



How do I create a perfect password? (And write it in your password book)



Keep your password a **minimum of 12 characters**



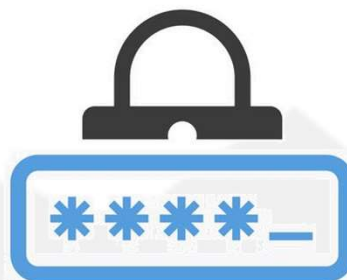
Stay away from apparent sequences and substitutions like @ for a or 0 for o



Don't use just one detail, create a **mix** of scenarios and personal information



Pick a **random** set of words that have a connection only **you** can think of



Password *

Password strength: Weak

For Example

1. Pick three words from the list below
2. Put a number or another non alphabetic character (ie: !"£\$%^&*@~#;) in the mix, use upper and lower case

1 belt	21 mobile	41 sticker	61 nail	81 finger
2 table	22 penguin	42 rose	62 light	82 bridge
3 dinner	23 swag	43 eggs	63 glass	83 chair
4 timer	24 moon	44 bottle	64 fixture	84 bangle
5 inventor	25 saddle	45 sofa	65 hoof	85 doll
6 cockatoo	26 ute	46 prism	66 pizza	86 sheep
7 spectacles	27 fugitive	47 whip	67 wing	87 money
8 swim	28 bake	48 football	68 wood	88 bubble
9 lagoon	29 nose	49 post	69 pet	89 waste
10 planter	30 wiper	50 basket	70 speech	90 pebble
11 juice	31 cover	51 stapler	71 autograph	91 leaf
12 glove	32 octopus	52 form	72 rain	92 rug
13 plate	33 wax	53 fountain	73 hide	93 arbor
14 pillow	34 memory	54 police	74 lily	94 frame
15 band	35 tunnel	55 rock	75 stubby	95 hamper
16 water	36 stinger	56 ranch	76 union	96 handle
17 willow	37 stove	57 butter	77 hand	97 cart
18 mud	38 apple	58 star	78 atlas	98 pear
19 stubble	39 horse	59 boat	79 brush	99 nozzle
20 shower	40 tongue	60 gravel	80 trek	100 hall

3. Et voilà an unbreakable password : **MoBile2belt%sticker**
4. Now write it down in your book, but remember:
 - a) Underline capitals
 - b) Put a / through zeros (0) dots over little i's, bars on big I's and L's (upper and lower) so they don't look like ones 1's etc.
 - c) **Plus:** For password recovery (when you forget it)...
 - i. A valid mobile phone number (not landline)
 - ii. A recovery email address
 - iii. The answers to the 'memorable questions' they asked



Eight ways to crack a Password

- 1. Phishing:** The most common password-stealing techniques currently in use today. They try to deceive a victim with seemingly legitimate information while acting on malicious intent. **Those odd phone calls 😊**
- 2. Social engineering:** Tricking users into believing the hacker is a legitimate agent. A common tactic is for hackers to call a victim and pose as technical support, asking for things like network access passwords in order to provide assistance. This can be just as effective if done in person, using a fake uniform and credentials. **"Hello I'm from your bank ..."**
- 3. Malware:** Keyloggers, screen scrapers, and a host of other malicious tools all fall under the umbrella of malware, malicious software designed to steal personal data. Alongside highly disruptive malicious software like ransomware, which attempts to block access to an entire system. Keyloggers, and their ilk, record a user's activity, whether that's through keystrokes or screenshots. **Don't click on things!**
- 4. Brute force:** Attacks involve hackers using a variety of methods, usually on a trial-and-error basis, to guess their way into a user's account. This could see attackers simply trying to use commonly used passwords like 'password123' against a known username, for example. A brute force attack can also take the form of an attacker making educated guesses. These (and 5,6 & 7) could mean that your data has been captured and sold on the Dark Web. **Check your email at haveibeenpwned.com**
- 5. Dictionary, Rainbow Tables and Mask Attacks:** Similar to brute force methods but involve hackers running automated scripts that take lists of known usernames and passwords and run them against a login system sequentially to gain access to a service. **Your username and a password may have been collected from a companies website you have used! A Mask Attack** use lists of all possible phrase and word combinations. **So always add numbers or other characters. Rainbow Tables** is just a reverse dictionary, where once a website has been compromised the hacker just looks up your real password from the encrypted one held by the site. **Therefore it is very important to have different passwords for each account you have!**
- 6. Network Analysis:** Network analysers are tools that allow hackers to monitor and intercept data packets sent over a network and lift the plain text passwords contained within. **A really good reason for not using public WiFi for banking.**
- 7. Shoulder Surfing:** Far from the most technically complex method in this list, shoulder surfing is one of the most rudimentary but effective techniques available to hackers, given the right context and target. **Who is BEHIND you (or camera)?**
- 8. Guess:** If all else fails, a hacker can always try and guess your password. 😊

The easy ones !

- | | |
|--------------|-------------------------|
| 1. password | 17. shadow |
| 2. 123456 | 18. master |
| 3. 12345678 | 19. jennifer |
| 4. 1234 | 20. 111111 |
| 5. qwerty | 21. 2000 |
| 6. 12345 | 22. jordan |
| 7. dragon | 23. superman |
| 8. pussy | 24. harley |
| 9. baseball | 25. 1234567 |
| 10. football | 26. football |
| 11. letmein | 27. hunter |
| 12. monkey | 28. monkey |
| 13. 696969 | 29. trustno1 |
| 14. abc123 | 30. ranger |
| 15. mustang | 31. buster |
| 16. michael | 32. thomas |

