

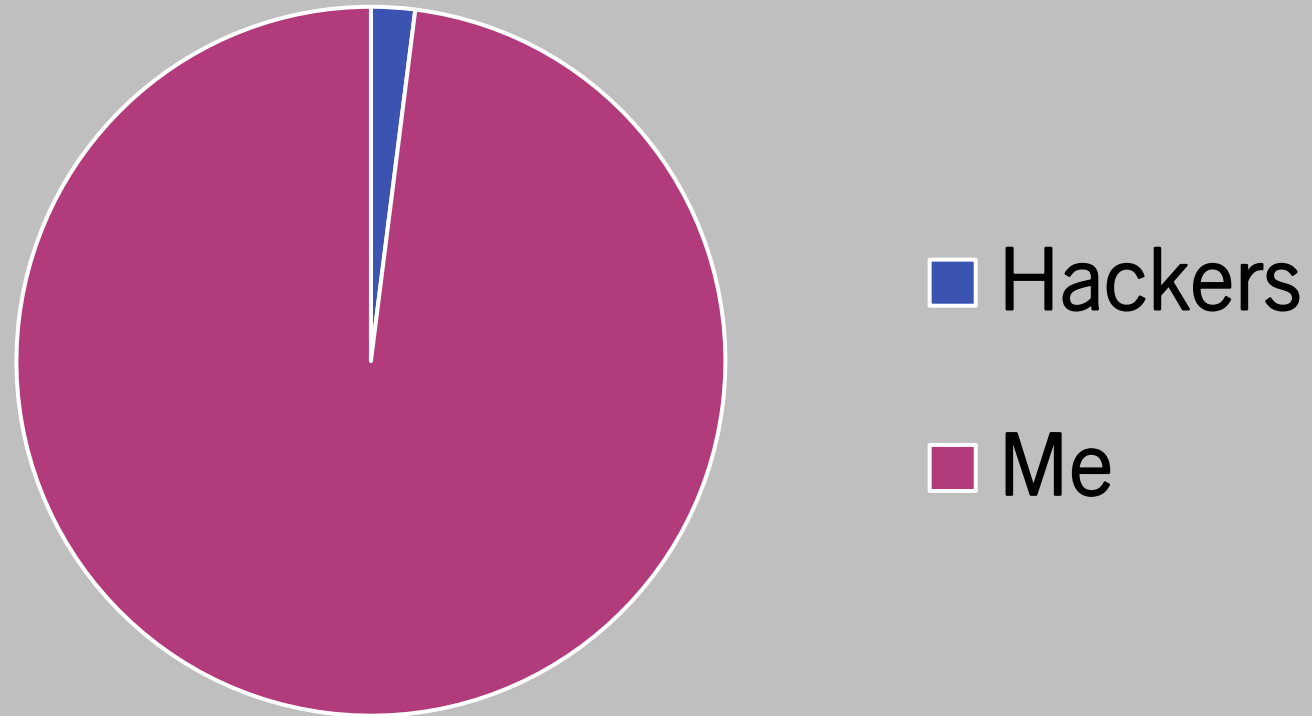
**HACKERS GET YOUR DATA
THROUGH WEAK PASSWORDS
PRACTICES: UNDERSTANDING WHY
AND HOW TO IMPROVE PASSWORD
PROTECTION**

Andréanne Bergeron

Cybersecurity Researcher



PEOPLE WHO CAN'T ACCESS MY ACCOUNT BECAUSE OF MY HIGH SECURITY PASSWORD



UNDERSTANDING PASSWORD RECOMMENDATIONS (MICROSOFT 2022)

- **Resisting common attacks**
- **Containing successful attacks**
- **Understanding human nature**

UNDERSTANDING PASSWORD RECOMMENDATIONS (MICROSOFT 2022)

- **Resisting common attacks**
 - Choice of where users enter passwords (known and trusted devices with good malware detection, validated sites)
 - Choice of what password to choose (length and uniqueness)



UNDERSTANDING PASSWORD RECOMMENDATIONS (MICROSOFT 2022)

- **Containing successful attacks**
 - Limiting exposure to a specific service if a user's password gets stolen
 - E.g.: Ensuring that a breach of your social networking credentials doesn't make your bank account vulnerable

UNDERSTANDING PASSWORD RECOMMENDATIONS (MICROSOFT 2022)

- **Understanding human nature**

- Almost every rule you impose on your users will result in a weakening of password quality.



