CMPU1022
Password Hacking

Lecturer Paul Kelly

Password Hacking

Let’s look at the most used passwords in 2022.

The top 100 are here:

https://nordpass.com/most-common-passwords-list/

Most Common Passwords 2022

The worst passwords you can choose:

#1 password
#2 123456
#3 123456789
#4 guest
#5 qwerty
#6 12345678
#7 111111
#8 12345
#9 col123456
#10 123123

#11 1234567
#12 1234
#13 1234567890
#14 000000
#15 555555
#16 666666
#17 123321
#18 654321
#19 7777777
#20 123

Most Common Passwords 2022

The worst passwords you can choose:

#1 password
#2 123456
#3 123456789
#4 guest
#5 qwerty
#6 12345678
#7 111111
#8 12345
#9 col123456
#10 123123

#11 1234567
#12 1234
#13 1234567890

Password Tips (1 of 2)

- The average length is 7-9 characters (a lot of companies do “month you joined” + “Day”, e.g. March04)
- The average person knows about 75,000 words
- There’s a 50% chance someone’s password will contain vowels
- Women prefer names in their passwords, men prefer hobbies and movies

Password Tips (2 of 2)

- If there's a number in the password, it's most likely 0, 1, or 2, and towards the end of the password
- If there's a capital letter, it's usually at the start of the password, and followed by a vowel
- 65% of people have a maximum of 3 passwords for all the accounts (email, social media, PC, etc.)
- 1 in 100 people will have the top 100 Most Common Passwords.

Password Hacking

Easy to hack passwords are:

#1 Repeating previously used passwords
#2 Names of close family members or friends
#3 Your name
#4 Words in the dictionary
#5 Common names
#6 Repeating your login code
#7 Keyboard patterns and swipes (i.e., 123456 or QWERTY)

Hacking Attacks

Common hacking attacks are:

#1 Dictionary Attack
#2 Brute Force Attacks
#3 Rainbow Table Attacks
#4 Phishing
#5 Social Engineering
#6 Malware/Key loggers
#7 Shoulder surfing
#8 Spidering

#1 Dictionary Attack

It uses a simple file containing words that can be found in a dictionary, hence its rather straightforward name. In other words, this attack uses exactly the kind of words that many people use as their password.

Cleverly grouping words together such as "letmein" or "superadministratorguy" will not prevent your password from being cracked this way – well, not for more than a few extra seconds.

#2 Brute Force Attacks

It is similar to the dictionary attack.

It comes with an added bonus for the hacker. Instead of simply using words, it detects non-dictionary words by working through all possible alpha-numeric combinations from aaa1 to zzz10.

It’s not quick, provided your password is over a handful of characters long, but it will uncover your password eventually.

#3 Rainbow Table Attacks

Rainbow tables are a list of pre-computed hashes – the numerical value used when encrypting a password. These tables contain hashes of all possible password combinations for any given hashing algorithm.

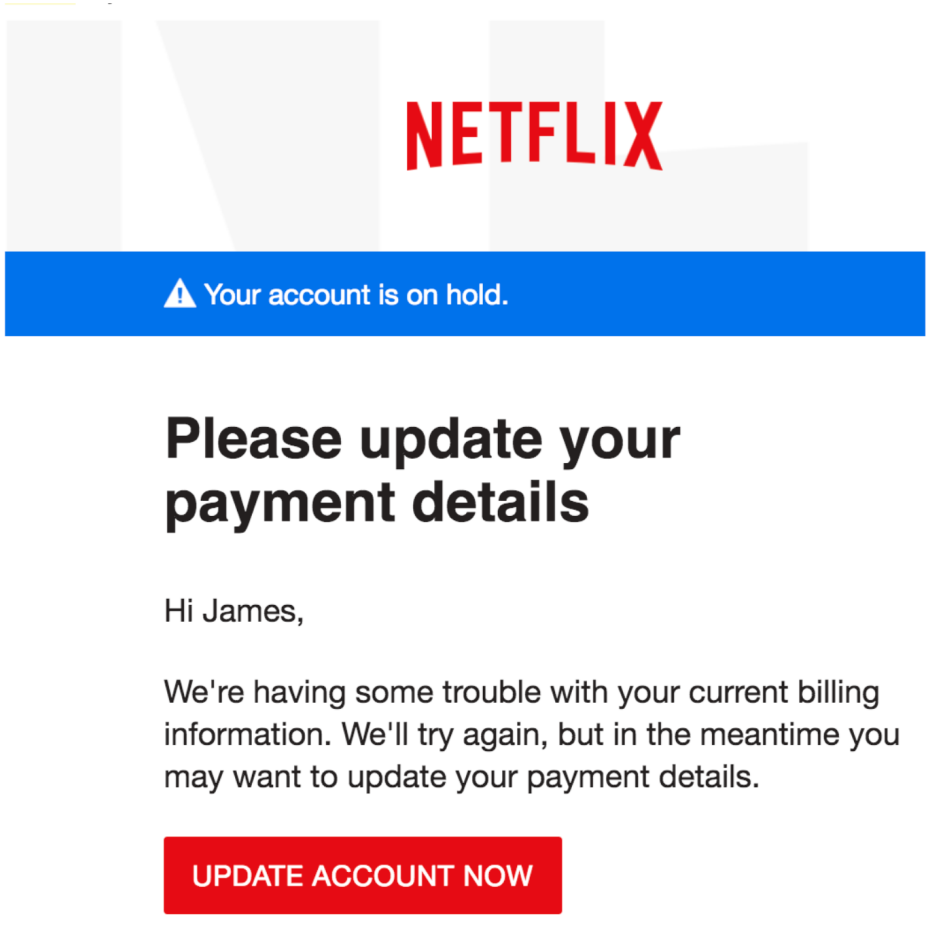
These attacks are attractive as it reduces the time needed to crack a password hash to simply just looking something up in a list.

