From: dig-comments@list.nist.gov on behalf of [redacted]
To: dig-comments@nist.gov
Cc: lorrie@cmu.edu
Subject: [dig-comments] DISCOURAGING Password complexity rules - in "addition" to the already proposed SHALL NOT prohibition on complexity mandates.
Date: Friday, September 27, 2024 12:14:58 PM

A proposed variation on 64B (3.1.1.2 Point 5)

https://pages.nist.gov/800-63-4/sp800-63b.html#passwordver
Comment for: NIST SP 800-63-4 Suite (Second Public Draft)
5. Verifiers and CSPs SHALL NOT impose other composition rules (e.g., requiring mixtures of different character types) for passwords.

Proposed variation:

Comment Template for: NIST SP 800-63-4 Suite (Second Public Draft)
5. Verifiers and CSPs SHALL NOT impose other composition rules (e.g., requiring mixtures of different character types) for passwords,
and also SHOULD NOT encourage or promote these to users as being better or important.

Mandated password complexity has been a major issue for user convenience and misguided password security. The 'SHALL NOT' impose mandated complexity rules is GOOD. However, this fails to adequately cover verifiers from ENCOURAGING special symbols, even if they do not anymore mandate them. With an enormous number of verifiers currently enforcing such rules, we ask NIST to cover BOTH cases. Removing a mandate is entirely different from Discouraging a behaviour. NIST Should IMO go further, by 'actively discouraging' their use, in addition to prohibiting their being mandated.

Many verifiers encourage complexity, even if they **do not actively enforce it -**
e.g. https://www.airbnb.com/help/article/980#section-heading-1-0 says
"It's best to make your password... mix of letters, numbers and special characters"

Removing the mandates is only half the solution. Removing the ENCOURAGEMENT is what is needed to properly close the gap.
Else verifiers may remove mandates but not 'encouragement' text. They will leave such text in, out of apathy (as NIST doesn't discourage it), or out of an 'abundance of caution' (e.g. think of the children!).

NIST should encourage REMOVAL of the 'Verifier prompt text / encouragement' which guilt users towards unreasonably complex passwords

FYI It's a bugbear of mine - I wrote https://www.tesla.tours/campaigns/password-rules a few years ago.
I also authored https://www.neomatrix.com.au/books which covers security and social engineering a lot.

Thank you,

Chris Cooper
CEO & Director of Innovation
Neomatrix Ltd

[redacted]