt zahlreiche Versuche die Wurzel des Problems zu beseitigen und Passwörter zu ersetzen, z.B. mit Biometrie. Jedoch kann bisher kein anderes Verfahren sie vollkommen ersetzen, so dass Passwörter wohl für absehbare Zeit die Hauptauthentifizierungsmethode bleiben werden.

ExpertInnen aus Forschung und Industrie haben sich deshalb zum Ziel gefasst, die Situation der NutzerInnen auf verschiedene Wege zu verbessern. Es existieren zwei Forschungsstränge darüber wie man NutzerInnen bei der Erstellung von sicheren und benutzbaren Passwörtern helfen kann. Auf der einen Seite haben Regeln bei der Passworterstellung deutliche Auswirkungen auf Passwortpraktiken, weil sie bestimmte Charakteristiken durchsetzen. Jedoch reduziert diese Durchsetzung die Autonomie der NutzerInnen und verursacht Frustration, wenn die Anforderungen schlecht kommuniziert oder übermäßig komplex sind. Auf der anderen Seite stehen nutzerzentrierte Designs: Hilfestellung und Überzeugungsarbeit sind typischerweise nutzerfreundlicher wobei ihr Einfluss begrenzt ist. In dieser Arbeit erkunden wir die potenziellen Gründe für die Ineffektivität bestimmter Überzeugungsstrategien. Von dem hierbei gewonnenen Wissen leiten wir neue persuasive Designelemente für Hilfestellung bei der Passwortauthentifizierung ab.

Die Exploration von Kontextfaktoren im Umgang mit Passwörtern basiert auf vier Projekten, die sowohl psychologische Aspekte als auch Einschränkungen in der Praxis aufdecken. Hierbei untersuchen wir inwiefern Mental Modelle von Passwortstärke und -managern wichtige Hinweise auf das Design von persuasiven Interventionen liefern. Darüber hinaus werden die Zusammenhänge zwischen Persönlichkeitsmerkmalen und Passwortpraktiken in drei Nutzerstudien untersucht. Eine gründliche Überprüfung von Passwortregeln in der Praxis zeigt die Einschränkungen für Passwortselektion und -wiederverwendung.

Basierend auf der Durchleuchtung der Kontextfaktoren erweitern wir hierauf den Design-Raum von persuasiver Passworthilfestellung mit drei Projekten. Zuerst schildern wir die expliziten und impliziten Bedürfnisse in punkto Hilfestellung. Daraufhin erstellen und evaluieren wir eine Entscheidungsarchitektur, welche veranschaulicht wie ein Marketingphänomen neue Einsichten in das Design von Nudging-Strategien liefern kann. Im Schlussgang versuchen wir NutzerInnen dabei zu stärken, gut merkbare Passwörter mit Hilfe von Emojis zu erstellen. Die Ergebnisse zeigen die Herausforderungen und Potenziale von Emoji-Passwörtern auf verschiedenen Plattformen.

Zuletzt präsentiert diese Arbeit ein Rahmenkonzept für das persuasive Design von Passworthilfestellungen. Es soll die benötigten Aktivitäten während des gesamten Prozesses strukturieren. Dies erlaubt ExpertInnen neuartige Systeme zu entwickeln, die über traditionelle Ansätze hinausgehen, was durch eine Designstudie veranschaulicht wird.