Comment Template for: NIST SP 800-63-4 Suite (Second Public Draft)

Please submit responses to dig-comments@nist.gov by October 7, 2024.

Organization:	*Unaffiliated*
Name of Submitter/POC:	*Chris Warrick*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63B	3.1.1.2	13	735	Some service providers (e.g. banks) employ a scheme in which users are asked for a subset of characters from their password. This supposedly prevents phishing/impersonation attacks, as the service providers teach their users that they will never ask for the entire password. However, this scheme makes it harder to use password managers (some of them support this scheme, but many don't) and encourages users to write out their password in cleartext to be able to count characters. The security benefit is also dubious, as in the case of a bank, a phishing site may operate "live" on the real bank's website – request the needed characters from the real website, present them to the victim, and then exfiltrate the money.	Add a rule to ban this practice. For example: "Verifiers and CSPs SHALL always request the password to be provided in full (and not request only a subset of it)."