[redacted]

From: dig-comments@list.nist.gov on behalf of Michael Evans [redacted]
Sent: Wednesday, September 25, 2024 6:59 PM
To: dig-comments@nist.gov
Subject: [dig-comments] SP 800-63-4 - Thank you for common sense!

I just read the ArsTechnica article "NIST proposes barring some of the most nonsensical password rules" which covers NIST update SP 800-63-4

Thank you, ALL of these are the bare minimum of what should be allowed. The only point I'd encourage a change on would be a revision to 510 characters (or greater). There's no good reason to not support at least that much input.
"Verifiers and CSPs SHOULD permit a maximum password length of at least 510 characters."

I worry that 64 plain text ascii characters may not allow sufficient entropy in all cases when utilizing correct horse battery staple (E.G.
the XKCD password entropy example) style passwords.

"""
Verifiers and CSPs SHALL require passwords to be a minimum of eight characters in length and SHOULD require passwords to be a minimum of
15 characters in length.
Verifiers and CSPs SHOULD permit a maximum password length of at least
64 characters.
Verifiers and CSPs SHOULD accept all printing ASCII [RFC20] characters and the space character in passwords.
Verifiers and CSPs SHOULD accept Unicode [ISO/ISC 10646] characters in passwords. Each Unicode code point SHALL be counted as a single character when evaluating password length.
Verifiers and CSPs SHALL NOT impose other composition rules (e.g., requiring mixtures of different character types) for passwords.
Verifiers and CSPs SHALL NOT require users to change passwords periodically. However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.
Verifiers and CSPs SHALL NOT permit the subscriber to store a hint that is accessible to an unauthenticated claimant.
Verifiers and CSPs SHALL NOT prompt subscribers to use knowledge-based authentication (KBA) (e.g., “What was the name of your first pet?”) or security questions when choosing passwords.
Verifiers SHALL verify the entire submitted password (i.e., not truncate it).
"""

--
To unsubscribe from this group, send email to dig-comments+unsubscribe@list.nist.gov

View this message at https://list.nist.gov/dig-comments
To unsubscribe from this group and stop receiving emails from it, send an email to DIG-Comments+unsubscribe@list.nist.gov.