Justin Journals Stealth Password Report

Protect your confidential information by creating a secure password that makes sense to you, but not to others, and then make sure that no one else can find it.

Most people don't realize there are a number of common techniques used to crack passwords and plenty more ways we make our accounts vulnerable due to simple and widely used passwords.

How to get hacked

Dictionary attacks: Avoid consecutive keyboard combinations— such as qwerty or asdfg. Don't use dictionary words, slang terms, common misspellings, or words spelled backward. These cracks rely on software that automatically plugs common words into password fields.

Simple passwords: Don't use personal information such as your name, age, birth date, child's name, pet's name, or favorite color/song, etc. When 32 million passwords were exposed in a breach last year, almost 1% of victims were using "123456." The next most popular password was "12345." Other common choices are "111111," "princess," "qwerty," and "abc123."

Reuse of passwords across multiple sites: Reusing passwords for email, banking, and social media accounts can lead to identity theft. Two recent breaches revealed a password reuse rate of 31% among victims.

How to make them secure

1. Make sure you use different passwords for each of your accounts.
2. Be sure no one watches when you enter your password.
3. Always log off if you leave your device and anyone is around—it only takes a moment for someone to steal or change the password.
4. Avoid entering passwords on computers you don't control (like computers at an Internet café or library)—they may have malware that steals your passwords.
5. Avoid entering passwords when using unsecured Wi-Fi connections (like at the airport or coffee shop)—hackers can intercept your passwords and data over this unsecured connection.
6. Don't tell anyone your password. Your trusted friend now might not be your friend in the future. Keep your passwords safe by keeping them to yourself.
7. Depending on the sensitivity of the information being protected, you should change your passwords periodically, and avoid reusing a password for at least one year.

8. Do use at least eight characters of lowercase and uppercase letters, numbers, and symbols in your password. Remember, the more the merrier.

10. Strong passwords are easy to remember but hard to guess. **Iam:)2b29!** — This has 10 characters and says “I am happy to be 29!” I wish.

11. Use the keyboard as a palette to create shapes. **%tgbHU8*-** Follow that on the keyboard. It’s a V. The letter V starting with any of the top keys. To change these periodically, you can slide them across the keyboard. Use W if you are feeling all crazy.

12. Have fun with known short codes or sentences or phrases. **2B-or-Not_2b?** — This one says “To be or not to be?”

13. It’s okay to write down your passwords, just keep them away from your computer and mixed in with other numbers and letters so it’s not apparent that it’s a password. This is where the Justin Journals Password logs come in handy.

14. You can also write a “tip” which will give you a clue to remember your password, but doesn’t actually contain your password on it. For example, in the example above, your “tip” might read “To be, or not to be?” Maybe use the Justin Journals Password logs to do just this.

Our Stealth Password System

We found a safe secure way to have our passwords available to us at almost all times and at the same time be very secure. Here is what we do:

We record the website in a paper book such as this one. Then we make a Google Spreadsheet at Google Sheets. The name of this spread sheet is something innocent and not related to passwords. Maybe “Budget” or something along that line. At the top of this sheet we put a budget, so it looks perfectly innocent. But below this we have a numbered spread sheet with the passwords only.

So when you look in your password book at a specific website you wish to log into, you will see a number and that corresponds to the password in the Google Sheet. This is very easy and the only way someone will be able to get this information is if they have your login book and access to the Google sheet.

Use you imagination to make this as secure as you like.

Take a look at the Stealth Password books that Justin Journals has made at JustinJournals.com.