Darienite
News for Darien
https://darienite.com

Federal Trade Commission: 'Change Your Twitter Password. Now.'

Author : David Gurliacci

Categories : Public Safety

Tagged as : Cybersecurity Tips, Federal Trade Commission 2018, Password Tips, Safety Tips, Safety Tips 2018, Twitter

Date : May 7, 2018

You may have heard the recent news that Twitter discovered a bug that stored passwords "unmasked" in an internal log. What does this mean? If you are a Twitter user, your password could be exposed.

Twitter says that there are no signs of a breach or misuse by anyone currently, but it's still a good idea to change your password. Did you use the same password for other accounts? Change those, too.

— This article *is from the Federal Trade Commission's Consumer Information blog. Ari Lazarus is a consumer education specialist at the FTC.*

Here are some tips on creating passwords:

- **Make your password long, strong and complex.** That means at least twelve characters, with upper- and lowercase letters, numbers, and symbols. Avoid common words, phrases or information.
- **Don't reuse passwords used on other accounts.** Use different passwords for different accounts so that, if a hacker compromises one account, he can't access other accounts.
- **Use multi-factor authentication, when available.** For accounts that support it, two-factor authentication requires both your password and an additional piece of information to log in. The second piece could be a code sent to your phone, or a random number generated by an app or token. This protects your account even if your password is compromised.

- **Consider a password manager.** Most people have trouble keeping track of all their passwords. Consider storing your passwords and security questions in a reputable password manager, an easy-to-access application that stores all your password information. Use a strong password to secure the information in your password manager.
- **Select security questions only you know the answer to.**Many security questions ask for answers to information available in public records or online, like your zip code, mother's maiden name, and birth place. That is information a motivated attacker can get. And don't use questions with a limited number of responses that attackers can easily guess – like the color of your first car.
- **Change passwords quickly if there's a breach.** If you get a notification from a company about a possible breach, change the password for that account right away, and any other account that uses a similar password.

For more information on keeping your information secure, check out our article on Computer Security.

See also this Washington Post video from May 4:

"Everything you knew about creating passwords is wrong"