BACK 2 BASICS

BRIDGING THE GAP BETWEEN HIGHER EDUCATION AND LABOR MARKET BY FOSTERING DIGITAL SKILLS

Bridging the gap between HE and the labour market

2021-1-PT01-KA220-HED-000023543

This project has been funded with support from the European Commission. This publication and all its contents reflect the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the European Union

BACK 2 BASICS

BRIDGING THE GAP BETWEEN HIGHER EDUCATION AND LABOR MARKET BY FOSTERING DIGITAL SKILLS

Module 4

Online security and Data protection

2021-1-PT01-KA220-HED-000023543

This project has been funded with support from the European Commission. This publication and all its contents reflect the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the European Union

Contents

BACK 2 BASICS

BRIDGING THE GAP BETWEEN HIGHER EDUCATION AND LABOR MARKET BY FOSTERING DIGITAL SKILLS

Online security and Data protection

Part 1 – Common Threats | Malware, phishing, social engineering, among others

2021-1-PT01-KA220-HED-000023543

This project has been funded with support from the European Commission. This publication and all its contents reflect the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the European Union

Common threats

Illinois college, hit by ransomware attack, to shut down

Lincoln College, which broke ground in 1865, is one of only a handful of rural American colleges that qualify as predominantly Black institutions by the Department of Education.

Common threats

Illinois college, hit by ransomware attack, shut down

Lincoln College, which broke ground in 1865, is one of only a handful of rural American that qualify as predominantly Black institutions by the Department of Education.

Ransomware attack delays patient care at hospitals across the U.S.

CHI Memorial Hospital in Tennessee, some St. Luke's hospitals in Texas and Virginia Mason Franciscan Health in Seattle all have announced they were affected.

Common threats

Illinois colleg shut down

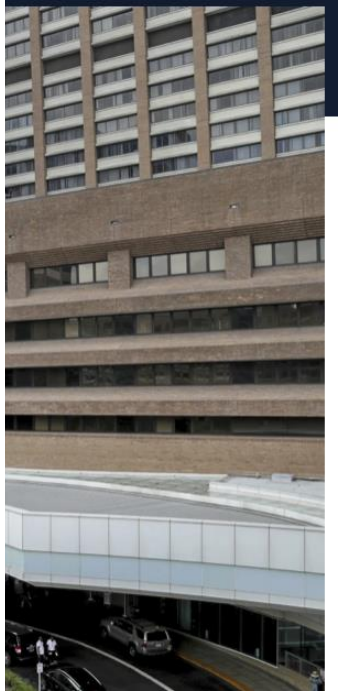
Lincoln College, which brok that qualify as predominantl

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

ent care at

xas and Virginia Mason



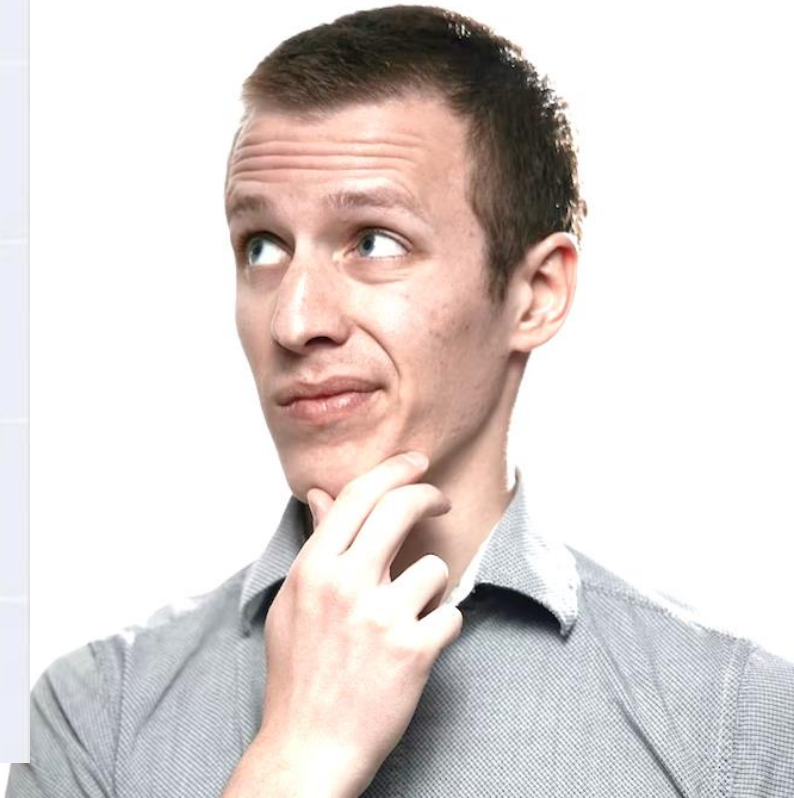
Threats

- Present a risk to secure operations

- Explore
  - Bugs in the applications
  - Insecure communications
  - Bad configurations
  - **Users**

Threats


Mike
wow! you can type your facebook password into a comment and it comes up as stars! too cool!
1 hour ago near Cary
Mike
****
1 hour ago · Like
Katie
OMG ******** That is so cool never knew that!
1 hour ago · Like
Jordan
********** omg it works!
1 hour ago · Like
Catherine
Catherine1234
1 hour ago · Like · 8
Catherine
Ok thats not funny
1 hour ago · Like · 1



BACK 2 BASICS

BRIDGING THE GAP BETWEEN HIGHER EDUCATION AND LABOR MARKET BY FOSTERING DIGITAL SKILLS

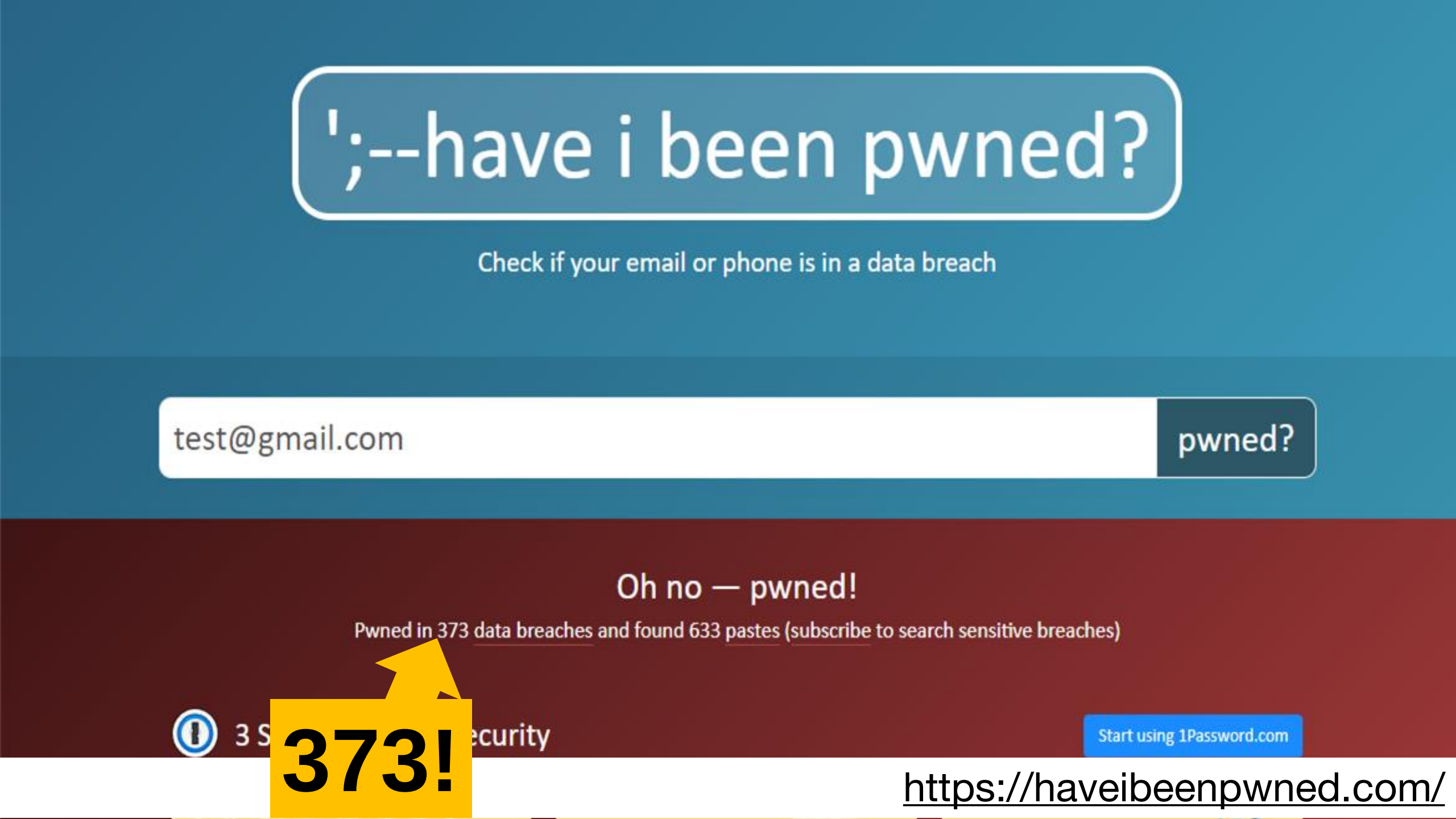
Online security and Data protection

Part 2 - Cyber-hygiene, Best practices

2021-1-PT01-KA220-HED-000023543

This project has been funded with support from the European Commission. This publication and all its contents reflect the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the European Union


