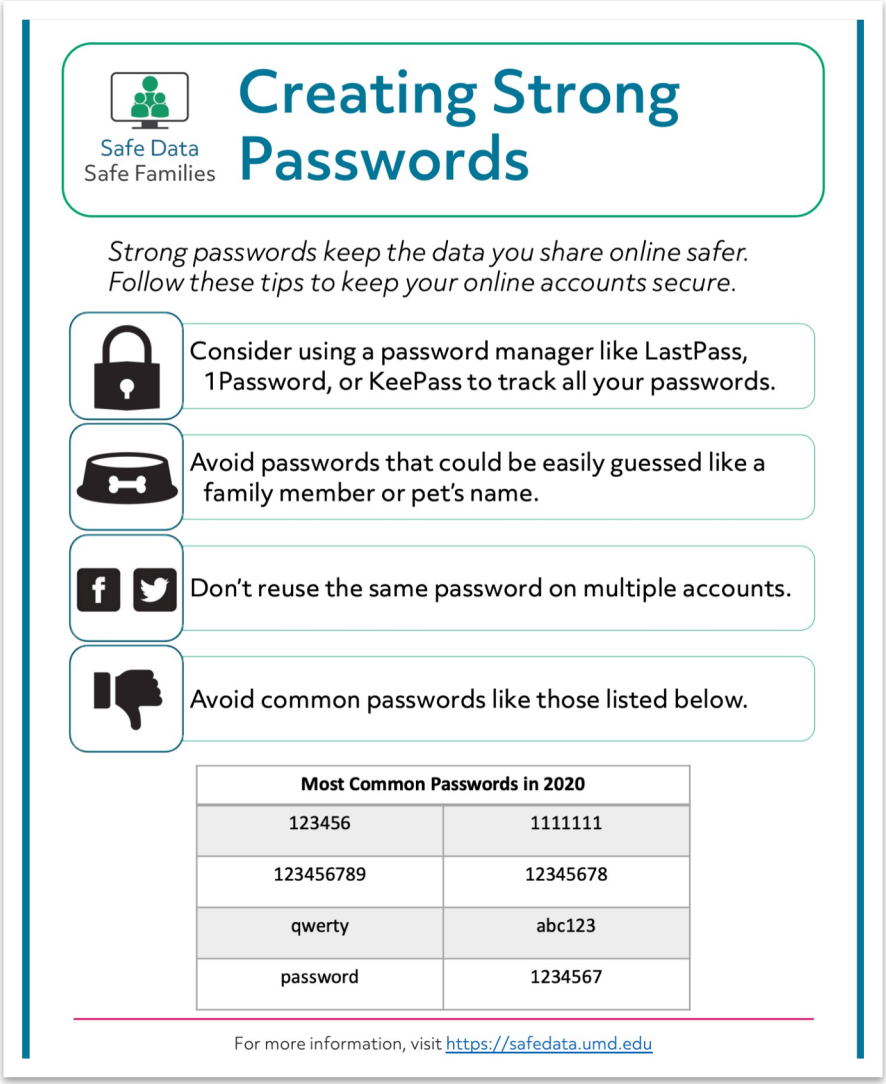
How to talk to patrons about: *Creating Strong Passwords*

- Tell them about 2-factor authentication (2FA), which provides an added layer of security for their account. 2FA should be used on your most important accounts (banking, email).
- Explain what makes a password weak (e.g., using sequential numbers or letters, using common words, using words about yourself).
- Explain what makes a password strong (long phrases; mix of letters, numbers, and/or symbols).

"Long passwords, at least 15 characters, are the most secure. Try to think of a phrase you can remember, but only makes sense to you."



Safe Data
Safe Families

Creating Strong Passwords

Strong passwords keep the data you share online safer. Follow these tips to keep your online accounts secure.

Consider using a password manager like LastPass, 1Password, or KeePass to track all your passwords.

Avoid passwords that could be easily guessed like a family member or pet's name.

Don't reuse the same password on multiple accounts.

Avoid common passwords like those listed below.

Most Common Passwords in 2020	
123456	1111111
123456789	12345678
qwerty	abc123
password	1234567

For more information, visit https://safedata.umd.edu