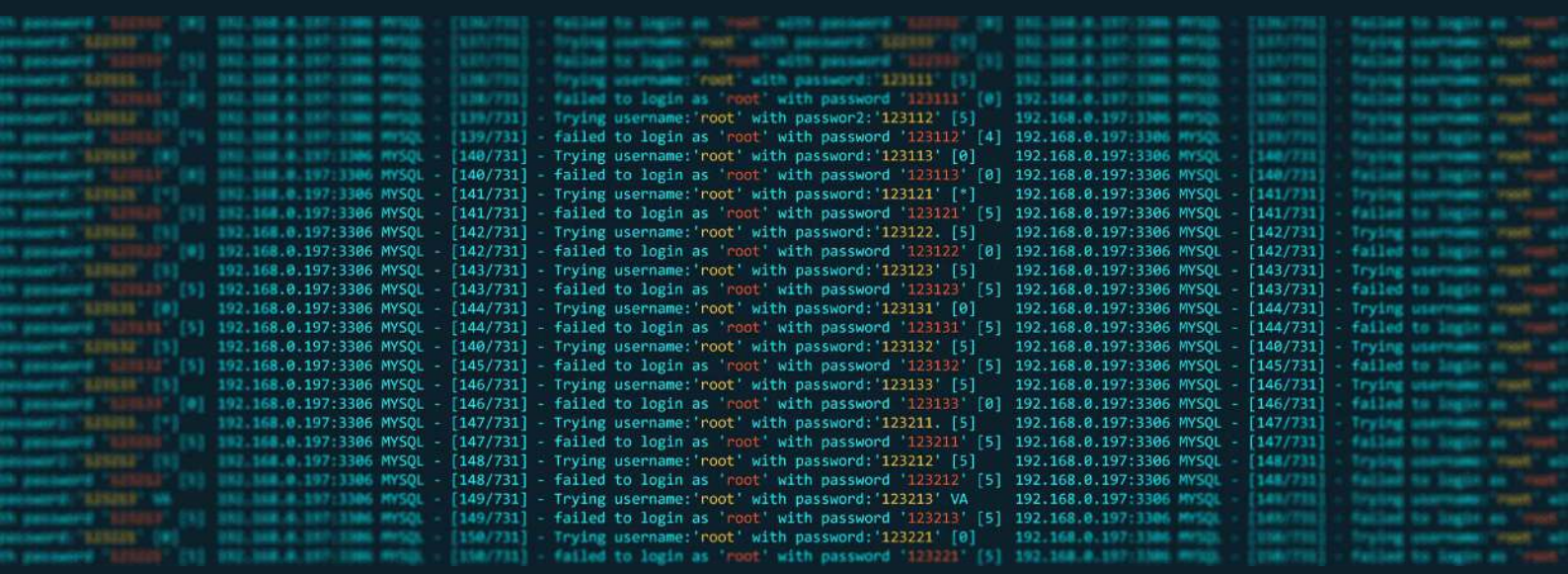
BitIDentify

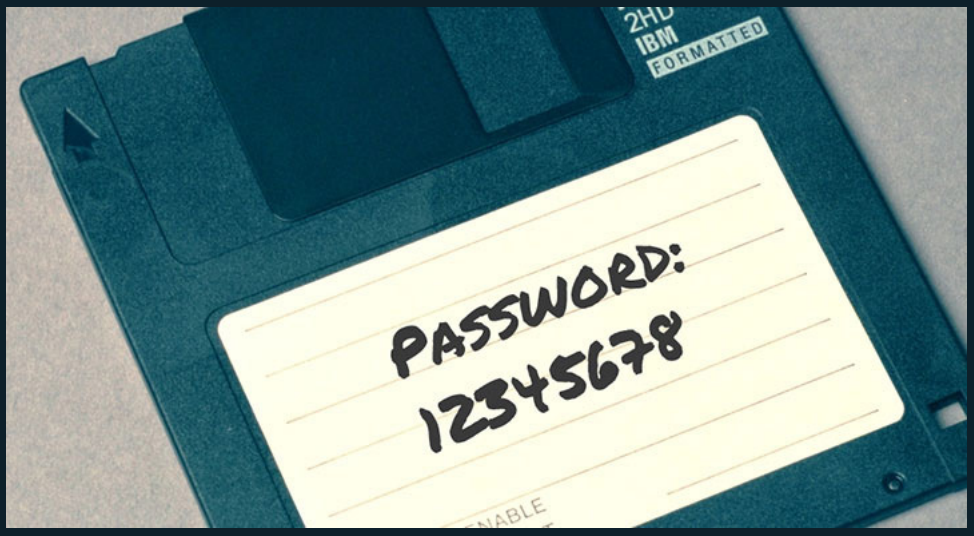


How to choose a password that's hard to crack

A good password is usually the first and only line of defense for your important web-services. Choosing a strong and memorable password can be a hassle since those two criteria don't always go hand in hand. It's tempting to reuse an old password, slightly modifying it, or even write it down on a text-file in the computer.

In this guide, we will show you how to choose a good password, how to remember it and just how easily bad passwords can get hacked.

Personal & Public information



1. **Use long passwords**
   Hackers use special programs to guess passwords; the technique is called “brute force attack,” a three character password takes less than a second to crack. Never use less than 8 characters and if possible, try to use 12 characters for a good safety margin.

   A good rule of thumb is to use the **”8-4-rule”**: *8 characters minimum, 1 lowercase, 1 uppercase, 1 number and 1 special character (8, 1+1+1+1=4).*

2. **Use nonsense phrases**
   Avoid using real dictionary words in any language, and avoid spelling dictionary words backward. Try to use words that are not grammatically correct, use your own spelling that you remember; this makes them much harder to crack.

   You probably have some funny spelling only you and your friends use, that’s a good word to use. Don’t use misspellings popular online; don’t use words from memes.

3. **Include numbers, symbols, uppercase, and lowercase letters**
   This is the “8-4-rule” again. The more you mix it up the harder it will be for a computer to guess. You could substitute the number zero for an “0” or an “@” for the letter “A”.

4. **Don’t use personal information**
   Easily discoverable information, such as your birthday, anniversary, address, city of birth, high school, relatives and pet’s names, should not be included in your password.

5. **Don’t reuse passwords**
