Study Series for Cyber Security

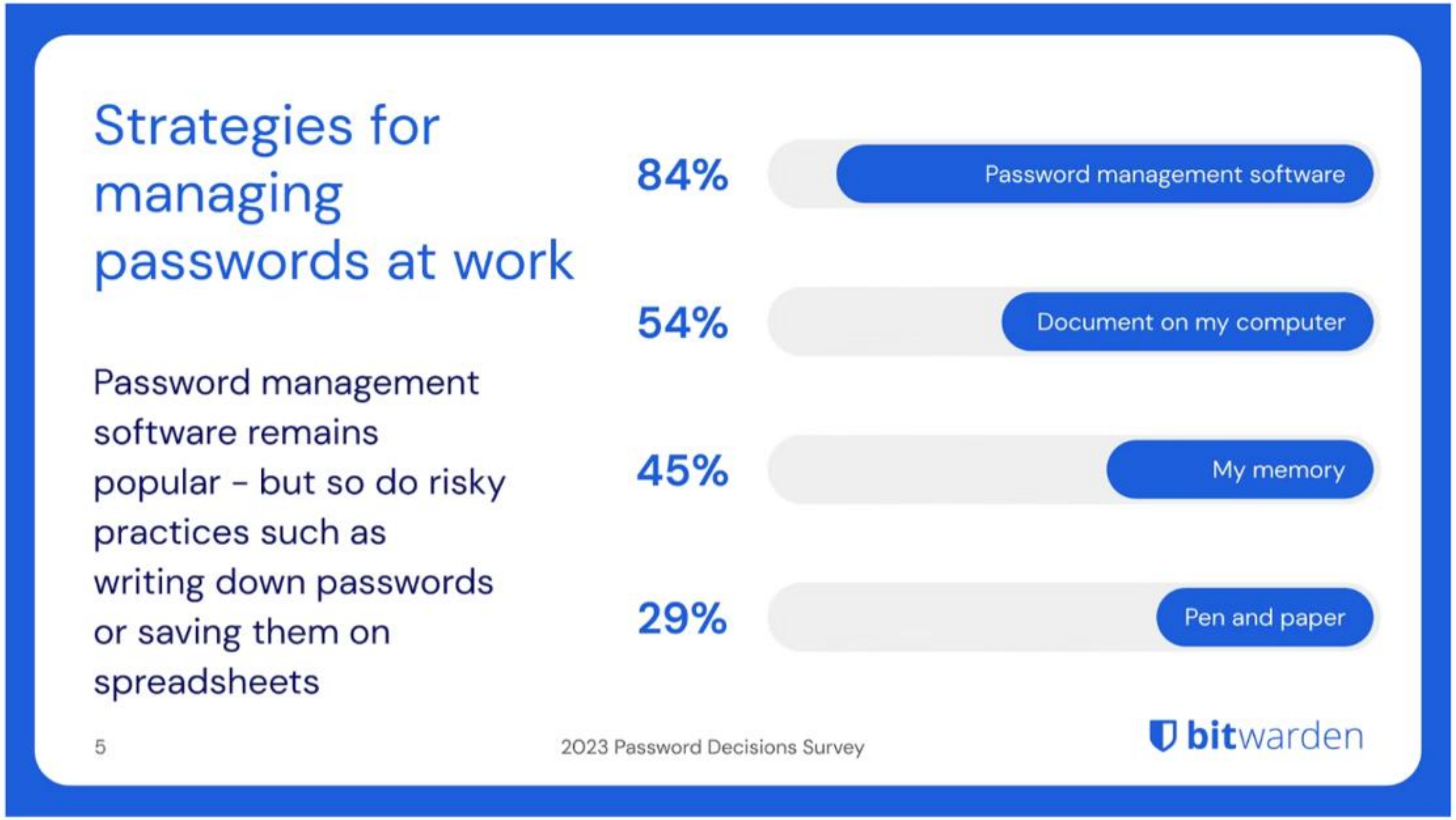
– TK

CURRENT CYBER SECURITY LANDSCAPE …

Disinformation, denial of Service attacks, **internet Threats**, ransomware, Malware, **social Engineering**, supply chain Attacks, and threats against data.

Where to Begin?

These are dangerous everyday habits of end-users.



