BRIDGEPOINT
TECHNOLOGIES

HOW TO CREATE, MANAGE AND REMEMBER A HACKERPROOF PASSWORD

(630) 320-3723 www.mybridgepoint.com 122 Eisenhower Ln N, Lombard, IL

HOW TO CREATE, MANAGE AND REMEMBER A HACKER-PROOF PASSWORD

Creating and remembering hacker-proof passwords is essential for protecting your online accounts and personal information. Here's a simple guide to help you generate strong passwords and keep them secure:

1 Use Long Passwords

•Aim for a minimum of 12 characters; longer is better.
•Longer passwords are exponentially more difficult for hackers to crack.

2 Mix Characters

•Include a combination of uppercase letters, lowercase letters, numbers, and special symbols (e.g., !, @, #, $, %).

3 Avoid Common Words And Phrases

•Don’t use easily guessable information like “password,” “123456,” or common phrases like “let me in.”
•Avoid using easily discoverable personal information like your name, birthdate, or family members’ names.

4 Create Randomness

•Generate random sequences of characters.
•Avoid patterns or easily guessable sequences (e.g., “abcd1234” or “qwerty”).

5 Use Passphrases

•Consider using a passphrase, which is a combination of random words.
•Make it long and include special characters for added complexity.

6 Avoid Dictionary Words

•Don't use complete words found in dictionaries, as hackers use dictionary attacks.

7 Unique For Each Account

•Use a different password for each online account.
•This prevents a security breach on one site from compromising your other accounts.

8 Password Managers

•Use a reputable password manager to generate, store, and autofill complex passwords.
•Password managers help you remember strong, unique passwords foreach site.

9 Two-Factor Authentication (2FA)

•Enable 2FA wherever possible.
•Even if someone gets your password, they won't be able to access your account without the second factor (e.g., a one-time code from an app or SMS).

10 Regularly Update Passwords

•Change your passwords periodically, especially for critical accounts like email and banking.
•Update passwords immediately if you suspect a breach.

11 Security Questions

•Be cautious with security questions. Avoid using easily discoverable answers that can be found online.

12 Test Your Passwords

•Some websites offer password strength checkers during the account creation process. Use them to gauge password strength.

13 Secure Password Recovery

•Ensure your password recovery options are secure. Don’t use easily guessable information.

14 Be Wary Of Phishing

•Avoid clicking on suspicious links or providing your password on unverified websites.
•Double-check the website’s URL before entering your password.

15 Education And Vigilance

•Stay informed about current security threats and best practices.
•Be vigilant and cautious online.
• Contact us to add you to our FREE weekly security tips.

Remember that no password is entirely hacker-proof, but by following these guidelines, you can significantly increase the security of your online accounts. Additionally, using a password manager can make it **easier** to maintain strong, unique passwords for **ALL** your accounts without the need to remember them all.