   When there is a large attack and hackers breached a system, the list of compromised email addresses and passwords are often leaked online. Other hackers will use these login credentials since many users are unaware of this breach and will often reuse passwords on different services. This is why you should never reuse passwords.

6. **Don’t tell anyone**
   This should go without saying, but people still do it out of laziness. Don’t give your password to anyone else and don’t type your password within plain sight of other people. Don’t write your passwords on post-its next to your computer; it’s like begging to be hacked.

Personal & Public information

- **Change your passwords**
  The more sensitive your information is, the more often you should change your password. For example, your Google or Facebook password should be changed at least once a year, and never to be reused.

- **Use 2FA when possible**
  2FA is short for "2 Factor Authentication" and is a second layer of security you can enable for more sensitive web services like Google or Facebook. For example, with 2FA enabled on Gmail, the user logs in as usual with his username and password, then a code gets sent to the user's cellphone that needs to be verified before login is completed. Since more than 80 percent of people use the same password across multiple services, enabling 2FA is vital to stop hackers.

- **Don't EVER write down your passwords on your computer**
  You should write down your passwords; you just have to use a pen and paper. Writing down passwords on your computer or mobile device is just a really bad idea, it's like begging to be hacked. If a hacker can compromise your devices, he can easily find your passwords if stored on the device.

- **Use a password manager**
  Using different passwords for all sites and changing them with regular intervals can easily become too much to manage. A good solution to this problem is password managers; it's an application that remembers all your passwords and automatically logs in to your services. All your passwords are stored in this app and are protected by a master password, it's the only passwords you need to remember to log in to all your services.