';--have i been pwned?
Check if your email or phone is in a data breach
test@gmail.com
pwned?
Oh no — pwned!
Pwned in 373 data breaches and found 633 pastes (subscribe to search sensitive breaches)
3 S ecurity
Start using 1Password.com
373!
https://haveibeenpwned.com/

Protect your workstation

It is the place where work-related tasks are carried out (daily)

Different systems and types of information are available

You are exposed to several risks:

- Paper information within everyone's reach
- Lack of confidentiality in some communication devices (telephone)
- Unsecured devices (unauthorized access)
- Malware infections
- Information theft

Clean desk policy

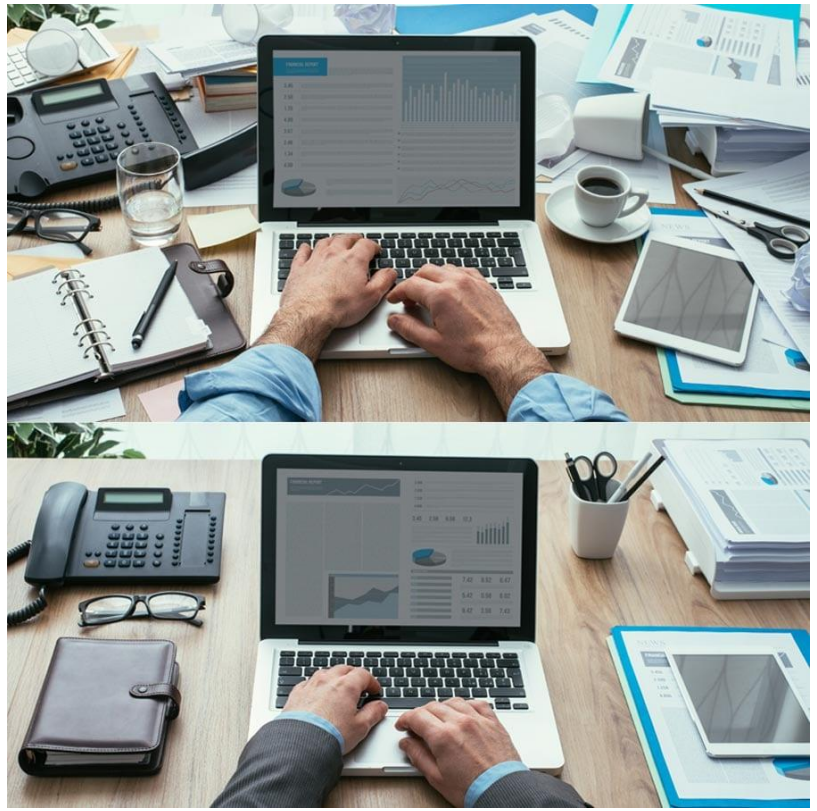
Paper documents left on desks

- For more convenience
- Needed for daily tasks

May contain confidential information

- Personal data of other employees
- Private data relating to projects

What if a colleague copies your work?



Block sessions

Getting up and leaving the computer

- Without blocking the equipment

What if someone accesses the equipment?

- *“That’s is not a problem!”*

Block sessions

Getting up and leaving the computer

- Without blocking the equipment

What if someone accesses the equipment?

- *“That’s is not a problem!”*

Install updates

Applications must be updated to the latest stable version

Ensures they are protected from the latest vulnerabilities

Automatic updates are recommended

- At the operating system level
- As of installed tools

An older version of applications raises more risks

- **Why?**

Install updates

Ransomware attacks in Europe target old VMware, agencies say

Cybersecurity agencies in Europe are warning of ransomware attacks exploiting a 2-year-old computer bug

