WP2C Wi-Fi Network Security Report

Report Generated on: 2023-04-10 21:12:32

Network Name:	404
Mac Address:	FA:AF:85:D0:1D:60
Encryption:	WPA
Password:	testme1234
Handshake Captured Date and Time:	2023-04-10 21:11:03
Password Cracked Date and Time:	2023-04-10 21:12:32

Password Vulnerabilities:

1. Password Strength: Weak (2/4)
2. Estimated number needed to guess the password: 1104500
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): 2 minutes
5. Estimated time needed to guess the password (online attack without throttling): 1 day
6. Estimated time needed to guess the password (online attack with throttling): 1 year

Password Exposure:

zxcvbn: testme found in passwords at position 10945.

zxcvbn: 1234 found in passwords at position 7.

WP2C: testme1234 found in probable at position 1.

Have I Been Pwned: testme1234 was found to be leaked 61 times. It is time to change it!

Comments and Recommendations for Weak Password:

1. 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