PROTECTING YOUR PASSWORD

February 2023

https://righttoconnect.org

Protecting Your Password

Some Password Requirements

The most common way a computer hacker will try to harm you is through your passwords. Online businesses routinely ask you to update your login details and choose passwords that follow strict security procedures.

This can be annoying if the password you want to use is too short and doesn't contain a special character, a number, or a capital letter. Despite the inconvenience, security guidelines are provided for your protection. While choosing a
password:

- write down a new strong password rather than using a short, obvious one;
- use symbols, capital and small letters, signs, and numbers in your password;
- don't rely on Windows passwords. They are swiftly obliterated;
- use passwords with a minimum of eight characters;
- always use a new password if you change it;
- use strong passwords that are not directly related to your interests or life;
- modify passwords every month, every other month, every three months, and or at least every six months; and
- Use password managers.

Password Attacks

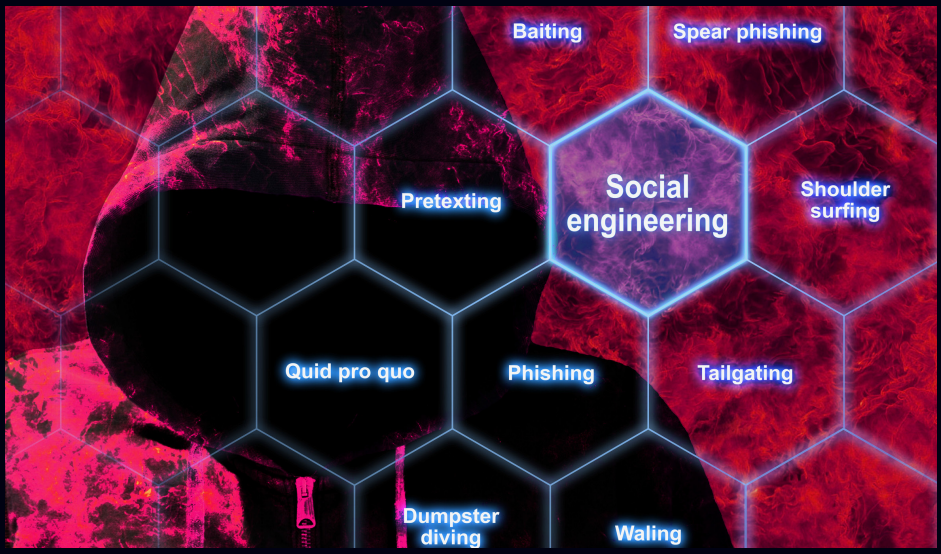
Effective computer service necessitates the use of strong passwords. You have the chance to utilize different passwords for different accounts. This makes it more difficult for intruders to enter. The most crucial element of any system when it comes to digital security is a strong password. History shows that password cracking is the most common method used by hackers and attackers to target your information systems.

Password Attack - Profiling

Profiling means making an accurate guess about the information and personal data of the password's owner. Your passwords frequently include easy-to-remember words and signs, such as your loved ones' names, the year of your birth, the name of an important person, your hometown, your favorite sports and or teams, etc. The profilers take into account these and similar data. For those intruders who can't benefit from hacking technology, password guessing is the most widely used method of breaking into a system.

Password Attacks - Social Engineering

Many people fall for cleverly constructed scenarios and queries that trick them into exposing their passwords. It might come in the shape of a phone call from your internet service provider (ISP), who claims to be performing server updates and requires your password to ensure that you don't lose any email in the process. This method is referred to as social engineering. It is still a feasible approach for hackers to try to break into a system.



Password Attacks - Dictionary Attacks

Sometimes an intruder tries any words from a dictionary as a password to obtain access to a computer, network, or other IT resource that is password-protected. A dictionary attack can also be used to attempt to crack an encrypted message or document. In this attack, the document will be attacked using a list of potential passwords.

Password Attacks - Brute force Attacks

This attack will typically be over in less than five seconds. This method does not rely on a list of imaginable passwords that have been pre-loaded. Instead, it will attempt any password that is possible, including those that contain letters, numbers, and special characters. To avoid being hacked, use more than eight different characters. Using a password manager can also be helpful in avoiding Brute Force Attacks.

Password Autosave

Some browsers and apps offer you an auto-saving option for passwords. When you log into an online account, the browsers will prompt you to save the password. When you choose this option, you are granting the browser permission to save the password on your computer. In order to extract the saved passwords from unencrypted data, numerous apps, and tools have been created. Therefore, never save your password automatically requested by the browser and app. If you have already given this permission to a browser and app, you can change it on Internet Explorer, Mozilla Firefox, Google Chrome, and Safari.

Auto Login

Additionally, operating systems provide you the option to log in automatically. This is helpful, while it is quite dangerous. This might be acceptable if the system is locked away in a place where only you can access your computer. However, it could be risky if someone else has access to your computer. If so, nothing stops them from accessing your private data.

Use Password Managers

Use one of these reliable password managers to protect your passwords.

1. NordPass – leading password manager https://nordpass.com
2. Keeper – ideal for Apple devices https://www.keepersecurity.com
3. RoboForm – intent for browsers https://www.roboform.com
4. Dashlane – perfect for sharing passwords https://www.dashlane.com
5. 1Password – ideal for family use https://1password.com
6. LastPass – the most feature-rich choice https://www.lastpass.com
7. Passwarden – ideal for personal use https://www.keepsolid.com/passwarden

Resources:

https://support.google.com
https://support.mozilla.org
https://learn.microsoft.com
https://support.google.com
https://support.apple.com/en-us/safari
https://nordpass.com
https://www.keepersecurity.com
https://www.roboform.com
https://www.dashlane.com
https://1password.com
https://www.lastpass.com
https://www.keepsolid.com/passwarden
https://www.bitdefender.com
https://ca.norton.com
https://www.totalav.com
https://surfshark.com
https://nordvpn.com