Code Book: Participants' Perceptions of Inconsistency.

Category	Subcategory	Explanation	Quote	Percentage
Attitude	Negative	Feelings of being upset, disappointed, frustrated, and concerned.	"It was very much confusing to understand what was actually strengthen of the passwords at the point of time."	42.52%
	Positive	Believing PSMs are more effective.	"My view is the PSMs are more effective compared to actual strength."	6.34%
	Neutral	Feeling indifferent, considering it normal.	"I think both are same." or "I think none of it matters if hackers steal everyone's passwords it doesn't matter how strong or weak they are."	6.06%
Perception	Algorithm Limitations	Thinking that there may be inadequacies in the algorithm's capabilities.	"Many PSMs use basic algorithms that may not fully account for the complexities of password security. They often focus on character variety and length without considering context or common vulnerabilities."	20.47%
	Predictable Patterns	Thinking that PSMs fail to identify some predictable patterns.	"Many PSMs struggle to identify complex patterns, sequences or substitutions, underestimating password vulnerability."	10.67%
	Surprising Attitude	Being surprised and finding the result unexpected.	"I believe this inconsistency is surprising, always believed that passwords in accordance to their requirements were sufficient for being strong."	2.31%

Code Book: Participants' Future Measures for Password Creation.

Category	Explanation	Quote	Percentage
Increase password complexity	Adding diverse character types, increasing length, avoiding common patterns.	"I will create long passphrases using a combination of random words or a memorable sentence. This approach balances complexity with the memorability and is typically more secure than traditional passwords."	63.72%
Stick to current habits	Following personal criteria or patterns for passwords.	"I don't plan to create passwords any differently in the future just based on the inconsistencies in PSMs. I plan to continue to use passwords that are easy for me to remember while still being sufficiently quirky to be hard for a hacker to guess."	40.57%
Follow PSM suggestions	Trusting the recommendations provided by PSMs.	"Still keep using PSMs' password suggestion as they're robust enough without me doing most of the work."	11.46%
Avoid password reuse	Minimizing reliance on PSMs and avoiding reusing passwords.	"Each password will be unique to each account to prevent a single breach from compromising multiple accounts."	12.65%
Adopt security tools	Using password managers and enabling 2FA for added security.	"I plan to use 2FA program to add another layer of security"	17.90%
Stay updated	Keeping up with security trends and adapting practices.	"I would stay informed about the latest trends in password security and potential vulnerabilities, ensuring that my practices evolve alongside new threats."	14.56%