By The Associated Press
February 6, 2023, 1:59 AM

An older version of applications raises more risks

- **Why?**

Firewall and antivirus

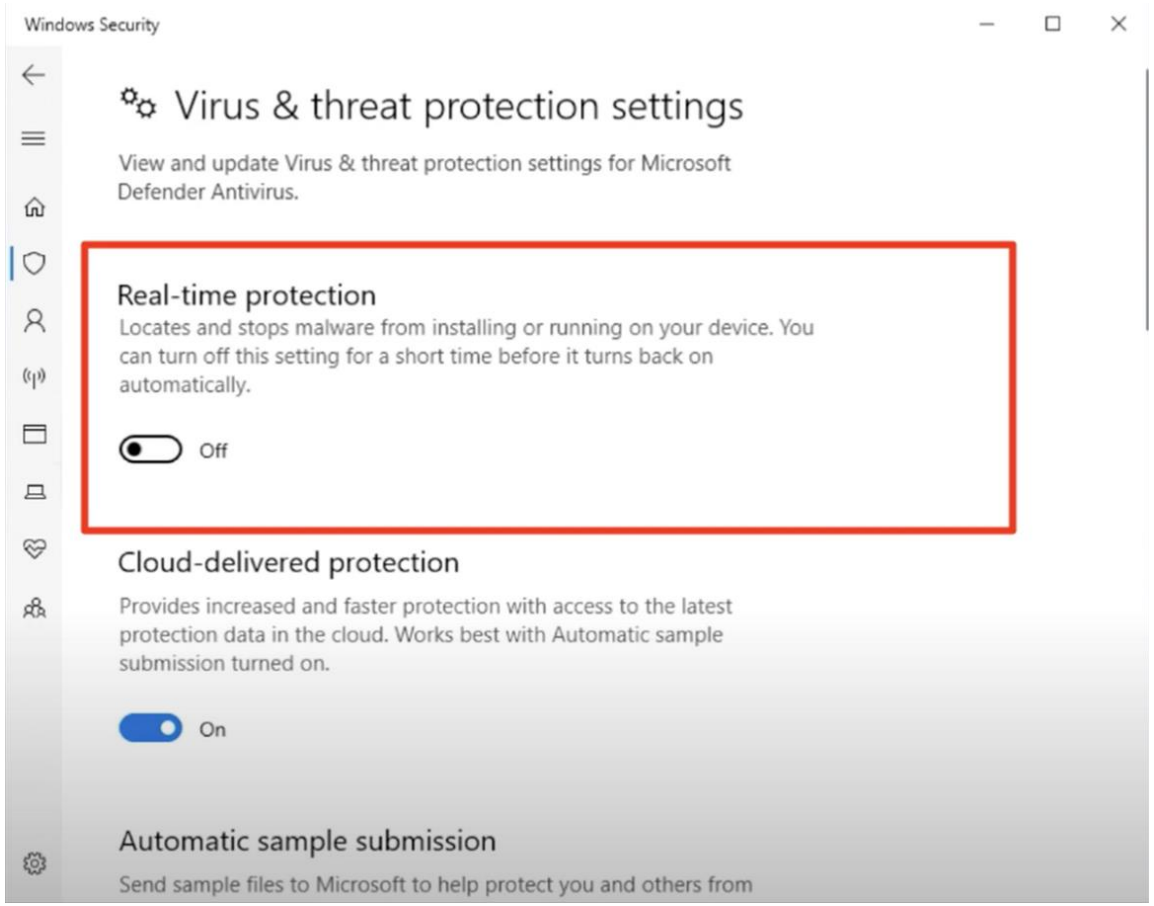
Protect devices from malicious software

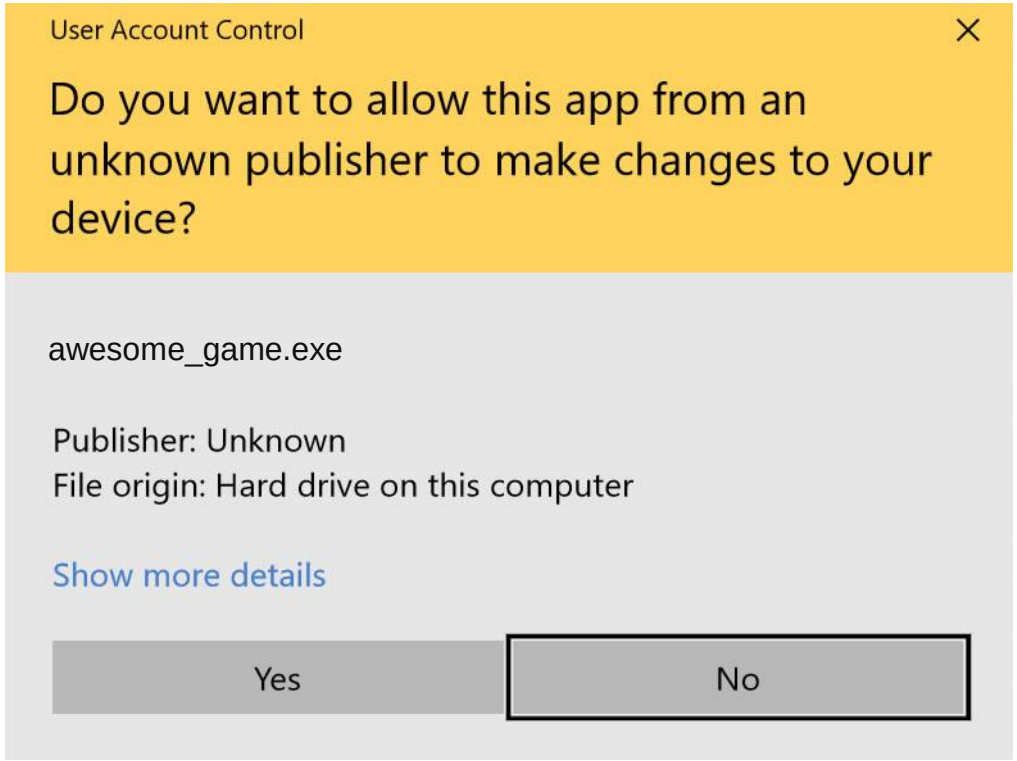
Keeping both up to date is essential

- Updates databases of malware
- Or get new recommendations

When is this extremely important?

Firewall and antivirus





BACK 2 BASICS

BRIDGING THE GAP BETWEEN HIGHER EDUCATION AND LABOR MARKET BY FOSTERING DIGITAL SKILLS

Online security and Data protection

Part 3 - Risks of weak password, Understanding the impact of different attacks

2021-1-PT01-KA220-HED-000023543

This project has been funded with support from the European Commission. This publication and all its contents reflect the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the European Union

How do hackers think?

There are different ways to obtain your password

The most common are when the password is:

- stored in compromised database
  - in clear text
  - represented using hashes
- intercepted in a communication
  - for instance, in an unprotected network

How do hackers think?

Attackers can test whether a password is correct

- They can perform thousands or millions of attempts per second.