Strategies for managing passwords at work

Password management software remains popular – but so do risky practices such as writing down passwords or saving them on spreadsheets

84% Password management software

54% Document on my computer

45% My memory

29% Pen and paper

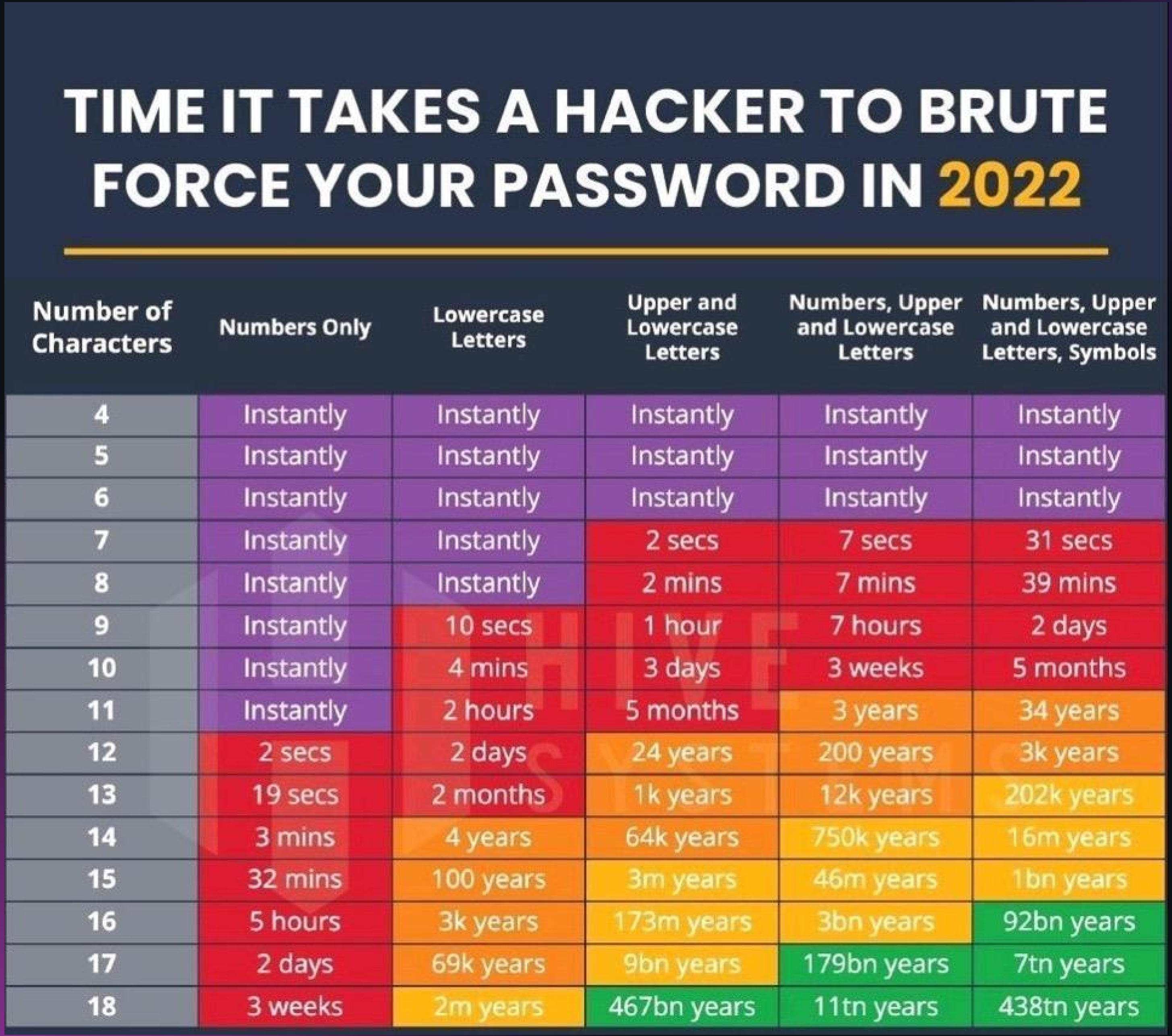
5

2023 Password Decisions Survey

bitwarden

2023 Password Decisions Survey

(“2023 Bitwarden Password Decisions Survey | Bitwarden Blog”)



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 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

This chart tells you how long it takes various brute force techniques to attain your password for a specific account.

This will only be the beginning if a determined hacker has targeted you or your organization.

Most people have heard it is not good to reuse passwords.
Why?

Hackers use tools to harvest credentials from compromised accounts. "…the **threat actor automates authentication** based on previously discovered credentials using customized tools.

This approach can entail **launching millions of attempts** to determine where [users] potentially reused their credentials on another website or application."

