Passwords *(Passwörter)*

An introduction to cybersecurity

25.01.2024, Lili Wilson

What is cybersecurity? *(Internet-Sicherheit)*

What is cybersecurity? *(Internet-Sicherheit)*

- Protect computers from **attacks** *(Angriffe)*

What is cybersecurity? *(Internet-Sicherheit)*

- Protect computers from **attacks** *(Angriffe)*

Big goals:

- **Secrecy** *(Geheimhaltung)*
- **Integrity** *(Integrität)*
- **Availability** *(Verfügbarkeit)*

What is cybersecurity? *(Internet-Sicherheit)*

Authentication *(Authentifizierung)*

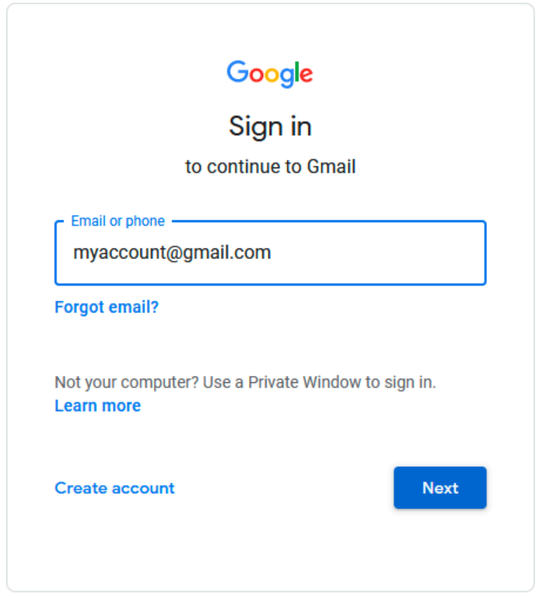
What is cybersecurity? *(Internet-Sicherheit)*

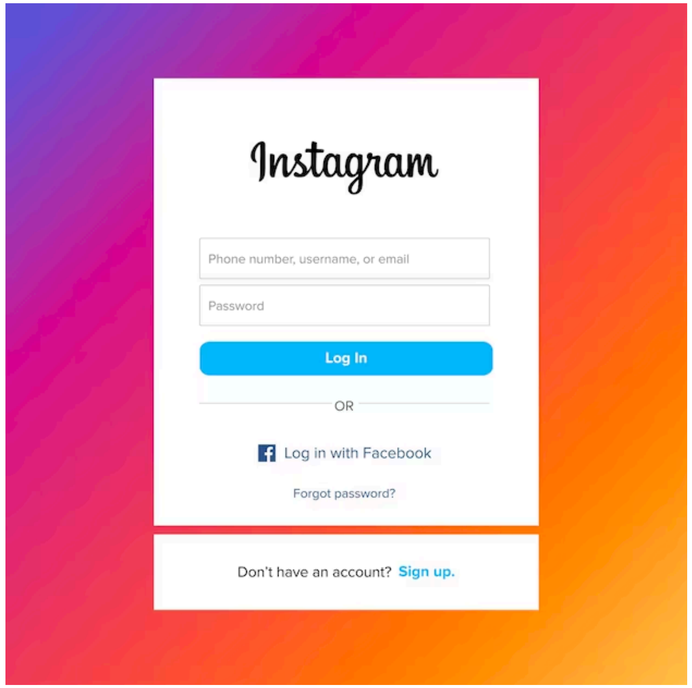
Authentication *(Authentifizierung):* prove that you are who you say you are

What is cybersecurity? *(Internet-Sicherheit)*

Authentication *(Authentifizierung):* prove that you are who you say you are

Passwords!