Blindly

- Brute Force attacks use all possible combinations

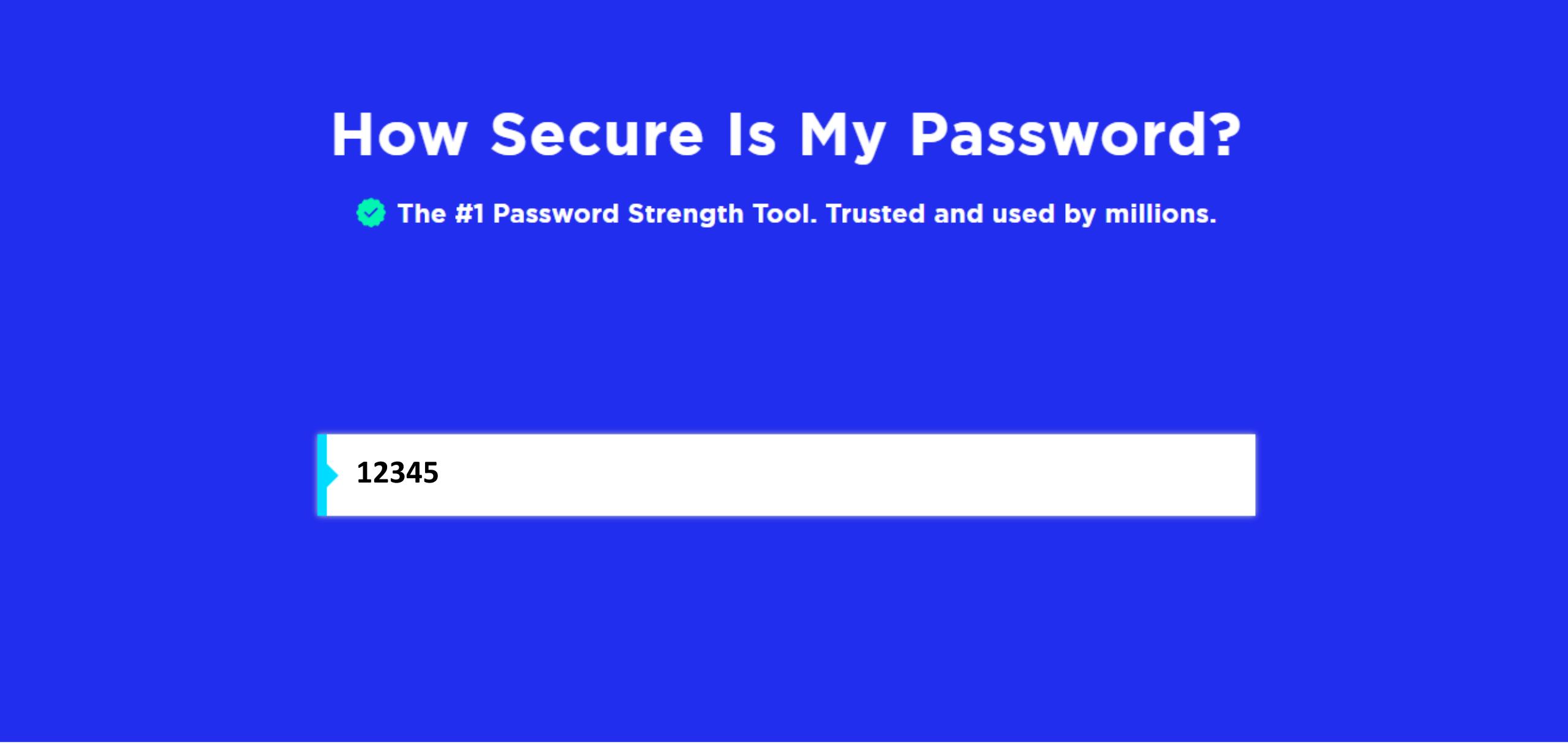
Exploiting weaknesses

- Dictionary attacks with common symbols

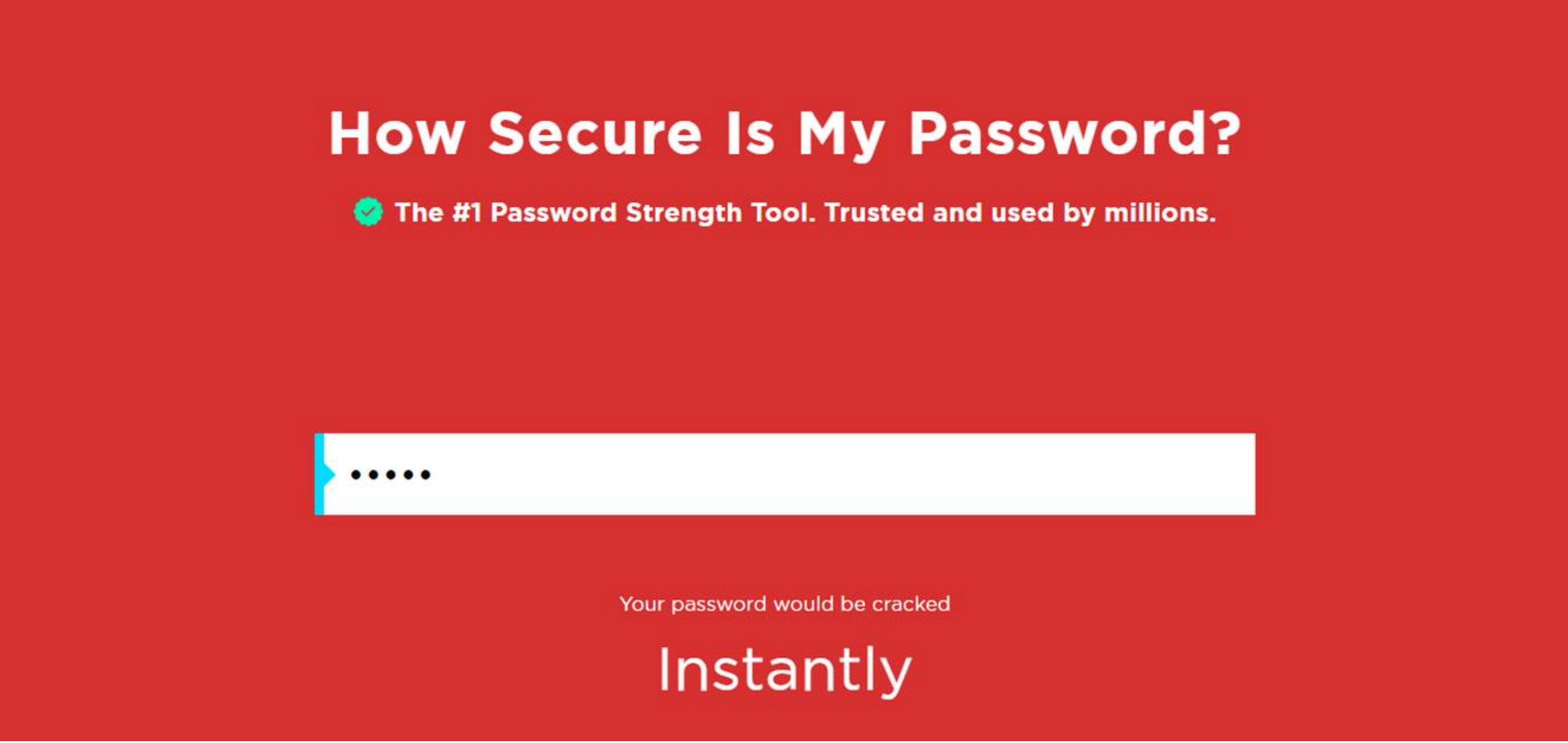
What is a strong password?

Top 10 passwords most used in 2023

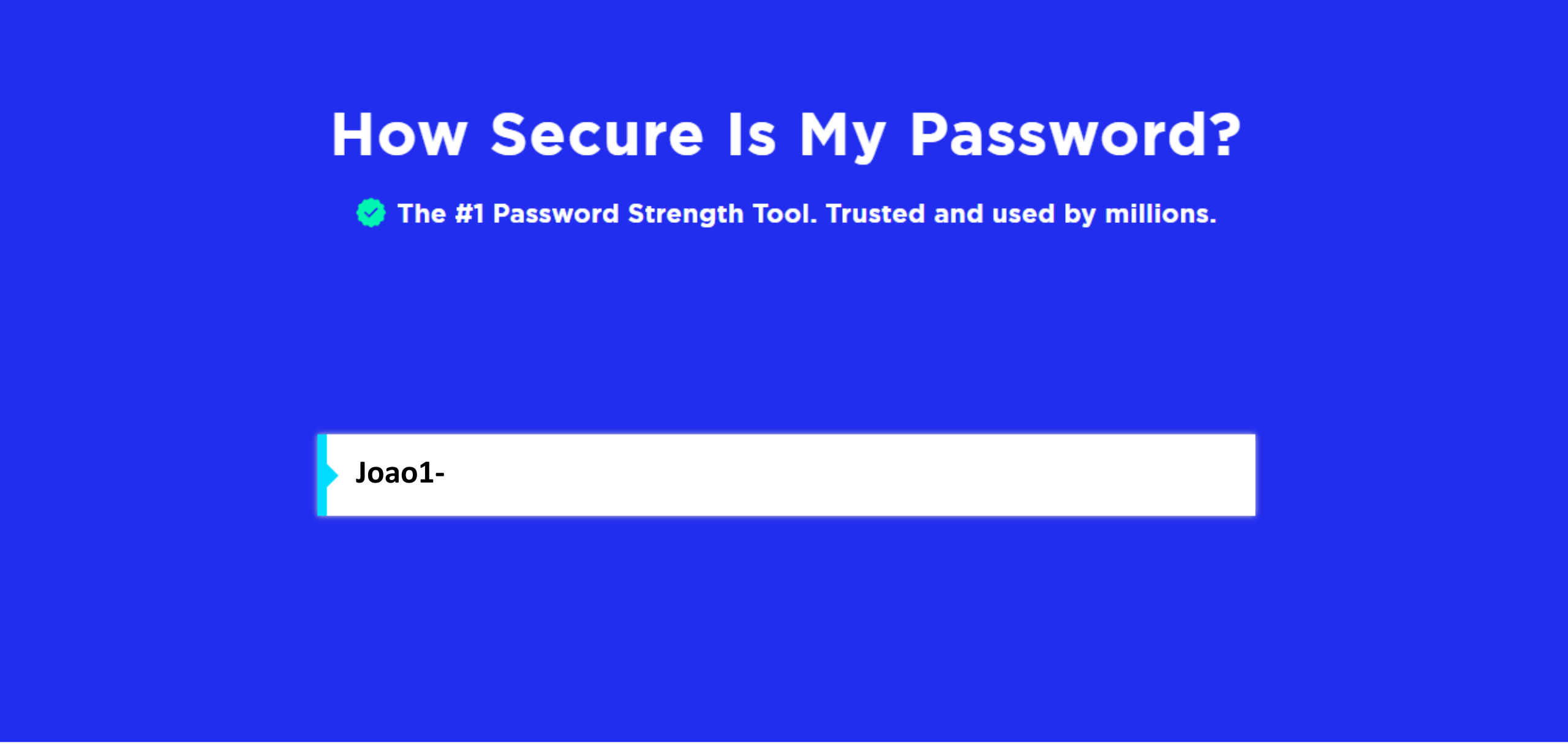
1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890



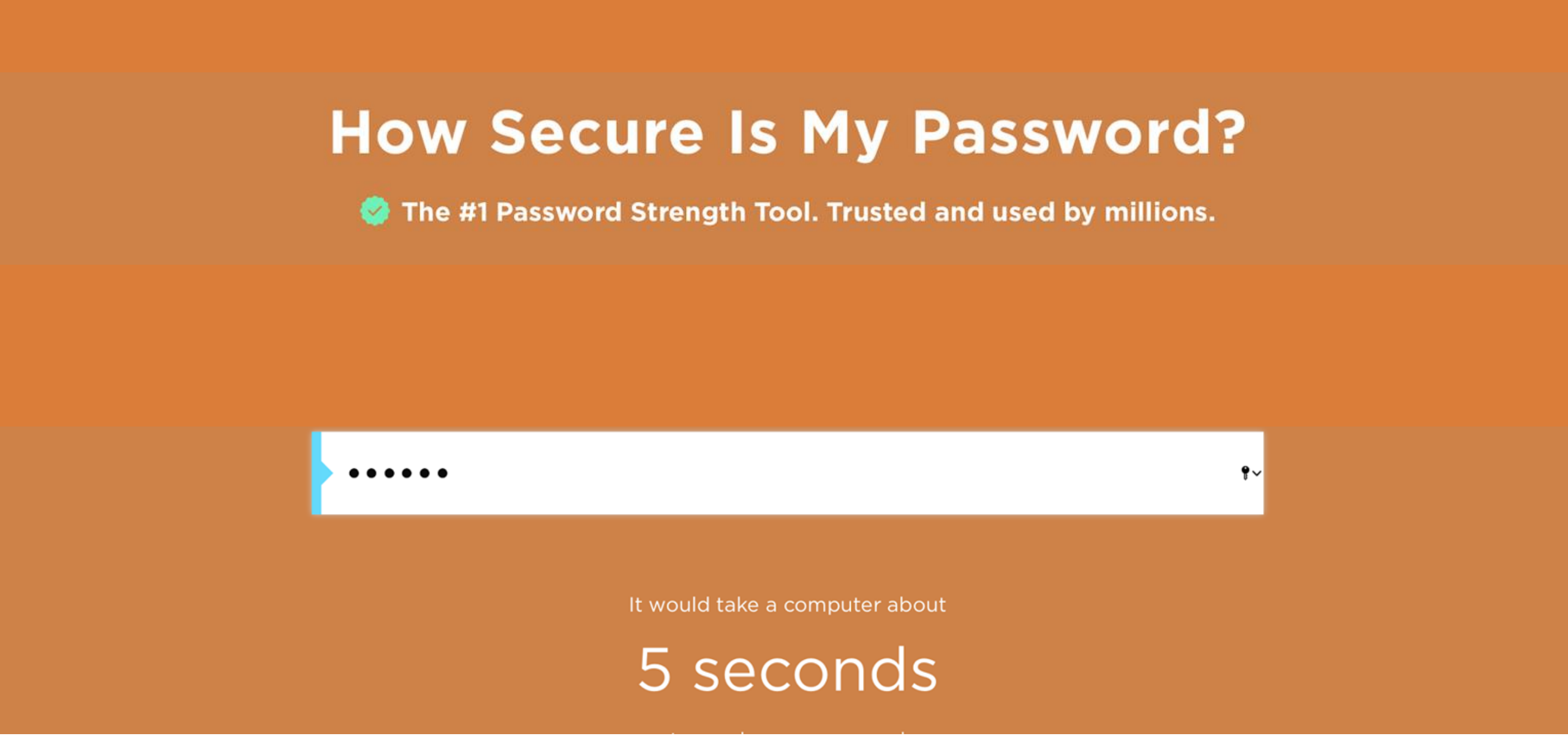
https://www.security.org/how-secure-is-my-password/