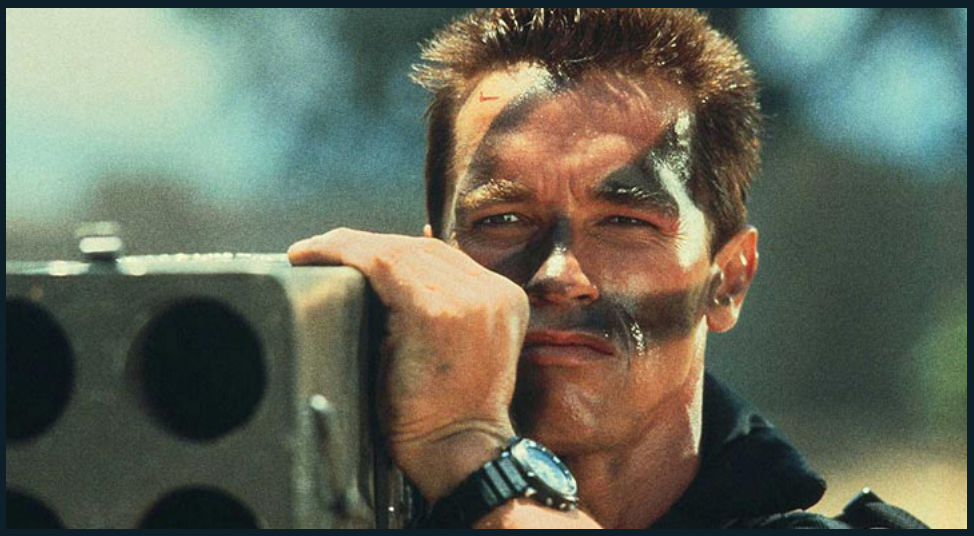
  A good and highly recommended password manager is **KeePassXC**

  - Open-source and audited
  - Uses modern non-NIST crypto (Argon 2 KDF, ChaCha20) (sorry NSA)
  - Minimal attack surface (only password manager Tavis Ormandy of Google Project Zero recommends)
  - Immune from commercially pressures that tip security balance

  Download: https://keepassxc.org/download

How passwords get hacked?

Hackers employ different techniques depending on the situation and the type of password to be cracked. If it's a password that can be cracked offline they use Brute Force Attacks or Dictionary Attacks; if it's an online password they use Phishing.Delete and Ok.



1. **Brute Force Attack**
   A brute force attack works for shorter passwords up to 8 characters; it's essentially just a program that guesses passwords until it gets it right. It's one of the oldest methods used to crack passwords but still effective under the right circumstances. One hacker used a 25-GPU cluster to crack any 8-character Windows password back in 2012, having the ability to make 350 billion guesses per second.

2. **Dictionary attack**
   While brute force attacks try every combination of symbols, numbers, and letters, a dictionary attack tries a prearranged list of words found in a dictionary. A password consisting of a single English word is fairly easy to guess and even appending numbers behind that word might not be enough. The only way to survive a dictionary attack is to use uncommon words, misspellings, and more than one word, preferably eight.

3. **Phishing**
   Phishing is a type of social engineering attack where the hacker masquerades as a trusted entity, tricking the user into divulging their login details. Usually, the hacker sends the target a phishing email claiming there is a problem with some of their services they need to take action on. The email usually directs the user to a link that leads to a fraudulent website made to look exactly like the user's original service (bank, email etc). Once the user enters their info, it's stolen.

4. **Leaked passwords**
   After big data breaches, the information from those breaches is usually leaked online for other hackers to use. These databases contain billions of hacked usernames and passwords for many of the biggest online services, and for most people, this goes by unnoticed so they keep using the same passwords.

   Using these databases, the hacker can automatically cycle trough all previously hacked passwords, and more times than not; they find a match. This is why it's so important to change your password; the could already be leaked.

BitIDentify

Password examples:

Bad	Okey	Good
ilovelamp	il0velamp	iL0v3LamP
donalthedrumpf	Donald7heDrumpf	D0n@ld_7h3_Drumpf
kitty	1kitty	1Ki77y
susan	Susan53	.Susan53
jellyfish	jelly22fish	jelly22fi$h
usher	!usher	!ush3r

Check if you have been hacked

To check if your accounts have been hacked there are web services that collect the leaked information into searchable databases. If you find that an account has been hacked you should immediately change that password on all services it's used on.

https://haveibeenpwned.com

https://www.avast.com/hackcheck

Original post can be found at our homepage:
https://www.bitidentify.com/blog/how-to-choose-a-password-thats-hard-to-crack/