Password Security & Best Practices for Users

Use multi-factor authentication (MFA) when possible.

- The best passwords can still be cracked. Multi-Factor Authentication adds another layer of protection in addition to your username and password. Generally, the additional factor is a token or a mobile phone app that you would use to confirm that you really are trying to log in.

Use different passwords for different accounts.

- If one account is compromised, the others will not be at risk.

Make passwords that are hard to guess, but easy to remember.

- To make passwords easier to remember, use sentences or phrases. Example: "pineappleonpizzaistasty"
- Hackers will use dictionaries of words and commonly used passwords to guess your password. Avoid single words, or a word preceded or followed by a single number (e.g., Password1).
- Do not use passwords that are based on personal information that can be easily accessed or guessed (e.g., birthdays, children's or pet's names, car model, etc.).

Length over complexity.

- The longer a password is, the better. Use the longest password or passphrase permissible by each password system.

But complexity still matters.

- To increase complexity, include upper- and lower-case letters, numbers, and special characters. Example: "pin3appl30nPizzaITaty

Never reveal your passwords to others.

- Your login credentials protect information that is as valuable as the money in your bank account. Nobody needs to know your password but you. If someone is asking for your password, it is a scam.

Use a password manager.

- Password management tools, or password vaults, are a great way to organize your passwords. A password manager allows users to generate complex passwords for online accounts on the spot and store them securely for later use. Many provide a way to back-up your passwords and synchronize them across multiple systems.
    - HHS does not recommend any password manager in particular, but some commonly used password managers are:
        - LastPass
        - KeePass
        - Keeper

U.S. Department of Health and Human Services
Health Sector Cybersecurity Coordination Center (HC3)
HC3@HHS.GOV www.HHS.GOV/HC3

- Password Safe
- Dashlane
- LogMeOnce
- Bitwarden
- 1Password

Password Security & Best Practices for Organizations: NIST Password Guidelines

NIST Password

A password that meets the regulations set out by the National Institution for Standards in Technology's Digital Identity Guidelines. Passwords that comply with NIST password guidelines will be tough to crack and easy to use.

NIST Password Guidelines

For their password guidelines, NIST not only focuses on the qualities of the password, but the behaviors of the people who create those passwords, to offer recommendations for how to create, authenticate, implement, store, and update passwords over time.

Enable Show Password

It is unlikely that the person behind you is going to record your password data, so there is little reason to hide your password as you type. You are more likely to make mistakes in typing if you cannot see the characters, and mistakenly think you have forgotten your password. This error leads to potential data exposure every time you need to reset your password.

Use a Password Manager

NIST suggests that companies use a password manager to help their employees and stakeholders encrypt and generate strong passwords. Even if you are securing your own servers, you will want to help reduce human error by giving your users access to a password manager, which will automatically generate long, strong passwords and passphrases for them.

Store Securely

NIST requires that organizations remove the user-generated password from their server as soon as it is created, either using a zero-knowledge password protocol or zeroization. They also suggest "hashing" and "salting" stored passwords. NIST defines a hash as "a function that maps a bit string of arbitrary length to a fixed-length bit string." Using hashes to store password data will ensure that you never expose a database of passwords to a hacker; instead, they would get a list of hashes that would take much longer to crack and give you more time to recuperate. Salting adds unique markers to each password, so even if two people had the same password, they are assigned two distinct hashes.

Lock After Multiple Attempts

NIST suggests locking a user out of password-protected programs if they use an incorrect password multiple times; per Section 5.22 of Special Publication NIST 800-63b, which provides guidelines for "rate-limiting" on authentication attempts, the verifier should allow no more than 100 attempts to input a password. However, most good programs limit far before that threshold and use strategies like making a user wait a period of time before attempting to sign on again.

Employ Two-Factor Authentication

Two-factor or multi-factor authentication requires that someone entering their password authenticates their login from another device or through a code sent to an alternate location (example: email or text), or with another form of data (fingerprint, face scan, etc.).

Do not focus on password complexity

NIST password guidelines say you should focus on length, as opposed to complexity when designing a password. Using complex passwords (adding special characters, capitalization, and numbers) may make it easier to hack your code, and this mostly has to do with user behavior. Complex passwords are harder to remember, which means users may need to update their passwords more often, making minor changes, which makes them easier prey for cyber-attacks.

Monitor New Passwords Daily

Some passwords are compromised even before they are created; ensure that new passwords are not just strong, long, and complex, but they are not on lists of commonly used, easily compromised passwords (example: "123456" and "password").

References

"Creating and Managing Strong Passwords," CISA. 27 March 2018. https://www.cisa.gov/uscert/ncas/current-activity/2018/03/27/Creating-and-Managing-Strong-Passwords

Kurko, Michael. "Best Password Managers," Investopedia. 9 June 2022. https://www.investopedia.com/best-password-managers-5080381

"NIST Password Guidelines: The New Requirements You Need to Know," Auditboard. 24 September 2021. https://www.auditboard.com/blog/nist-password-guidelines/

"Password Best Practices," UC Santa Barbara. N.d. https://www.it.ucsb.edu/secure-compute-research-environment-user-guide/password-best-practices

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and new products. Share Your Feedback