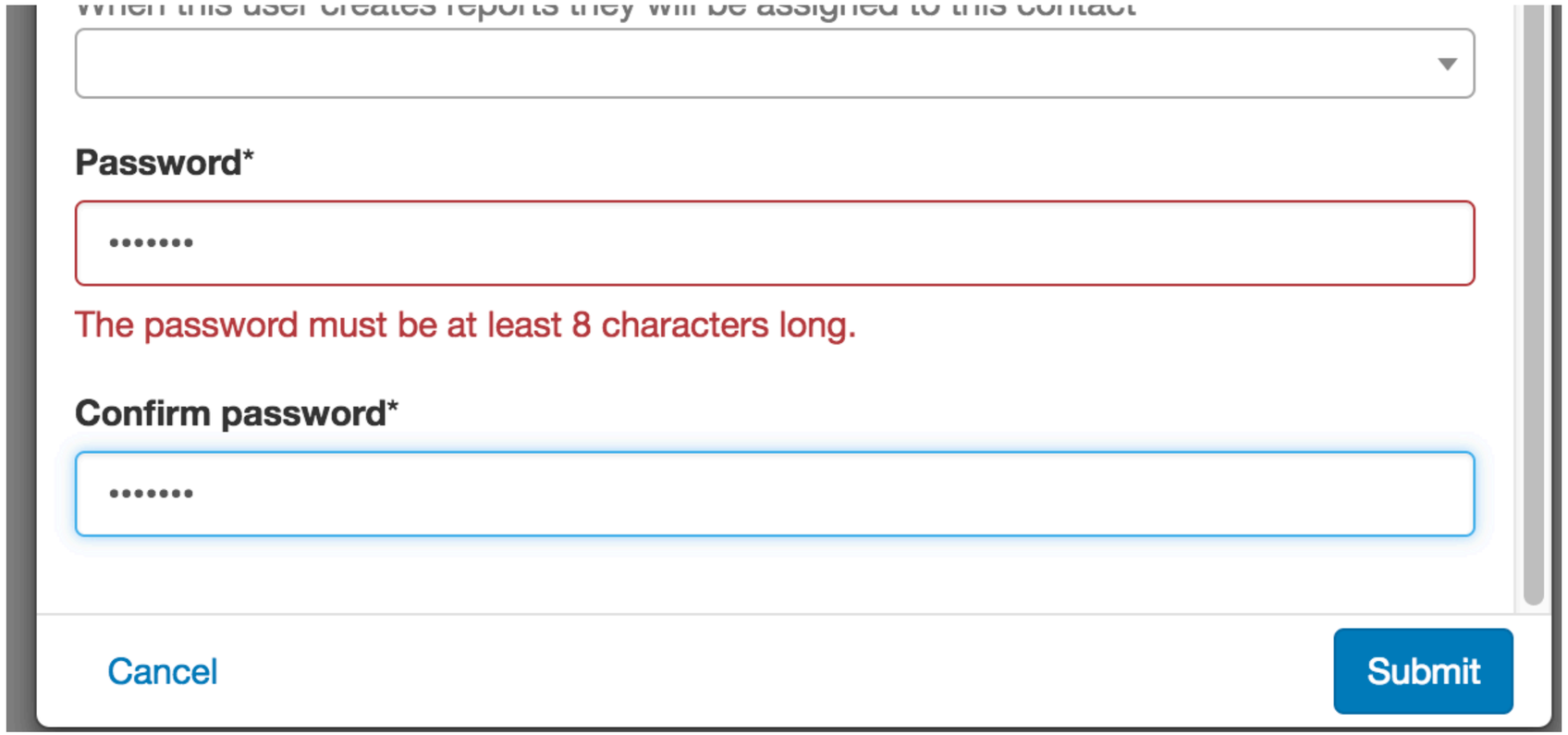


Passwords

What is some typical advice for making a password?