https://www.security.org/how-secure-is-my-password/



https://www.security.org/how-secure-is-my-password/



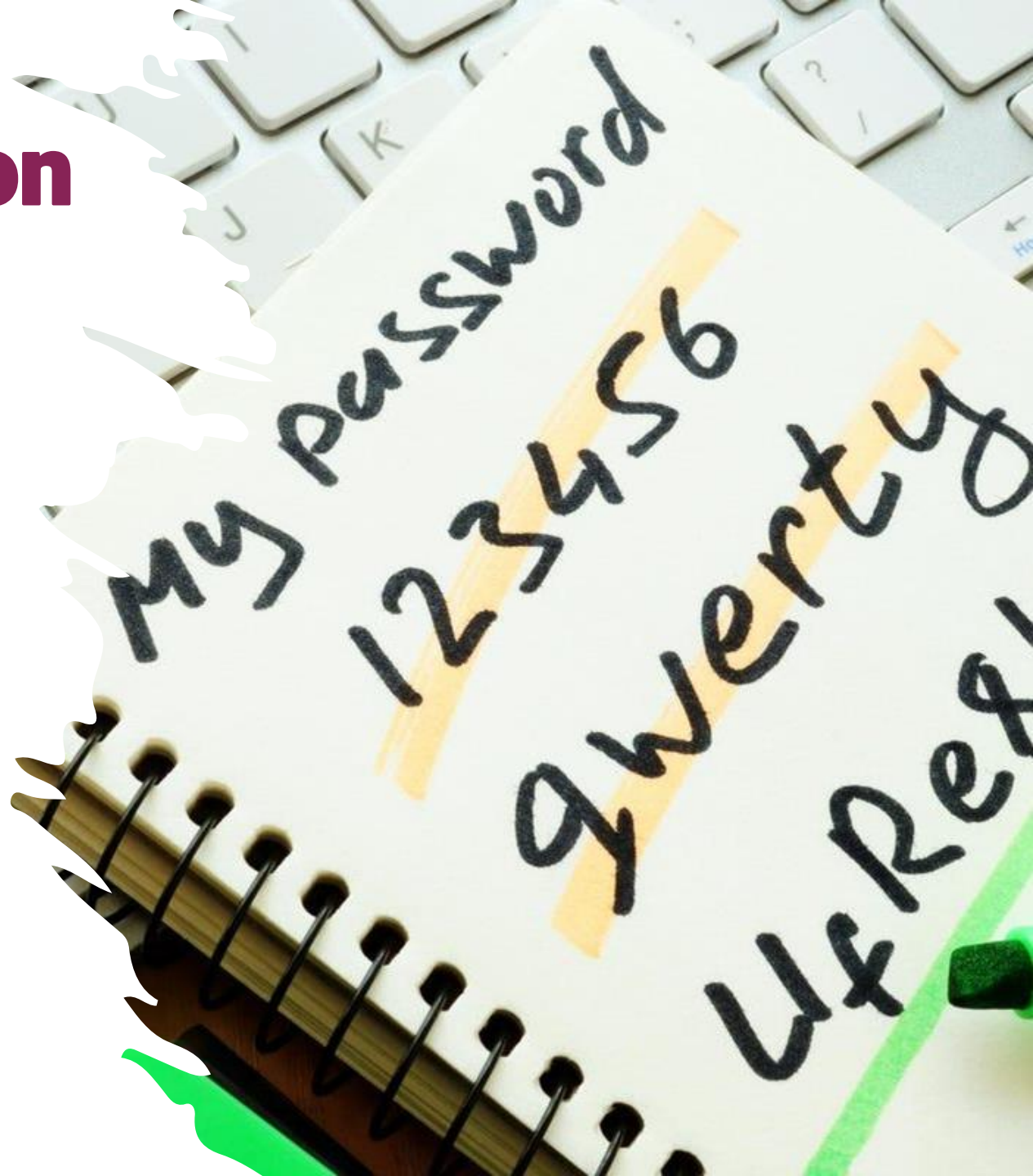
https://www.security.org/how-secure-is-my-password/

Password reutilization

It is easy to generate a safe password

- For instance: 5zRY[wWM}zU/'$ws+C%jXVR

How can you handle 10, 100, 1000 passwords? Oops…



Password reutilization

Attackers exploit vulnerable services and acquire passwords

Password reutilization

Attackers will sell and use them to attack users and systems

Check if your password was exposed

There are services online to check for exposed accounts

- F-secure
- Cybernews
- Intelligence X (my favourite but is currently down for updates)

Sometimes they are paid

- But you can have an idea which platforms leaked your information

F-secure

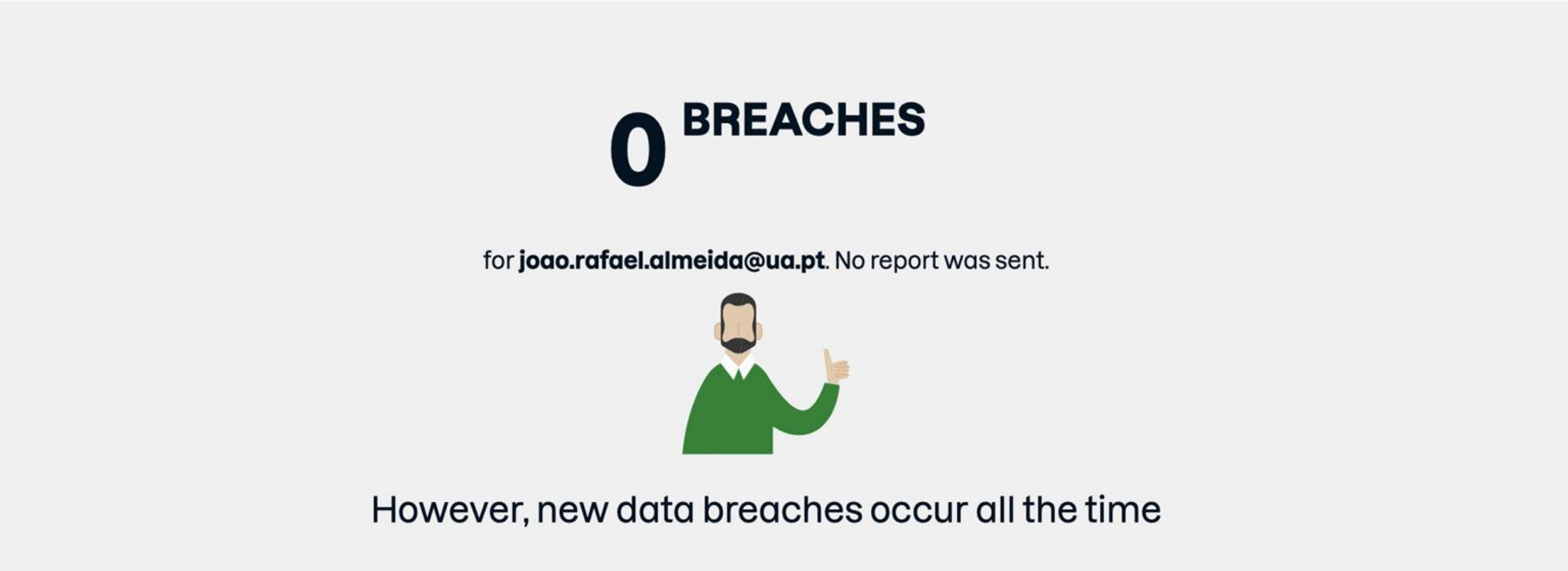
Check if your personal information has been exposed