OVERVIEW

- How do attackers proceed?
- What is a strong password?
- Prevalence of password strength among GoSecure clients
- What is a good password?



HOW DO ATTACKERS PROCEED?

Facebook

Login

[Forgot password](#)

Facebook

Email

Password

Login

[Forgot password](#)



Username	Password
VillaneuvaM@gmail.com	VillaneuvaM01
Mignon08@hotmail.fr	57367233
CloClo@hotmail.com	baseball123
Melich1996@gmail.com	qwerty
DDH666@umontreal.ca	password
Kitkat@gosecure.net	Caramilk\$2
MaPC!@yahoo.com	ILOVEU2004

Facebook

Email

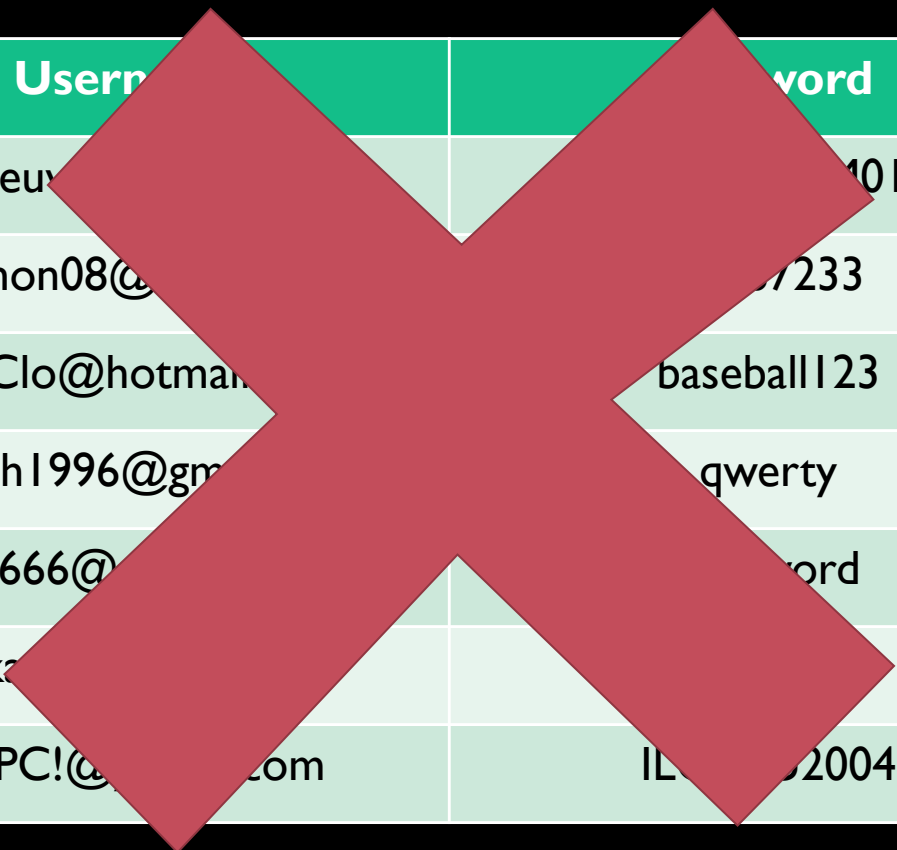
Password

Login

[Forgot password](#)



Username	Password
Villaneu	101
Mignon08@	7233
CloClo@hotmail	baseball123
Melich1996@gm	qwerty
DDH666@	ord
Kitka	
MaPC!@com	IL 2004



Hashed passwords

9c898fc91987d3a07e92efdb22f0a533:2fnKDA sf

b2bd18b0081c0ddfb4abd5996ac62916:OE2SuGcP

1d61f91492b6c2144adf33bbad7c9918:7FcsIRvM

fae2dff15bd864fdf13a9f71ddddd35d4:PTYKYK6M

207ea21eaa47b28728bc298a786fb101:JoRrEUV7

d9bf6bb63cdc61ead6e288557973bc54:aCy54uQC

WHAT IS A HASH?

