You may already have addressed this. I'm commenting on https://pages.nist.gov/800-63-4/sp800-63b.html (as accessed today), if that's the relevant document.

I understand from lay news media coverage that you recommend passwords be simpler and less-often changed. Presumably, this is to make writing them less common.

One problem with this is if an authentication token for one use is rarely needed. I have passwords I think I haven't used in years and which may not have been invalidated.

I'm no star memorizer. I forget some passwords. On a few days, I've even forgotten my exact password for a service I use several times a week, maybe because I was thinking of something else, got myself confused, and got stuck in a loop with a wrong password and likely nearly got locked out.

I don't want to rely on a password manager someone may have cracked, or if someone cracked a non-air-gapped platform where I unlock my password manager.

I write them down. I do that in cipher and on paper, with a paper backup locked away offsite, and it helps that I'm virtually asocial anyway. I use only a small number of ciphers, so that I won't forget the ciphers. The ciphers are not difficult, and there are a few cases where using a cipher would make deciphering other tokens easy and for those I don't use a cipher but label them as literal (although I probably could create a cipher just for those and limit the risk to just that group (although would still risk the members of that group itself), and, on balance, maybe I should implement that). The paper, as you might guess, has very limited circulation.

Thank you.

--
Nick