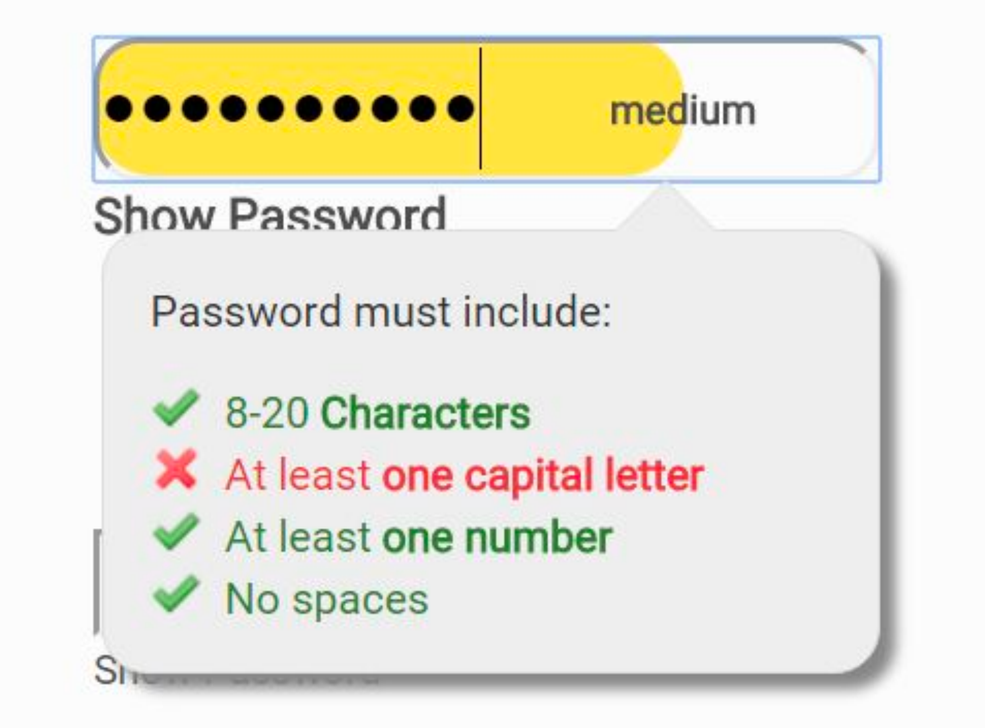
Passwords

What is some typical advice for making a password?



Passwords

What is some typical advice for making a password?



Passwords

What is some typical advice for making a password?

Password Requirements

- ✗ MUST contain at least 8 characters (12+ recommended)
- ✗ MUST contain at least one uppercase letter
- ✗ MUST contain at least one lowercase letter
- ✗ MUST contain at least one number
- ✗ MUST contain at least one special character (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~)
- ✓ MAY NOT contain more than two identical characters in a row
- ✓ MAY NOT contain first name, last name, email address mailbox or domain, company name or commonly used passwords
- ✓ MAY NOT match commonly used password character patterns

5 remaining rules need to be met

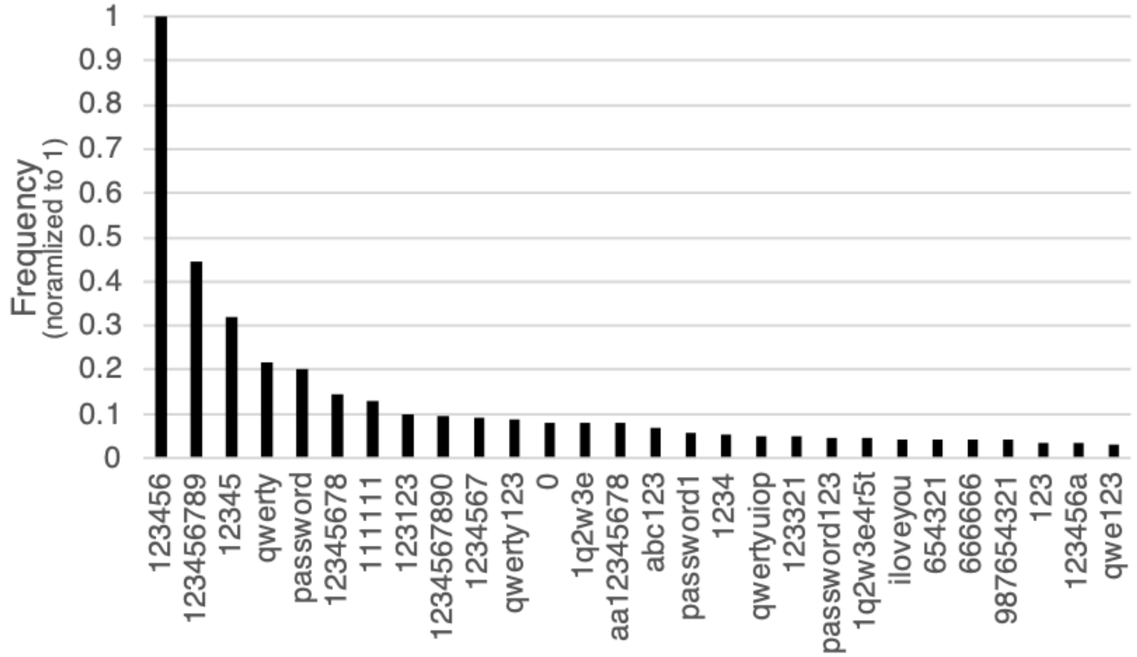
create a very strong password for me

Password statistics

80% of data breaches are a result of poor password choice and management

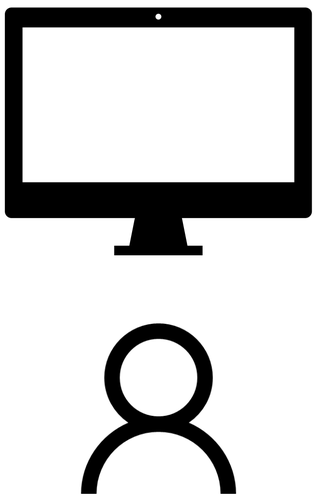
~60% of users create passwords containing their names or birthdays