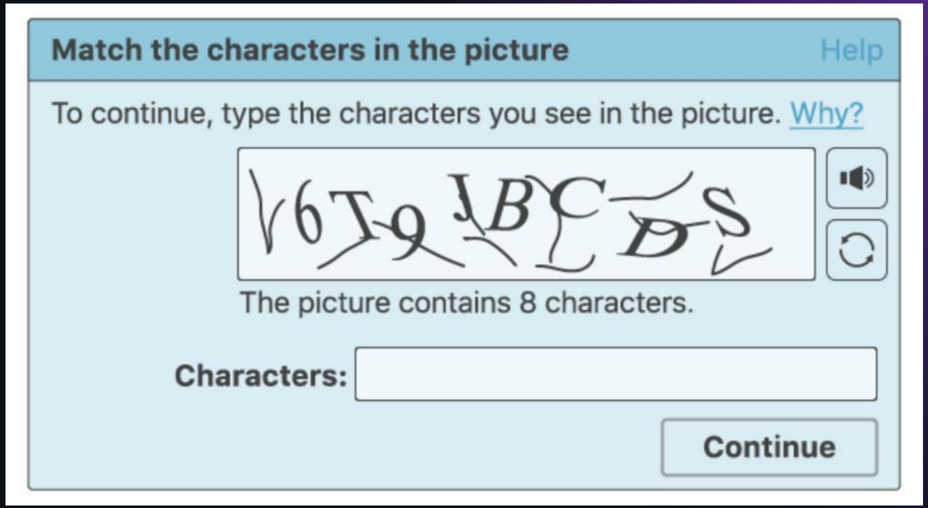
("password cracking 101: attacks & defenses explained | beyondtrust")

Brute force attacks attempt to guess passwords by changing the characters and numbers. To protect against this, companies can limit the number of failed login attempts using a captcha … “captcha is an acronym for ‘completely automated public TURING TEST to tell computers and humans apart.”

(“How captchas work | what does captcha mean? | cloudflare”)

Users often encounter captcha and recaptcha tests on the internet.” Recaptcha protects websites from spam and abuse by distinguishing human users from automated bots using various recaptcha tests. Companies can also require users to use longer passwords.

Captcha example



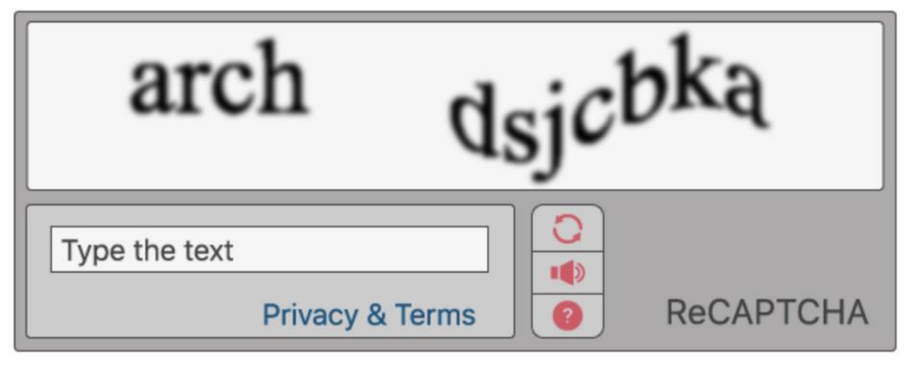
Match the characters in the picture

To continue, type the characters you see in the picture. Why?

The picture contains 8 characters.

Characters:

ReCaptcha example



(“How CAPTCHAs Work | What Does CAPTCHA Mean? | Cloudflare”)

However, a strong password won’t stop a cybercriminal from accessing an account via credential stuffing because the password is already known. Even CAPTCHA's or brute force protection’s ability to protect users is limited since users often change their passwords in predictable patterns, and cyber criminals have a breached password to iterate from. (“What Is Credential Stuffing?”)

Four Easy Steps to Harden Your Sign-On Credentials

01

Using a password management system across multiple platforms saves login time

02

Only change passwords if you suspect an account was compromised

03

Use strong and unique passwords that have randomness and paraphrases

04

Enable multi-factor authentication whenever possible to provide an additional layer of security for online accounts

Artwork created with DALL-E

Works Cited

- @tilpa. “How Long It Would Take a Hacker to Brute Force Your Password in 2022, Ranked - Digg.” Digg.com, digg.com/technology/link/how-long-it-takes-to-get-password-hacked-1IvDFspF6p.
- “2023 Bitwarden Password Decisions Survey | Bitwarden Blog.” Bitwarden, bitwarden.com/blog/password-decisions-survey-2023.
- “Five Best Practices for Password Management | Bitwarden Blog.” Bitwarden, www.bitwarden.com/blog/five-best-practices-for-password-management/.. Accessed 18 Dec. 2022.
- “How CAPTCHAs Work | What Does CAPTCHA Mean? | Cloudflare.” Cloudflare, www.cloudflare.com/learning/bots/how-captchas-work/.
- “Password Cracking 101: Attacks & Defenses Explained | BeyondTrust.” Www.beyondtrust.com, www.beyondtrust.com/blog/entry/password-cracking-101-attacks-defenses-explained.
- “What Is Credential Stuffing?” Auth0 - Blog, auth0.com/blog/what-is-credential-stuffing/.