WP2C Wi-Fi Network Security Report

Report Generated on: 2023-04-05 15:12:16

Network Name:	Magic
Mac Address:	BA:5F:84:17:FA:52
Encryption:	WPA
Password:	11223344
Handshake Captured Date and Time:	2023-04-05 15:12:13
Password Cracked Date and Time:	2023-04-05 15:12:16

Password Vulnerabilities:

1. Password Strength: Very weak (0/4)
2. Estimated number needed to guess the password: 347
3. Estimated time needed to guess the password (offline fast hashing with many processors): less than a second
4. Estimated time needed to guess the password (offline slow hashing with many processors): less than a second
5. Estimated time needed to guess the password (online attack without throttling): 35 seconds
6. Estimated time needed to guess the password (online attack with throttling): 3 hours

Password Exposure:

zxcvbn: 11223344 found in passwords at position 346.

WP2C: 11223344 found in probable at position 159.

WP2C: 1122334455 found in probable at position 888.

WP2C: 112233445566 found in probable at position 6156.

WP2C: 112233445566778899 found in probable at position 49991.

WP2C: 11223344a found in probable at position 68324.

WP2C: 112233445 found in probable at position 84191.

WP2C: a11223344 found in probable at position 144403.

WP2C: 0011223344 found in probable at position 145455.

WP2C: 11223344aa found in probable at position 167935.

WP2C: 1122334455667788 found in probable at position 203523.

WP2C: 11223344556677 found in probable at position 203524.

WP2C: 11223344 found in top 10k known passwords at position 205720.

Have I Been Pwned: 11223344 was found to be leaked 272164 times. It is time to change it!

Comments and Recommendations for Weak Password:

1. This is a very common password.
2. Add another word or two. Uncommon words are better.

Recommendations to Avoid WPA Vulnerabilities:

1. Use WPA3 instead of WPA2
2. Use a strong, unique password for your Wi-Fi network
3. Regularly update the firmware of your Wi-Fi router
4. Disable WPS (Wi-Fi Protected Setup)
5. Disable legacy Wi-Fi protocols (e.g. 802.11b)
6. Avoid using dictionary words in your password
7. Use a combination of uppercase and lowercase letters, numbers, and symbols
8. Use a longer password, at least 12 characters
9. Change your password regularly
10. Consider using a password manager to generate and store strong passwords
11. Use WPA3 or WPA2 with AES encryption instead of WEP, which is vulnerable to attacks