almost **25%** of people use the same password, or a variation of the same password for multiple accounts

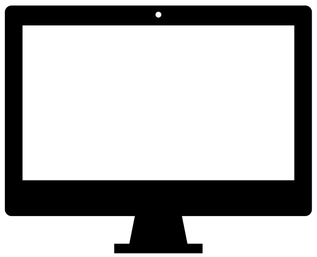


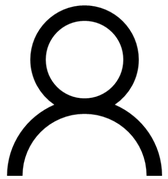
https://www.verizon.com/business/en-au/resources/articles/analyzing-covid-19-data-breach-landscape/, https://www.passwordmanager.com/password-manager-trust-survey/, https://nordpass.com/most-common-passwords-list/

Password storage



Password storage

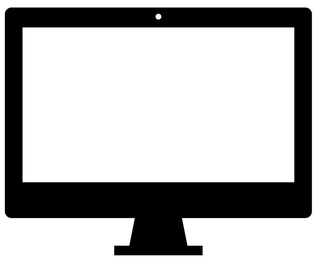




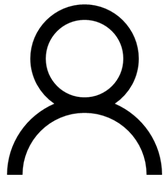
Microsoft

```
username: bob
password: iambob
```

Password storage

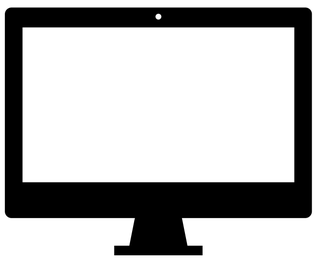


can i log into teams please?



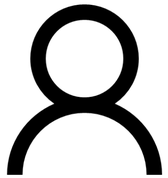
```
username: bob
password: iambob
```

Password storage



can i log into teams please?

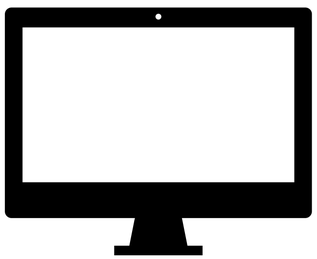
is the password they gave me bob's password?



`username: bob`

`password: iambob`

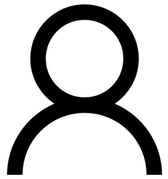
Password storage



can i log into teams please?

Microsoft

is the password they gave me bob's password?



`username: bob`

`password: iambob`

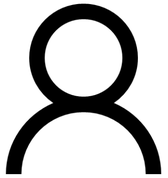
Attempt 1: storing plaintext

username	password
user1	adfjsksshfds
user2	vcncxmnskfh
user3	qwpeeruwrew
bob	iambob
user5	cbxmpsfqpew
user6	irewioosfdks
user7	owriuakdfbvx
user8	fldsasdjdhfj

Attempt 1: storing plaintext

username	password
user1	adfjsksshfds
user2	vcncxmnskfh
user3	qwpeeruwrew
bob	iambob
user5	cbxmpsfqpew
user6	irewioosfdks
user7	owriuakdfbvx
user8	fldsasdjdhfj

can i log into teams please?



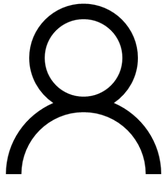
username: bob

password: iambob

Attempt 1: storing plaintext

username	password
user1	adfjsksshfds
user2	vcncxmnskfh
user3	qwpeeruwrew
bob	iambob
user5	cbxmpsfqpew
user6	irewioosfdks
user7	owriuakdfbvx
user8	fldsasdjdhfj

can i log into teams please?

