Personal Security

TIAA

Quote:

Two-step verification via text or phone

Verify your identity each time you log in using a temporary identification code sent to you via text or a phone call.

This helps ensure no one can access your account fraudulently, even if they did have your password.

University of Wyoming

Yes you can get a “number” sent to you via SMS.

Phones rely on you not loosing your number.

1. The number is “public”
2. Anybody can “call” the phone company and claim to be you. The phone company will ask
3. Last 4 digits of SSN
4. Mothers madden name
5. Previous home address
6. or about 4 other “easily” found chunks of data
7. Then the malicious actor provides the “key” of of a new SIM card for a burner phone and takes over your phone number.
8. Then the reset your email account - ‘Recover Password” - sends them a 6 digit conformation to the new phone number.
9. Now they recover the password to X using your email.

from the NIST standards

Summary that I will quot from (readable):

https://stealthbits.com/blog/nist-password-guidelines/

Actual guidelines by National Institute of Standards (NIST):

https://pages.nist.gov/800-63-3/sp800-63b.html

No More Hints or Knowledge-based Authentication (KBA)

Although password hints were intended to allow users to create more complex passwords, they ultimately caused users to leave hints that practically gave passwords away. To prevent this, password hints shouldn't be used in any form. This also includes knowledge-based authentication (KBA), such as questions like "What was the name of your first pet?".

Password Managers & Two Factor Authentication (2FA)

To account for the growing popularity of password managers, users should be able to paste passwords. Previously it was common to prevent the ability to paste in password fields, which made the use of these services difficult.

Regarding two factor authentication (2FA), SMS is no longer considered a secure option. In the place of SMS, one-time code provider/authenticators, such as Google Authenticator or Okta Verify, should be permitted.

How stuff is breached:

80% of breaches involve weak or compromised passwords and the top 10 common passwords still including '123456', 'password', and 'qwerty'.

Biometrics

This is fingerprints, iris scans and other things.

1. You can't change them. OMB lost 5.5 million biometrics probably to the China - in a single breach.
2. They can be remotely "collected".

This means that this should be a "username" not a "password"