CHOOSING AND PROTECTING PASSWORDS

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. But if you choose good passwords and keep them confidential, you can make it more difficult for an unauthorized person to access your information.

Why you need strong passwords

Think about the number of personal identification numbers (PINs), passwords, or passphrases you use every day: getting money from the ATM or using your debit card in a store, logging on to your computer or email, or signing in to an online bank account. The list of things that you can do online gets longer every day. Keeping track of all of the number, letter, and word combinations may be frustrating at times, and maybe you've wondered if all of the fuss is worth it. After all, what attacker cares about your personal email account, right? Or why would someone bother with your bank account when there are others with much more money? Often, an attack is not specifically about your account but about using the access to your information to launch a larger attack. And while having someone gain access to your personal email might not seem like more than an inconvenience or embarrassment, think of the implications of an attacker gaining access to your Social Security number or your medical records.

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 if you don't choose good passwords and keep them confidential, they're almost as ineffective as not having any passwords at all. Many systems and services have been successfully breached because of insecure and inadequate passwords, and some viruses and worms have exploited systems when attackers were able to guess weak passwords.

How to choose good passwords

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? Or 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. Your best defense, though, is to use a combination of numbers, special characters, and both lowercase and capital letters. Changing the

same example used above to "Il!2pBb." creates a password very different from any dictionary word.

Longer passwords are more secure than shorter ones because there are more characters to guess, so consider using passphrases when you can. For example, "Passwd 4 miemale!" would be a strong password because it has many characters and includes lowercase and capital letters, numbers, and special characters.

You may need to try different variations of a passphrase—some applications limit the length of passwords, and some do not accept spaces. Avoid common phrases, famous quotations, and song lyrics.

Don't assume that once you've developed a strong password you should use it for every system or program. If attackers do guess it, they would have access to all of your accounts. You should use these techniques to develop unique passwords for each of your accounts:

- Use different passwords on different systems and accounts.
- Don't use passwords that are based on personal information that can be easily accessed or guessed.
- Use a combination of capital and lowercase letters, numbers, and special characters.
- Don't use words that can be found in any dictionary of any language.
- Develop mnemonics such as passphrases for remembering complex passwords.
- Consider using a password manager program to keep track of your passwords. (See more information below.)

How to protect your passwords

Now that you've chosen a password that's difficult to guess, you have to make sure not to leave it someplace for people to find. Writing it down and leaving it in your desk, next to your computer, or, worse, taped to your computer, is just making it easy for someone who has physical access to your office. Don't tell anyone your passwords, and watch for attackers trying to trick you through phone calls or email messages requesting that you reveal your passwords. (See Avoiding Social Engineering and Phishing Attacks for more information.)

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.

Other password problems stem from web browsers' ability to save 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. So, 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.

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

Don’t forget security basics

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

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

Source:
United States Computer Emergency Readiness Team. “Security Tip (ST04-002) Choosing and Protecting Passwords.” October 1, 2016.