Choosing and Protecting Passwords | CISA

Authors CISA

6-8 minutes

Passwords are a common form of authentication and are often the only barrier between you and your personal information. There are several programs attackers can use to help guess or crack passwords. By choosing good passwords and keeping them confidential, you can make it more difficult for an unauthorized person to access your information.

Why you need strong passwords

You probably use personal identification numbers (PINs), passwords, or passphrases every day: from getting money from the ATM or using your debit card in a store, to logging in to your email or into an online retailer. Tracking all of the number, letter, and word combinations may be frustrating, but these protections are important because hackers represent a real threat to your information. Often, an attack is not specifically about your account, but about using the access to your information to launch a larger attack.

One of the best ways to protect information or physical property is to ensure that only authorized people have access to it. Verifying that those requesting access are the people they claim to be is the next step. This authentication process is more important and more difficult in the cyber world. Passwords are the most common means of authentication, but only work if they are complex and confidential. Many systems and services have been successfully breached because of non-secure and inadequate passwords. Once a system is compromised, it is open to exploitation by other unwanted sources.

How to choose good passwords

Avoid common mistakes

Most people use passwords that are based on personal information and are easy to remember. However, that also makes it easier for an attacker to crack them. Consider a four-digit PIN. Is yours a combination of the month, day, or year of your birthday? Does it contain your address or phone number? Think about how easy it is to find someone's birthday or similar information. What about your email password—is it a word that can be found in the dictionary? If so, it may be susceptible to dictionary attacks, which attempt to guess passwords based on common words or phrases.

Although intentionally misspelling a word ("daytt" instead of "date") may offer some protection against dictionary attacks, an even better method is to rely on a series of words and use memory techniques, or mnemonics, to help you remember how to decode it. For example, instead of the password "hoops," use "IlTpbb" for "[I] [l]ike [T]o [p]lay [b]asket[b]all." Using both lowercase and capital letters adds another layer of obscurity. Changing the same example used above to "Il!2pBb." creates a password very different from any dictionary word.

Length and complexity

The National Institute of Standards and Technology (NIST) has developed specific guidelines for strong passwords. According to NIST guidance, you should consider using the longest password or passphrase permissible (8–64 characters) when you can. For example, "Pattern2baseball#4mYmiemale!" would be a strong password because it has 28 characters and includes the upper and lowercase letters, numbers, and special characters. You may need to try different variations of a passphrase—for example, some applications limit the length of passwords and some do not accept spaces or certain special characters. Avoid common phrases, famous quotations, and song lyrics.

Dos and don'ts

Once you've come up with a strong, memorable password it's tempting to reuse it—don't! Reusing a password, even a strong one, endangers your accounts just as much as using a weak password. If attackers guess your password, they would

have access to your other accounts with the same password. Use the following techniques to develop unique passwords for each of your accounts:

- Use different passwords on different systems and accounts.
- Use the longest password or passphrase permissible by each password system.
- Develop mnemonics to remember complex passwords.
- Consider using a password manager program to keep track of your passwords. (See more information below.)
- Do not use passwords that are based on personal information that can be easily accessed or guessed.
- Do not use words that can be found in any dictionary of any language.

How to protect your passwords

After choosing a password that's easy to remember but difficult for others to guess, do not write it down and leave it someplace where others can find it. Writing it down and leaving it in your desk, next to your computer, or, worse, taped to your computer, makes it easily accessible for someone with physical access to your office. Do not tell anyone your passwords, and watch for attackers trying to trick you through phone calls or email messages requesting that you reveal your passwords.

Programs called password managers offer the option to create randomly generated passwords for all of your accounts. You then access those strong passwords with a master password. If you use a password manager, remember to use a strong master password.

Password problems can stem from your web browsers' ability to save passwords and your online sessions in memory. Depending on your web browsers' settings, anyone with access to your computer may be able to discover all of your passwords and gain access to your information. Always remember to log out when you are using a public computer (at the library, an internet cafe, or even a shared computer at your office). Avoid using public computers and public Wi-Fi to access sensitive accounts such as banking and email.

There's no guarantee that these techniques will prevent an attacker from learning your password, but they will make it more difficult.

For more information on passwords, multi-factor authentication, and related password topics, see Supplement Passwords.

Don’t forget security basics

- Keep your operating system, browser, and other software up to date.
- Use and maintain antivirus software and a firewall.
- Regularly scan your computer for spyware. (Some antivirus programs incorporate spyware detection.)
- Use caution with email attachments and untrusted links.
- Watch for suspicious activity on your accounts.

Reprinted from: https://www.cisa.gov/uscert/ncas/tips/ST04-002