Hashed passwords

9c898fc91987d3a07e92efdb22f0a533:2fnKDAsf
b2bd18b0081c0ddfb4abd5996ac62916:OE2SuGcP
1d61f91492b6c2144adf33bbad7c9918:7FcslRvM
fae2dff15bd864fdf13a9f71dddd35d4:PTYPYK6M
207ea21eaa47b28728bc298a786fb101:JoRrEUV7
d9bf6bb63cdc61ead6e288557973bc54:aCy54uQC

- Objective: attributing unique value
- Irreversible
- Example:

andrea = 1c42f9c1ca2f65441465b43cd9339d6c

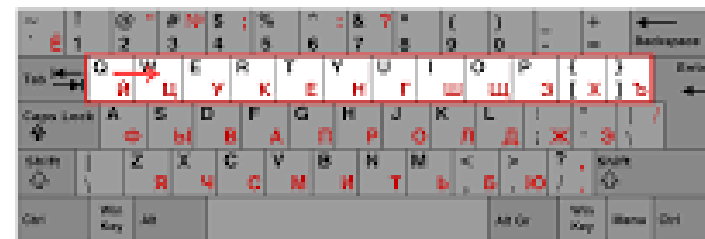
Andrea = 28f719c89ef7f33ce2e178490676b5ab

Tables to compare hash values

- Popular passwords
- Dictionary words
- Names

Word in clear text	Hash value
123456	e10adc3949ba59abbe56e057f20883e
123456789	25f9e794323b453885f5181f16624d0b
Password	5f4dcc3b5aa765d61d8327deb882cf99
Adobe123	7558af202997483d3afef3bb265a709d
12345678	25d55ad283a400af464c76d713c07ad
Qwerty	d8578edf8458ce06fbc5bb76a585ca4
1234567	fcea920f7412b5da7be0cf42b8c93759
111111	96e79218965eb72c92a549dd5a330112
Photoshop	c7c9cfbb7ed7d1cebb7a4442de308776
123123	4297f441395523524562497399d7a93

KEYBOARD WALK



BRUTE FORCE ATTACKS



Trying everything



TIME TO CRACK A PASSWORD ACCORDING TO ITS CHARACTERISTICS (2022)

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years



> Learn about our methodology at hivesystems.io/password

WHAT IS A STRONG PASSWORD?

- Length
- Combination of numbers, letters, symbols

WHEN BRUTE FORCING, FOR EACH OF THE
POSITION OF CHARACTERS IN THE PASSWORD:

32436632411



10 possibilities

hatiewpokhu



26 possibilities

dsg435ghhj



36 possibilities

olhgf5%489#



76 possibilities

WHAT IS A STRONG PASSWORD?

Email address	Passwords
Abergeron@gosecure.net	Abergeron@gosecure.net
Abergeron@gosecure.net	Abergeron
Abergeron@gosecure.net	Gosecure

WHAT IS A STRONG PASSWORD?

Email address	Passwords
Abergeron@gosecure.net	Abergeron@gosecure.net
Abergeron@gosecure.net	Abergeron
Abergeron@gosecure.net	GoSecure

WHAT IS A STRONG PASSWORD?

- Length
- Combination of numbers, letters, symbols
- No account information

WHERE DO OUR
CLIENTS STAND IN
TERM OF PASSWORDS'
STRENGTH?