#4 Phishing

There's an easy way to hack: ask the user for his or her password. A phishing email leads the unsuspecting reader to a faked log in page associated with whatever service it is the hacker wants to access, requesting the user to put right some terrible problem with their security.

That page then skims their password, and the hacker can go use it for their own purpose.

#4 Phishing


NETFLIX
Your account is on hold.
Please update your payment details
Hi James,
We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.
UPDATE ACCOUNT NOW

#5 Social Engineering

Social engineering takes the whole "ask the user" concept outside of the inbox that phishing tends to stick with and into the real world.

A favourite of the social engineer is to call an office posing as an IT security tech guy and simply ask for the network access password. You'd be amazed at how often this works. Some even have the necessary gonads to don a suit and name badge, walk into a business to ask the receptionist the same question face to face.

#6 Malware/Key loggers

A keylogger, or screen scraper, can be installed by malware which records everything you type or takes screenshots during a login process, and then forwards a copy of this file to hacker central.

Some malware will look for the existence of a web browser client password file and copy this which, unless properly encrypted, will contain easily accessible saved passwords from the user's browsing history.

#7 Shoulder surfing

The most confident of hackers will take the guise of a parcel courier, aircon service technician or anything else that gets them access to an office building. Once they are in, the service personnel "uniform" provides a kind of free pass to wander around unhindered and make note of passwords being entered by genuine members of staff. It also provides an excellent opportunity to eyeball all those post-it notes stuck to the front of LCD screens with logins scribbled upon them.

#8 Spidering

Savvy hackers have realised that many corporate passwords are made up of words that are connected to the business itself. Studying corporate literature, website sales material and even the websites of competitors and listed customers can provide the ammunition to build a custom word list to use in a brute force attack. Really savvy hackers have automated the process and let a spidering application, like those employed by leading search engines to identify keywords, collect and collate the lists for them.

Password Hacking

Who has been hacked already?

Who?	How many?	When?
Yahoo	3 billion accounts	2017
Twitter	330 million accounts	2018
Facebook	553 million accounts	2019
CAM4	10.88 billion records	2020
LinkedIn	700 million accounts	2021
Exactis	340 million accounts	2018
Verifications.io	763 million users	2019
First American Financial Corp	885 million users, including bank account records	2019

https://www.upguard.com/blog/biggest-data-breaches

Password Hacking

Sample Hack: How to bypass the Android 5.0 Lock Screen

1. Click on Emergency Dialler option
2. Keep on typing any random numbers and characters until it reaches its maximum limit
3. Write down the number that you have typed
4. Open the camera that you can even access with a locked screen
5. Try to drag the screen downward and it will ask you to enter a password. There paste in the code that you had copied
6. If the camera app doesn’t crash then repeat step from 1 to 5 while pressing the volume keys while pasting the code in
7. Repeat this until the camera app crashes and you moved to main menu with unlocked screen.

Password Hacking Tools

#1 Brutus

#2 RainbowCrack

#3 Wfuzz

#4 Cain and Abel

#5 John the Ripper

#6 THC Hydra

#7 Medusa

#8 OphCrack

#9 L0phtCrack

#10 Aircrack-NG

Recap

Who remembers what phishing is?

Any questions on what we covered?