Type your email address here

Check for breaches

https://www.f-secure.com

F-secure



https://www.f-secure.com

F-secure

6 breach(es) that contain your personal information:

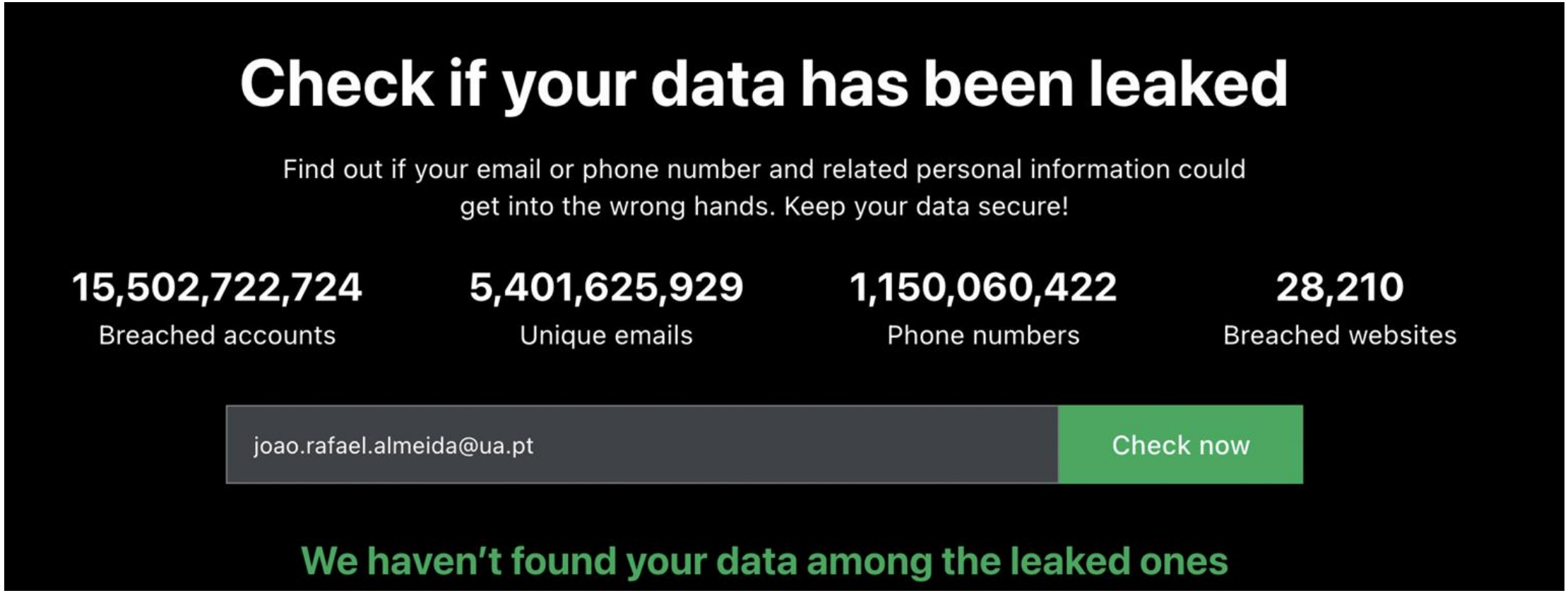
The date mentioned is the date the data breach was discovered.

Breached Service	Exposed data
Canva 06/2019	Email address , Full name , Username
Collection Combo List 02/2019	Email address , Password
Collection Combo List 01/2019	Email address , Password
Undisclosed Service 11/2018	Email address , First name , Full name , Last name
Warmane.com 01/2018	Email address , Password
Warmane Forums 11/2017	Email address , Password , Username

Cybernews

https://cybernews.com/personal-data-leak-check/

Cybernews



https://cybernews.com/personal-data-leak-check/

BACK 2 BASICS

BRIDGING THE GAP BETWEEN HIGHER EDUCATION AND LABOR MARKET BY FOSTERING DIGITAL SKILLS

Online security and Data protection

Part 4 – Recommendations, Learning how to define strong passwords

2021-1-PT01-KA220-HED-000023543

This project has been funded with support from the European Commission. This publication and all its contents reflect the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the European Union

Recommendations for strong passwords

Never reuse keywords

Never share a keyword

Authentication with multi-factor

- More about this in a few minutes

Adopt a password manager

- For example, Vault HashiCorp

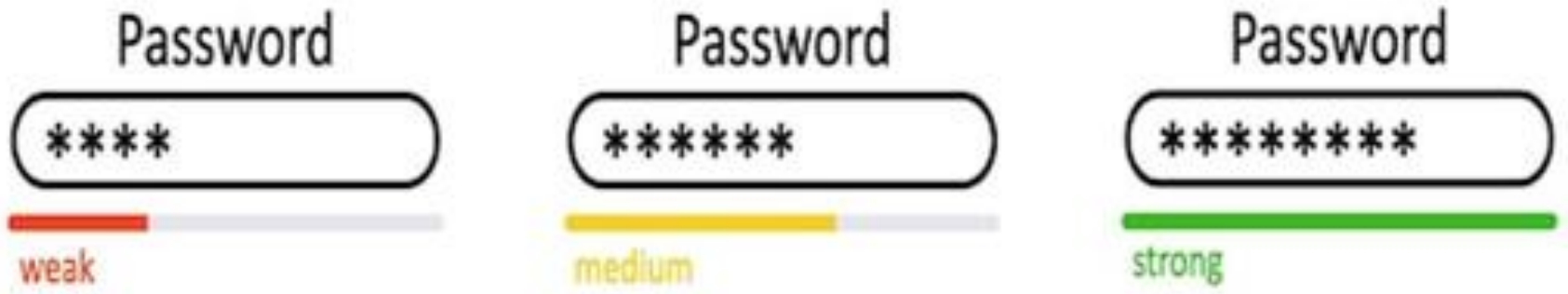
Length

Make your passwords long

Minimum length of 15 characters

- The longer the better

The minimum of 8 is no longer enough. Why?



Length

Example

- Alphabet of 62 characters
  - 26 lower case characters
  - 26 upper case characters
  - 10 possible digits

- Cracking time
  - 10 000 000 000 of passwords per second
  - This number can be higher

Length

Possible combinations = Number of characters$^{\text{Password length}}$

Time to test = Possible combinations / Passwords per second

Password length	Number of possible combinations	Time to test them all
5	62^5 = 916 132 832	0,09 sec
6	62^6 = 56 800 235 584	5 sec
8	62^8 = 218 340 105 584 896	6 hours
15	$62^{15} = 7{,}689 \times 10^{26}$	2 438 196 680 years
20	$62^{20} = 7{,}044 \times 10^{25}$	$2{,}23 \times 10^{18}$ years

Complexity

Combinations of all possible character types

- Uppercase and lowercase, numbers and symbols
- For instance, use the word “João” instead of “joao”

Using the same example

- Alphabet of ~~62~~ **94** characters
  - 26 lower case characters
  - 26 upper case characters
  - 10 possible digits
  - **32 special characters**

Complexity

Greatly increases the number of possible combinations

- 8 times only for 5-length passwords (4 118 for 20-length passwords)

Password length	Number of possible combinations	Time to test them all
5	$94^5 = 7\ 339\ 040\ 224$	0,7 sec
6	$94^6 = 6{,}899 \times 10^{11}$	68 sec
8	$94^8 = 6{,}096 \times 10^{15}$	7 days
15	$94^{15} = 3{,}953 \times 10^{29}$	$1{,}3 \times 10^{12}$ years
20	$94^{20} = 2{,}901 \times 10^{39}$	$9{,}2 \times 10^{21}$ years

How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

João_Almeida_likes_dogs!2

https://www.security.org/how-secure-is-my-password/

https://www.security.org/how-secure-is-my-password/

Strong passwords

We solved one part of the problem

- Brute force attacks

Dictionary attacks can be more personalized

- Using information available on social networks
- For instance, dates, names, relatives, etc.