DATA SOURCE

- Anonymized database of GoSecure clients' passwords
- Not all users: Only those we were able to crack

PREVALENCE OF GOOD PRACTICES AMONG GOSECURE CLIENTS



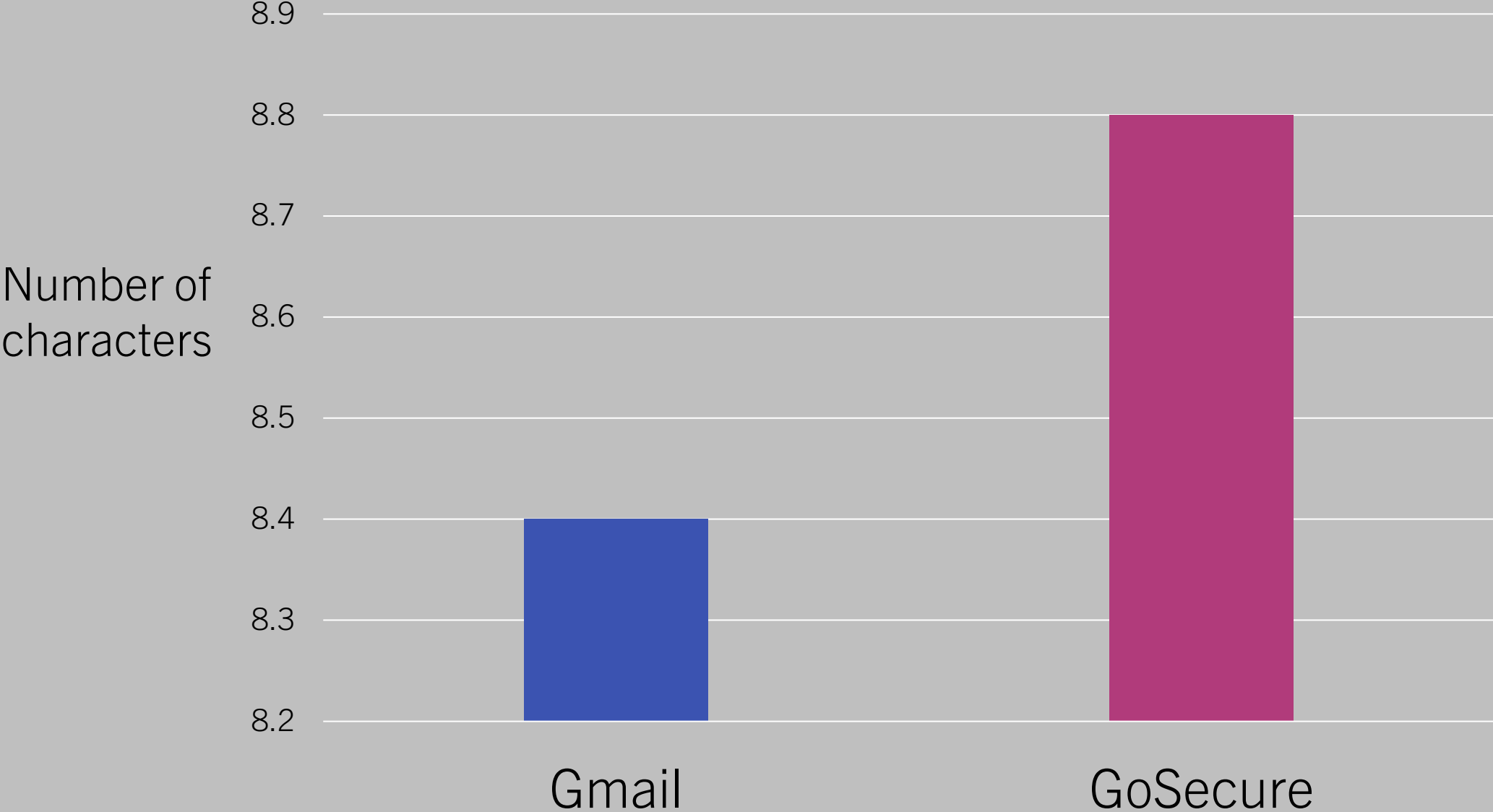
VS



