[redacted]

From: 'Jeff White' via DIG-Comments <DIG-Comments@list.nist.gov>
Sent: Thursday, September 26, 2024 8:50 PM
To: dig-comments
Subject: [dig-comments] SP 800-63-4

Regarding draft SP 800-63-4, section 3.1.1.2 points one and five:

I applaud the updated practices in the other sections. However, I believe in the age of AI it would be more practical to have an absolute minimum of 12 characters, and to require a mix of character types, avoiding dictionary words.

In conjunction with the other guidelines, this should allow people to set passwords that are significantly complex, ie use acronyms and abbreviation, to create memorable and long passwords when they are not created by a password manager.

I work for a managed service desk and some of our clients still use passwords that are six characters in length, or only allow maximum of 16 characters for example. Systems like that are not good enough, even if the password is generated by a password manager.

As a standard to add: Where users have multiple sets of credentials to manage, organizations must provide education in the use of password managers, even if none is provided by the organization.

This alone would make a huge difference.

Sent from ProtonMail mobile