Things to avoid

Do not use the same password in different platforms

- Even when these do not contain important information
- Instead, generate random password that you don’t need to memorize

Do not use predictable patterns

Dictionary words (in any language)

Words spelled backwards, abbreviations or common misspellings

Personal information, like name, dog’s name, birthdates, etc.

BACK 2 BASICS

BRIDGING THE GAP BETWEEN HIGHER EDUCATION AND LABOR MARKET BY FOSTERING DIGITAL SKILLS

Online security and Data protection

Part 5 - More robust authentication, Multi-factor authentication

2021-1-PT01-KA220-HED-000023543

This project has been funded with support from the European Commission. This publication and all its contents reflect the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the European Union

That was not enough

We cannot stop data breach

- But you can make your password less useful to hackers

How?

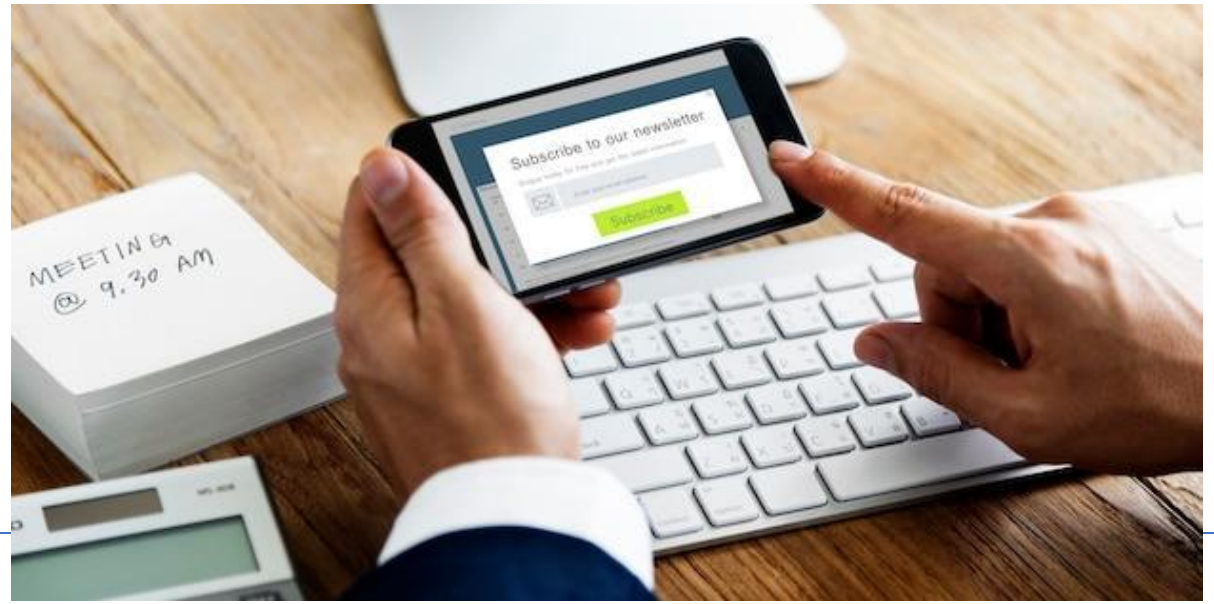
- Using multi-factor authentication

What is Multi-Factor Authentication?

It is a process to identify a person multiple ways

It **insures a stolen password** itself

Doesn't lead to a stolen **email, banking, or social media account**



What is Multi-Factor Authentication?

Something you
KNOW

Password or phrase
PIN

Something you
HAVE

Code from app or SMS
Push notification
USB token

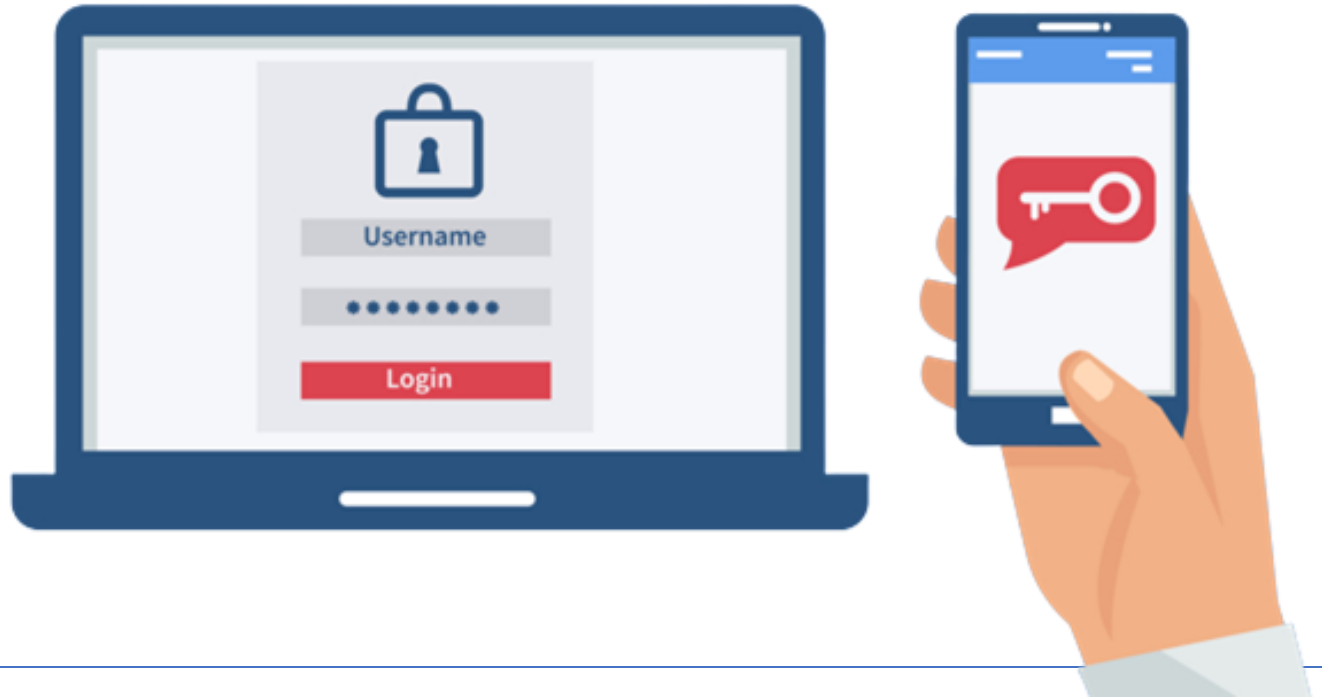
Something you
ARE

Finger or thumb print
Face scan
Iris scan

Why is it important?

A message is sent every time someone is authenticated

- If was not you, you will know



Examples

- Log into website, then receive one-time password via email or SMS
- Access VPN with password, answer prompt in app on a mobile device
- Access corporate network via USB device and password
- Enter high security facility with retina scan and code/pin

Downsides

Sometimes it is inconvenient

- Take extra time to log in
- Can’t log in without a device (well, not really)

Some implementations provide a list of codes for emergencies

- That should be carefully protected

Can cause issues with applications

- That depending on this implementation

BACK 2 BASICS

BRIDGING THE GAP BETWEEN HIGHER EDUCATION AND LABOR MARKET BY FOSTERING DIGITAL SKILLS

Online security and Data protection

Part 6 - More robust authentication, Certificate-based authentication

2021-1-PT01-KA220-HED-000023543

This project has been funded with support from the European Commission. This publication and all its contents reflect the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the European Union

Overview

Certificate is a digital document that includes

- Distinguished Name (DN)
- Associated public key

The certificate is digitally signed by a trusted third party

- Known as Certificate Authority (CA)

It is stronger as compared to password based authentication

It expects that the users **has** something

- Rather than **know** something

How it works?

