Karlsruhe Institute of Technology

Institute of Applied Informatics
and Formal Description Methods
Prof. Dr. Melanie Volkamer

Addressing Misconceptions About Password Security Effectively*

Peter Mayer, Melanie Volkamer

Problem

- Users want to behave securely, but face problems handling, choosing, or remembering passwords
- To mitigate problems, users develop coping strategies
- When coping strategies are based on misconceptions intention to behave securely is – unbeknownst to the users – compromised

Approach

Step 1: Identification of misconceptions about password security in the literature

Step 2: Development of interventions including round of expert feedback

Step 3: Evaluation of interventions in three small and medium sized enterprises

Step 4: Proposal of refined version of the interventions based on evaluation findings

Step 1: Identification of Misconceptions

Method

- Systematic literature review of publications since 2007
- Search terms developed with consultation of native english-speaking experts

Results

- 20 relevant publications
- Identification of 23 misconceptions
- Wide range of topics

Misconceptions about password security																						
Composition					Handling						Attacks								Miscellaneous			
M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23
Including numbers makes passwords automatically more secure	Including symbols makes passwords automatically more secure	Including uppercase letters makes passwords automatically more secure	Common substitutions (e.g. a → @) make passwords more secure	Words from other languages make passwords more secure	Reusing is OK for secure passwords, but should be avoided for weak passwords	Reusing is OK for more frequently used passwords	Reusing passwords is better than writing them down	Notes of passwords do not need to be particularly protected	Passwords have to be changed frequently	Storing passwords in the browser does not mean one is using a password manager	Keyboard patterns are secure passwords	Using dates of birth that are not my own makes passwords more secure	Attackers do not automate their attacks, but perform them by hand	Attackers are strangers which are (geographically) far away	Attackers are only people the users know	Email is security-wise not an important service	A SIM-PIN is sufficient to protect the data on a smartphone from unauthorized access	It is not necessary to lock the screen of unattended devices	Work accounts have lower security requirements - the IT staff is responsible	The frequency of use of an account is related to its security	Bank accounts are of low value if there is no money in them	It is possible to be too unimportant to be targeted

Step 2: Development of Interventions

Initial Development

- Development of text based interventions
- Explanations of misconceptions and, where it is relevant and underlying problem
- Wording iteratively improved with feedback from information security and psychology experts as well as lay-users

Round of Structured Expert Feedback

- Contacted 30 information security experts
- 13 responded: researchers, consultants, IT staff, and developers of security solutions
- Feedback: visual representation wanted

Using walks or patterns on your keyboard as password (e. g. "1q2w3e4r") is no good practice to generate secure passwords. While they may seem random, such patterns will be present in the dictionary of every attacker trying to guess passwords. Therefore, you should never use keyboard patterns as passwords, even if they contain uppercase letters, numbers, and symbols.

Step 3 & 4: Evaluation with Lay-users and Final Refinements

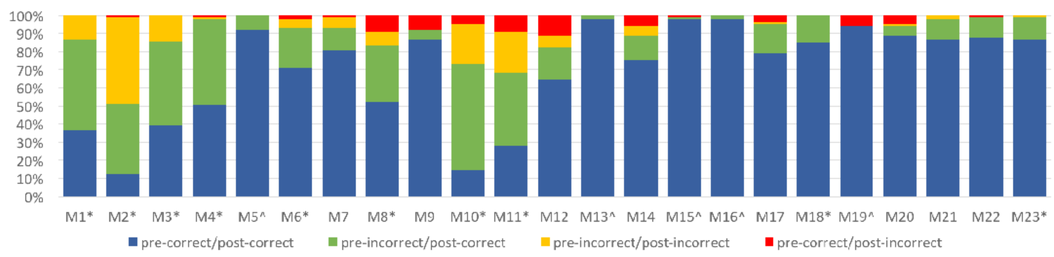
Method

- Participants: 90 employees of German SME
- Items developed from misconceptions with feedback from independent psychology experts

Pre-Treatment Questionnaire → Treatment (Interventions) → Post-Treatment Questionnaire

Results

- Most misconceptions prevalent in sample
- Correct responses increased from 72.8% to 90.2%
- Most misconceptions show significant improvements
- Formally evaluated effective intervention



*Published full paper: Mayer, P. & Volkamer, M., 2017.
Addressing Misconceptions About Password Security Effectively.
In International Workshop on Socio-Technical Aspects in Security and Trust.

KASTEL

SECUSO
SECURITY · USABILITY · SOCIETY