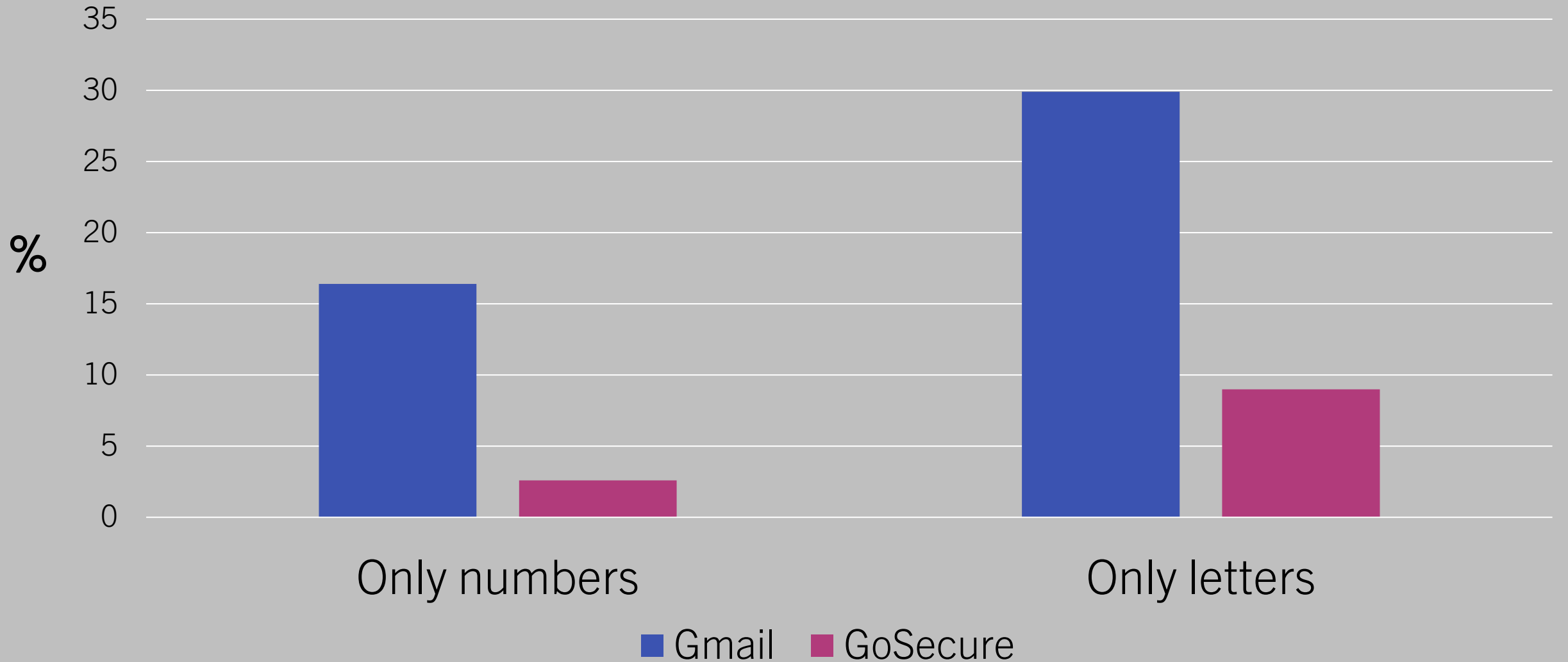
2,524,010 passwords

662,269 passwords

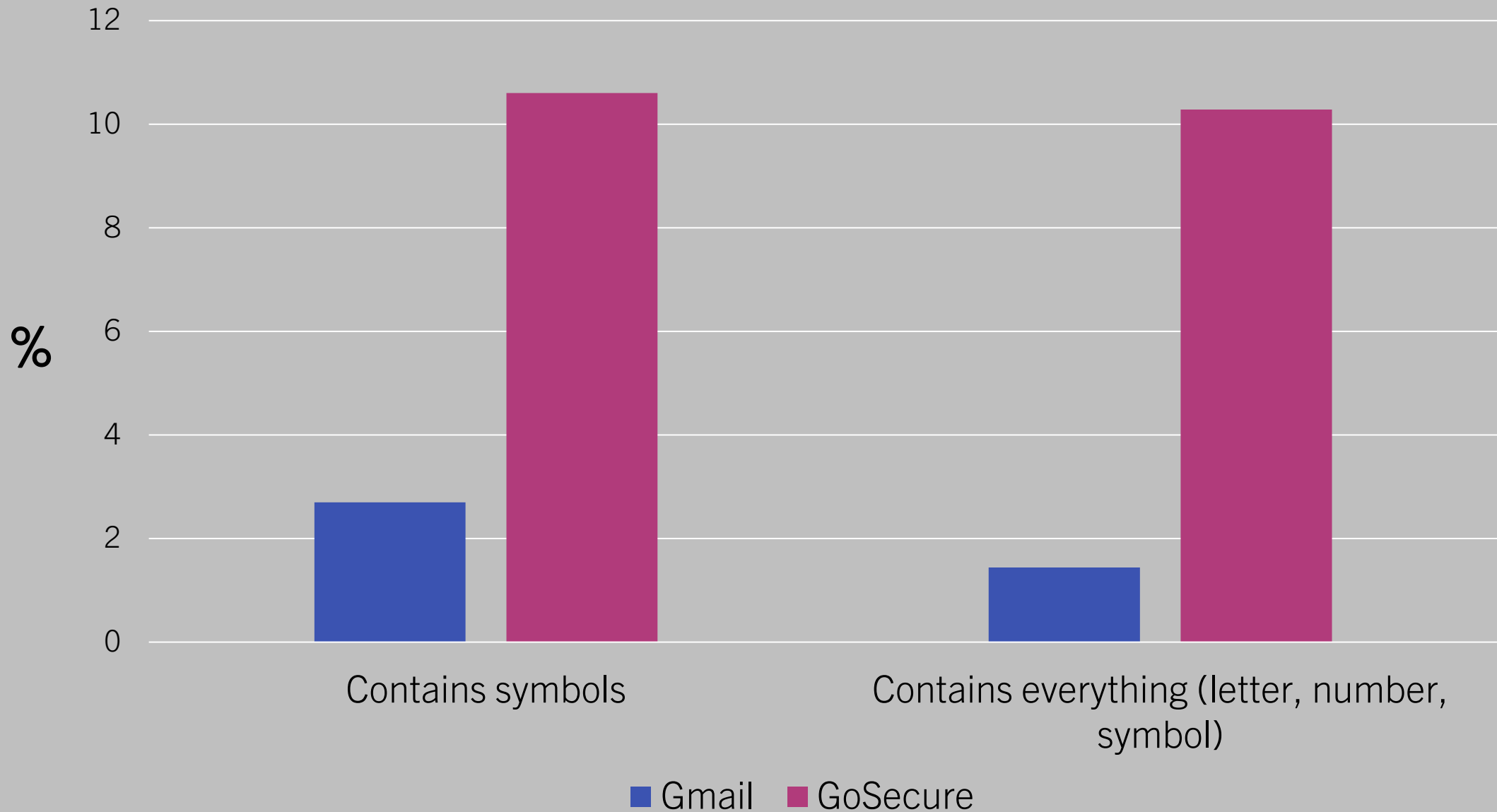
MEAN LENGTH OF PASSWORDS



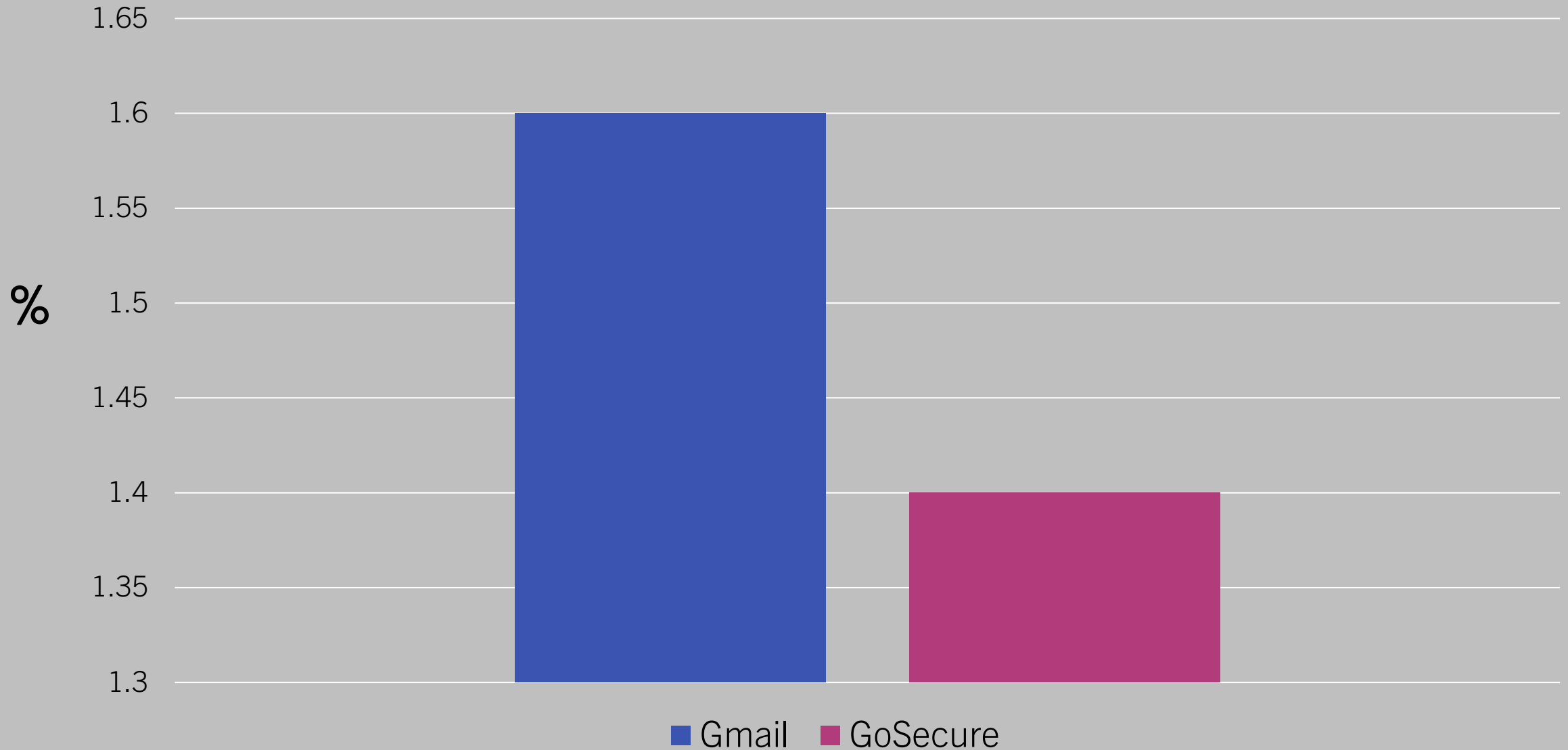
CHARACTERISTICS OF WEAK PASSWORDS



CHARACTERISTICS OF STRONG PASSWORDS



PRESENCE OF PROFANITY WORDS IN PASSWORDS



EXPLANATION OF RESULTS

- Work environnement versus personnal account
- Perception of sensitive information versus non-sensitive

IMPORTANT CONSIDERATION

- Unsignificant difference between samples
- Not all passwords: only those which were cracked/uncovered
- There is a large amount of good password not taken into consideration

WHAT IS A STRONG PASSWORD?