It uses asymmetric encryption

Operates in two stages

1. Certificate distribution
2. Authentication

Certificate distribution

The user receives or generates a pair of keys

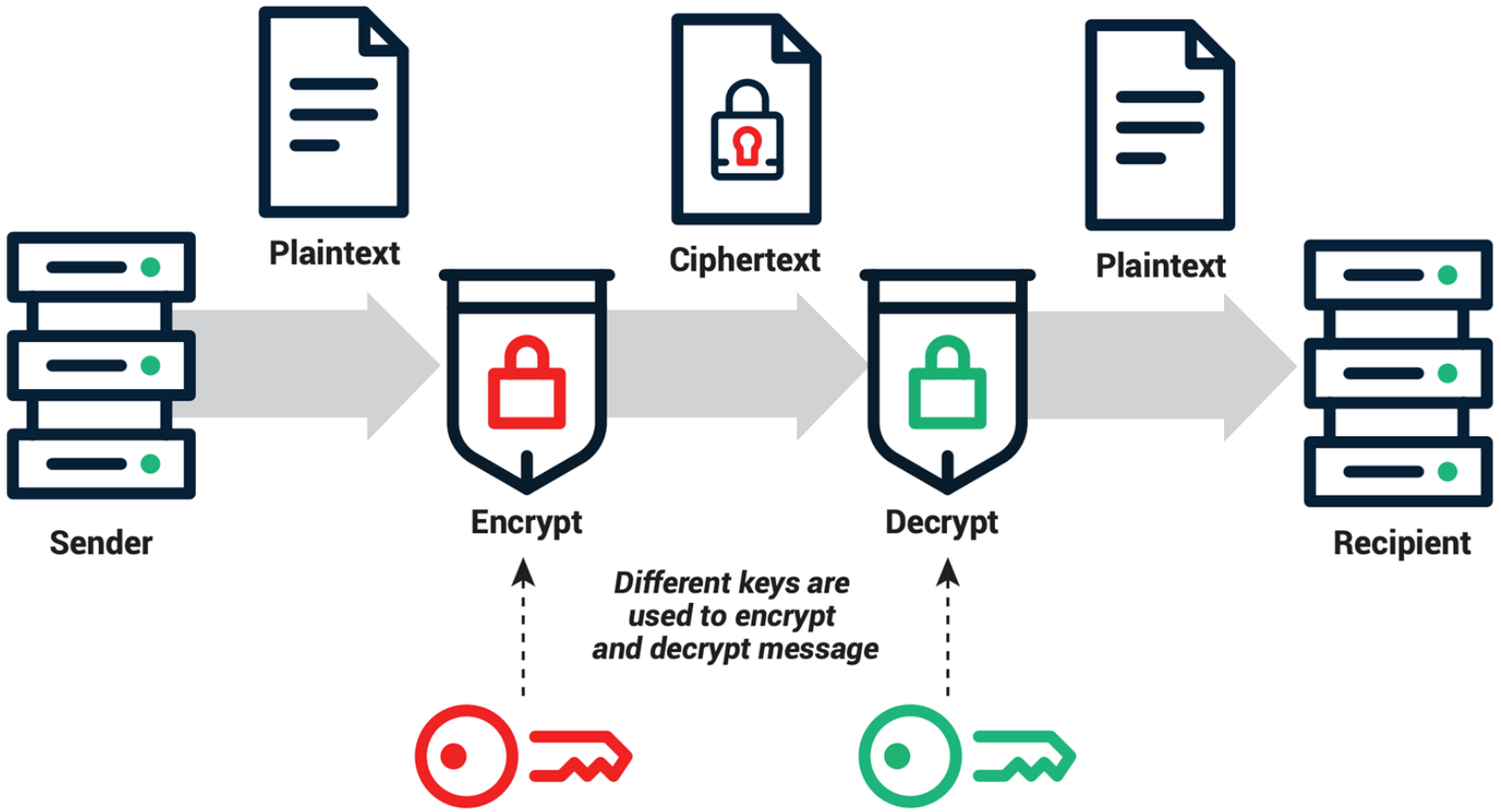
- Private and public keys

Different strategies can be used for distribution

- It depends on the use case

Certificates validate the authenticity of the public keys

Private and public keys



Authentication

The user receives a challenge

- It can be a random message

The challenge is encrypted with the user's private key

- Everyone can decrypt this message
- As long the person knows the user's public key

But this validates that only the user can create this encryption

Why?

Use cases

HTTPS protocol

- Now you know the meaning of the “s” at the end of the http://

Connections between machines

Connection to remote servers

- Password based authentication can be used
- But certificate-based is much more secure

Important

Private key means that the key is PRIVATE

BACK 2 BASICS

BRIDGING THE GAP BETWEEN HIGHER EDUCATION AND LABOR MARKET BY FOSTERING DIGITAL SKILLS

Group discussion

Part 1

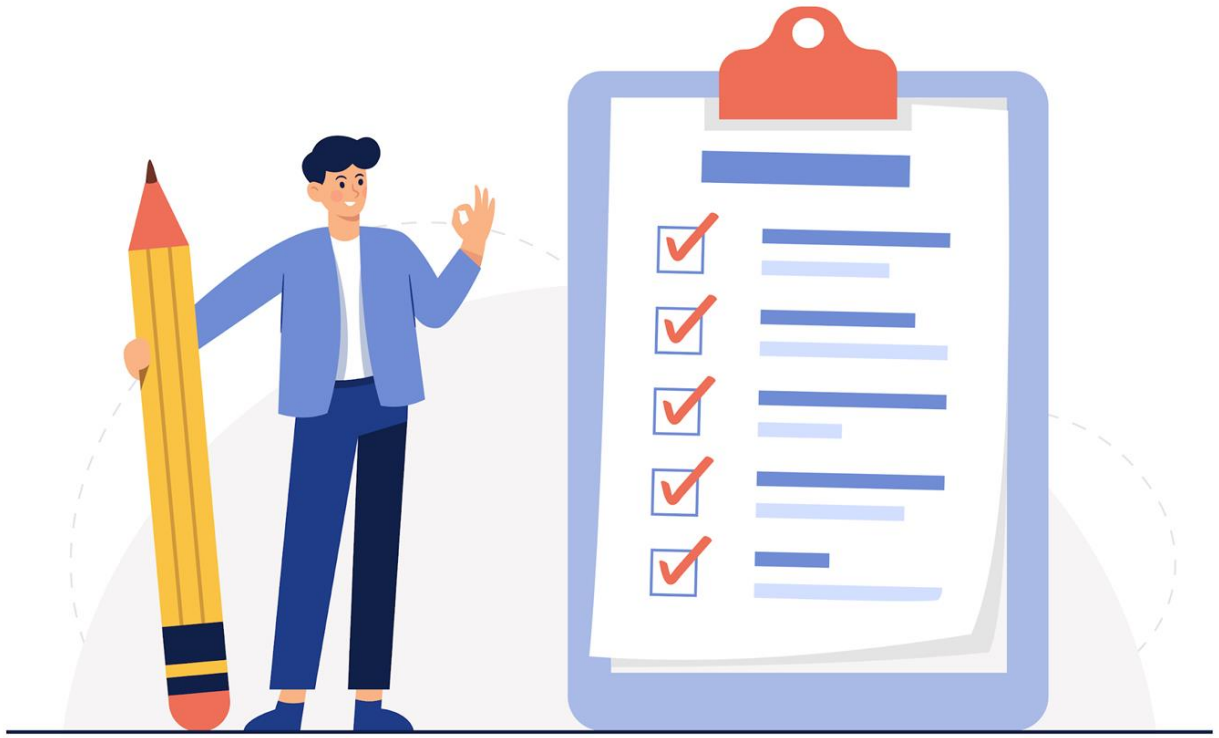
2021-1-PT01-KA220-HED-000023543

This project has been funded with support from the European Commission. This publication and all its contents reflect the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the European Union

Task

The teachers should write down the oral intervention individually, from memory, describing the main concepts



BACK 2 BASICS

BRIDGING THE GAP BETWEEN HIGHER EDUCATION AND LABOR MARKET BY FOSTERING DIGITAL SKILLS

Group discussion

Part 2

2021-1-PT01-KA220-HED-000023543

This project has been funded with support from the European Commission. This publication and all its contents reflect the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the European Union

Task

The teachers should compare and complete their notes with their neighbour in the row (groups 2 elements), and then to discuss in group, 3-4 elements, to complete the notes

BACK 2 BASICS

BRIDGING THE GAP BETWEEN HIGHER EDUCATION AND LABOR MARKET BY FOSTERING DIGITAL SKILLS

Gamified experience

Creating a strong password
https://tinyurl.com/2js5dv5c

2021-1-PT01-KA220-HED-000023543

This project has been funded with support from the European Commission. This publication and all its contents reflect the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the European Union

BACK 2 BASICS

BRIDGING THE GAP BETWEEN HIGHER EDUCATION AND LABOR MARKET BY FOSTERING DIGITAL SKILLS

Recap

2021-1-PT01-KA220-HED-000023543

This project has been funded with support from the European Commission. This publication and all its contents reflect the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the European Union

Important topics

- We cannot escape from threats
- But we can increase our defences
- Strong passwords make the difference
- Multi-Factor Authentication mechanisms are annoying but important

BACK 2 BASICS