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

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

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