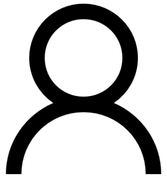


username: bob

password: iambob

Attempt 1: storing plaintext

username	password
user1	adfjsksshfds
user2	vcncxmnskfh
user3	qwpeeruwrew
bob	iambob
user5	cbxmpsfqpew
user6	irewioosfdks
user7	owriuakdfbvx
user8	fldsasdjdhfj



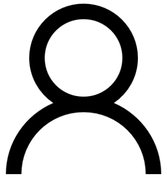
can i log into teams please?

`username: bob`

`password: iambob`

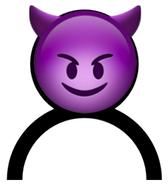
Attempt 1: storing plaintext

username	password
user1	adfjsksshfds
user2	vcncxmnskfh
user3	qwpeeruwrew
bob	iambob
user5	cbxmpsfqpew
user6	irewioosfdks
user7	owriuakdfbvx
user8	fldsasdjdhfj



can i log into teams please?

```
username: bob
password: iambob
```

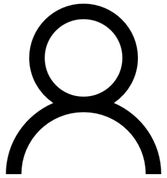


can i log into teams please?

```
username: bob
password: NotBob
```

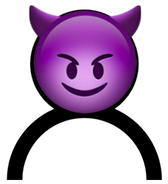
Attempt 1: storing plaintext

username	password
user1	adfjsksshfds
user2	vcncxmnskfh
user3	qwpeeruwrew
bob	iambob
user5	cbxmpsfqpew
user6	irewioosfdks
user7	owriuakdfbvx
user8	fldsasdjdhfj



can i log into teams please?

```
username: bob
password: iambob
```



can i log into teams please?

```
username: bob
password: NotBob
```

Attempt 1: storing plaintext (problems)

username	password
user1	adfjsksshfds
user2	vcncxmnskfh
user3	qwpeeruwrew
bob	iambob
user5	cbxmpsfqpew
user6	irewioosfdks
user7	owriuakdfbvx
user8	fldsasdjdhfj

What happens if an attacker (😈) can already see this table?

Attempt 2: encrypting

Attempt 2: encrypting

What is **encryption**? *(Verschlüsselung)*

Attempt 2: encrypting

What is **encryption**? *(Verschlüsselung)*

Hello world!

plaintext

(Klartext)

Attempt 2: encrypting

What is **encryption**? *(Verschlüsselung)*

encrypt

(verschlüsseln)

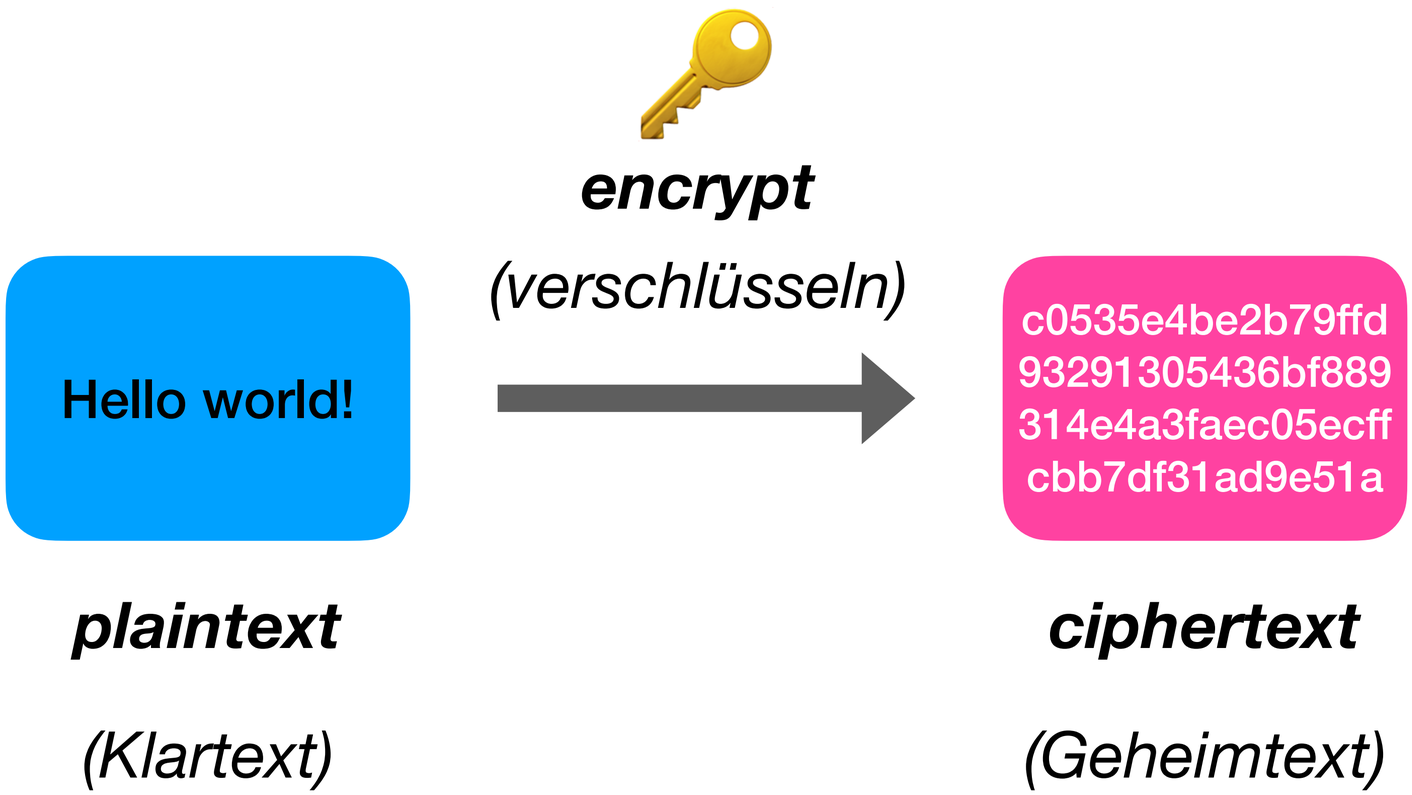
Hello world!