- Length
- Combination of numbers, letters, symbols
- No account information

WHAT IS A STRONG PASSWORD?

One solution:

Automatically generated password

STRONG ≠ GOOD

One solution:

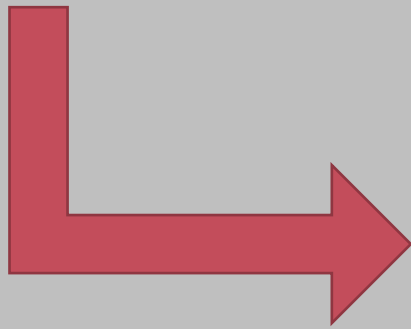
Automatically generated password

HYGf564THC22KJ&bdsj22

STRONG ≠ GOOD

- One solution:

Automatically generated password



- Help for the solution:

Passwords' manager

PASSWORDS' MANAGER

- It is hard to make people adopt it
 - Not part of habit
 - Do not enjoy using it
- Some are controlled by a third party
- Some have no backup alternative

STRONG ≠ GOOD

- Length
- Combination of numbers, letters, symbols
- No account information
- → **Memorable**

WHAT IS A GOOD PASSWORD?

macaronis

WHAT IS A GOOD PASSWORD?

M@C@r0n1s

WHAT IS A GOOD PASSWORD?

M@cc@r0n1s

- Long
- Mix of uppercase and lower case, number, symbols
- No account information

FIRST PROBLEM: HACKERS KNOW THIS

M@c@r0n1s



Common substitutions

SECOND PROBLEM: NOT SO EASY TO REMEMBER...

- What was the word?
 - Negroni?
 - Macarena?
 - Macaronic?
- Where was my uppercase?
- Was it a « @ » or « 4 » or « A » or « a » ?


THIRD PROBLEM: NOT SO HARD TO CRACK

M@c@r0n1s

Time to crack acknowledging common substitution:
2 min 41 seconds

- Time to crack acknowledging common substitution: **2 min 41 seconds**
- Brute force attack should take on average: **2 days**

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years


[Learn about our methodology at hivesystems.io/password](https://hivesystems.io/password)

WHAT IS A GOOD PASSWORD?

Potential solution:
Amalgam of words

WHAT IS A GOOD PASSWORD?

giraffe travel shelf empty



Four random common words

ADVANTAGES:

→ VERY HARD TO CRACK

→ YOU ALREADY

MEMORIZED IT!

giraffe travel shelf empty



TO KEEP IN MIND:

Acetophenetidin Chincherinchee Sesquipedalian Whatchamacallum

—



ANOTHER SOLUTION: LONG SENTENCE



Ididnotstealthegummy
bears,mybrotherdid.



EXAMPLES OF BAD SENTENCES TO USE IN YOUR PASSWORD

- *“Luke, I am your father” – Star Wars Episode V: The Empire Strikes Back*
- *“What words can I speak that they will heed.” – The Ten Commandments*
- *“'cause baby i'm the one who's keeping score – Someday by Mariah Carey*

EXAMPLES OF BAD SENTENCES TO USE IN YOUR PASSWORD

- “May the Force be with you.” - *Star Wars*
- “I'm the king of the world!” - *Titanic*
- “Elementary, my dear Watson.” - *The Adventures of Sherlock Holmes*
- “E.T. phone home.” - *E.T. the Extra-Terrestrial*
- “Hasta la vista, baby.” - *Terminator 2: Judgment Day*

KEEP UP THE EFFORTS!

Users tend to choose weak passwords

Users tend to reuse their password across many different sites

Users tend to use personal information in the composition of the password

Users tend to not change their password after a data breach

CONCLUSION

- Multi-authentication factors (MFA)
- Biometric recognition (face or fingerprints scanning)
- FIDO Alliance and their Client to Authenticator Protocol (CTAP)

QUESTIONS



Andréanne Bergeron
abergeron@gosecure.net

