

WP2C Wi-Fi Network Security Report

Report Generated on: 2023-03-28 18:48:52

Network Name: OnePlus8T
Mac Address: 7A:6F:4C:1F:F4:58
Encryption: WPA
Password: tp056181
Handshake Captured Date and Time: 2023-03-15 13:39:50
Password Cracked Date and Time: 2023-03-28 18:48:52

Password Vulnerabilities:

1. Password Strength: Weak (2/4)
2. Estimated number needed to guess the password: 100000001
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): 3 hours
5. Estimated time needed to guess the password (online attack without throttling): 4 months
6. Estimated time needed to guess the password (online attack with throttling): centuries

Password Exposure:

zxcvbn: No matches found.

WP2C: tp056181 found in top 10k known passwords at position 213815.

Have I Been Pwned: tp056181 was not found to be leaked. Carry on!

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