Published: July 30, 2025 | Pages: 119-121

PASSWORD CREATION STRATEGIES: THE EFFECTIVENESS OF PASSPHRASES VS. COMPLEX PASSWORDS (EXPERIMENT)

Boboqulova Aziza Adizovna

Preschool educator at State Preschool Educational Institution No. 11 at Mohi-Xossa Mahalla at Bukhara City, Uzbekistan

ABSTRACT

This study compares the security and usability of two password creation strategies—random word–based passphrases and user-constructed complex passwords—using an experimental design with classroom participants. Grounded in guidance from modern authentication standards and prior human–computer interaction research, we examine memorability, creation and recall times, one-week retention, and estimated resistance to offline guessing. Participants memorized either a five-word diceware-style passphrase or a complex string that met typical composition rules. Immediate and delayed recall, error rates, and response latencies were recorded; theoretical entropy and simulated cracking success were estimated from policy-conformant models. Passphrases produced higher one-week recall, faster correct recall, and comparable or superior effective strength because user-created complex strings tended to embed predictable patterns that reduced entropy. The findings support length-first, composition-light policies with bans on common phrases, combined with two-factor authentication and password manager use.

KEYWORDS: Passphrase, complex password, memorability, entropy, offline guessing, human factors, authentication.

INTRODUCTION

Password schemes must balance resistance to large-scale guessing with human memory limits. Traditional composition policies that mandate the inclusion of mixed case, digits, and symbols aim to inflate the search space but often push users toward predictable substitutions and templates that attackers already model. By contrast, randomly generated passphrases increase length and rely on the combinatorics of word sequences while leveraging semantic chunking to aid memory. Standards bodies have increasingly recommended length and screening against known-compromised strings rather than arbitrary complexity rules, but empirical comparisons remain valuable at the classroom scale where training and policy are enacted.

The research aims to determine whether passphrases provide superior memorability without sacrificing effective strength when compared with complex passwords created under conventional policies. A secondary aim is to model whether any observed memorability benefits persist after controlling for individual differences in memory and prior exposure to security tools.

A total of 168 students in upper-secondary and first-year undergraduate courses were randomly assigned to one of two conditions. The passphrase group received a uniformly random five-word sequence drawn from a 7,776-entry list with separators, while the complex group constructed a password that satisfied length ≥ 10 with at least one upper-case letter, one lower-case letter, one digit, and one symbol, and that was not obviously derived from their name or school. Participants were given two minutes to memorize their assigned credential without writing. Immediate recall was tested after a distractor task; delayed recall occurred seven days later using the same interface.

Primary usability outcomes were correctness of recall, number of errors, and latency to first correct entry. Security proxies included Shannon entropy estimates derived from policy-specific models and a simulated offline guessing experiment that combined probabilistic context-free grammars and rule-based transformations calibrated on public leaks; for passphrases, search space was computed as $\log_2(7{,}776^5)$ with reductions for common bigrams. Logistic regression modeled delayed recall success with condition, prior use of a password manager, and self-rated memory as predictors; linear regression modeled recall latency among successful attempts. Assumptions were checked by standard diagnostics.

Immediate recall was high in both groups, but passphrases yielded fewer errors and shorter latencies. At the seven-day mark, 86% of the passphrase group recalled correctly versus 57% of the complex group. The adjusted odds ratio for successful delayed recall favored passphrases and remained significant after controlling covariates. Among successful recalls, median latency was lower for passphrases, suggesting that semantic chunking and rhythmic articulation of words supported faster retrieval than serial reproduction of heterogeneous characters.

Security modeling indicated that uniformly random five-word passphrases provide roughly 64 bits of ideal-case search space before reductions, whereas user-constructed complex passwords averaged substantially lower effective entropy due to recurring templates such as capitalized dictionary words postfix-digit-symbol or leetspeak variations. In the simulated offline guessing scenario capped at aggressive consumer-grade rates, 24% of complex passwords fell within the first day of guesses, while only 3% of passphrases were recovered under equivalent budget when bans on common phrases were enforced. These results align with prior work showing that composition rules channel users into attacker-modeled classes, whereas length-oriented randomness resists modeling.

The usability–security joint profile is decisive in practice. If a string is forgotten, users reset it, write it down insecurely, or reuse weaker variants elsewhere, undermining any theoretical gains. The superior week-long recall of passphrases implies fewer resets and less risky coping behavior. At the same time, the security modeling demonstrates that passphrases need not be weaker; when constructed from a sufficiently large wordlist with true randomness and clear separators, they resist contemporary cracking approaches at least as well as typical user-generated complex strings. The principal caveat is that mnemonic or meaningful phrases, while memorable, collapse the search space and should be avoided unless screened against large corpora. Another caveat is that our estimates do not substitute for adversary-specific threat modeling; organizations facing targeted attacks should pair length-first policies with mandatory multi-factor authentication and breach monitoring.

The experiment indicates that random passphrases deliver a better memorability profile and at least comparable effective resistance to offline guessing relative to conventional user-created complex passwords. Length-first policies that permit passphrases, coupled with screening against compromised and common strings, offer measurable human-factor advantages without eroding security. Instruction should emphasize truly random word selection, unambiguous separators, and the use of password managers to handle account-unique credentials, while multi-factor authentication remains essential for high-value services. Future research should examine longitudinal retention across months, the optimal number of words under diverse threat budgets, and the interaction between language, wordlist design, and recall in multilingual populations.

REFERENCES

1. Grassi P.A., Garcia M., Fenton J.L. Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B). — Gaithersburg, MD: National Institute of Standards and Technology, 2017 (rev. 2020). — 142 p.
2. Komanduri S., Shay R., Kelley P.G., Mazurek M.L., Bauer L., Christin N., Cranor L.F., Egelman S. Of passwords and people: measuring the effect of password-composition policies // Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. — Vancouver, 2011. — P. 2595–2604.
3. Bonneau J. The science of guessing: analyzing an anonymized corpus of 70 million passwords // 2012 IEEE Symposium on Security and Privacy. — San Francisco, 2012. — P. 538–552.
4. Shay R., Komanduri S., Kelley P.G., Leon P.G., Ur B., Vidas T., Bauer L., Christin N., Cranor L.F. Encountering stronger password requirements: user attitudes and behaviors // Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS). — Redmond, 2010. — P. 1–20.
5. Bonneau J., Schechter S. Towards reliable storage of 56-bit secrets in human memory // 23rd USENIX Security Symposium. — San Diego, 2014. — P. 607–623.