plaintext

(Klartext)

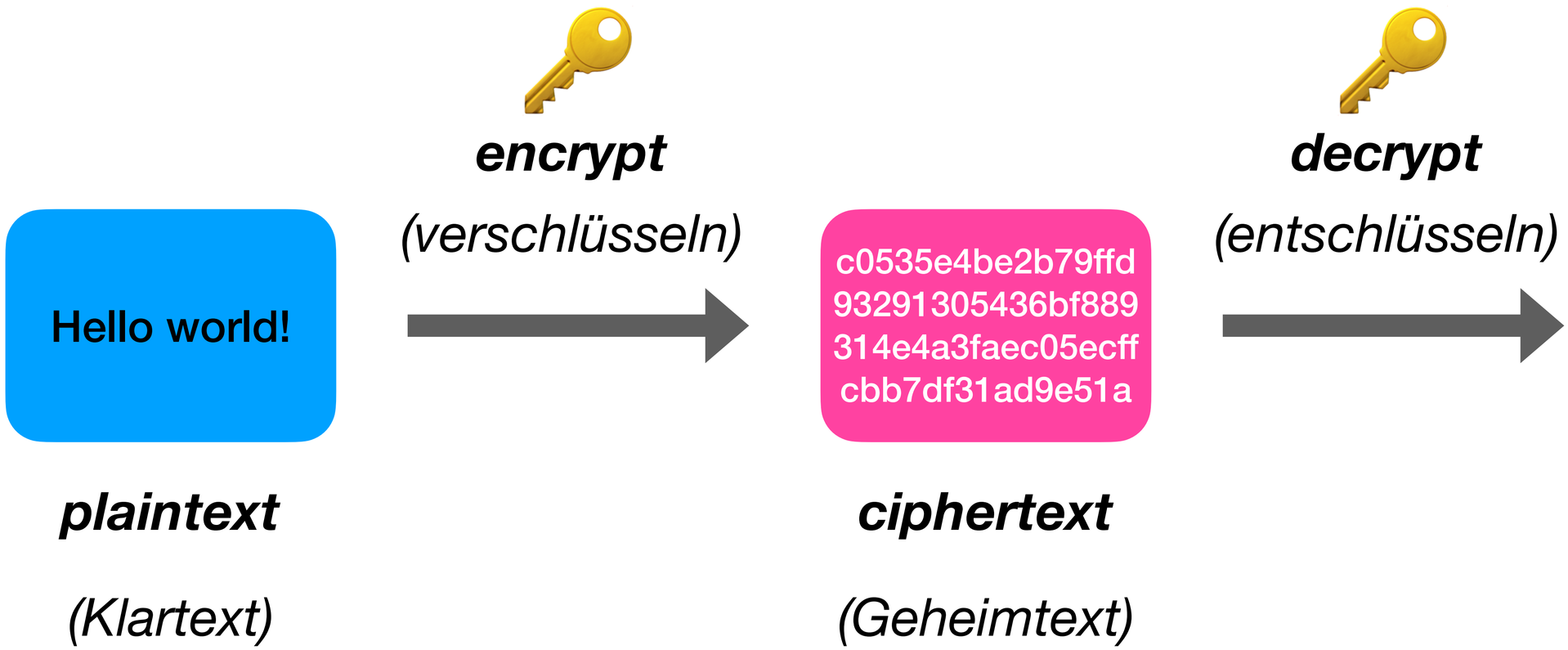
Attempt 2: encrypting

What is **encryption**? *(Verschlüsselung)*



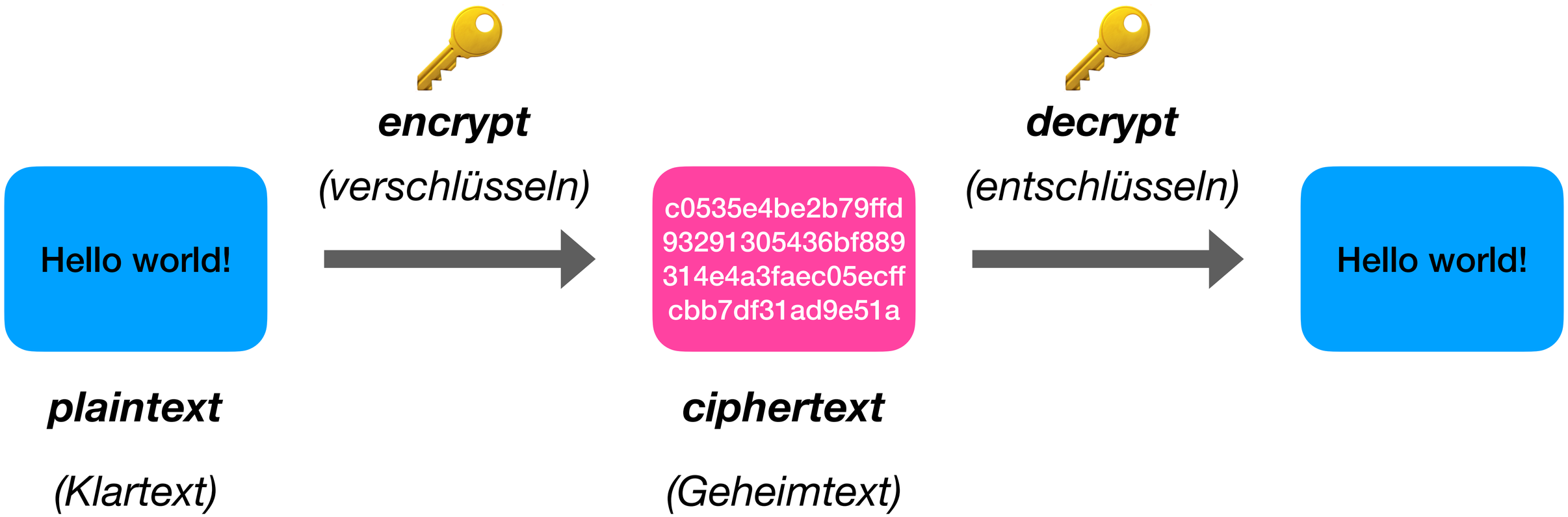
Attempt 2: encrypting

What is **encryption**? *(Verschlüsselung)*



Attempt 2: encrypting

What is **encryption**? *(Verschlüsselung)*



Attempt 2: encrypting

Idea: let's **encrypt** all of the passwords with a super secret key!

username	password
user1	adfjsksshfds
user2	vcncxmnskfh
user3	qwpeeruwrew
bob	iambob
user5	cbxmpsfqpew
user6	irewioosfdks
user7	owriuakdfbvx
user8	fldsasdjdhfj

Attempt 2: encrypting

Idea: let's **encrypt** all of the passwords with a super secret key!

username	password
user1	adfjsksshfds
user2	vcncxmnskfh
user3	qwpeeruwrew
bob	iambob
user5	cbxmpsfqpew
user6	irewioosfdks
user7	owriuakdfbvx
user8	fldsasdjdhfj

Attempt 2: encrypting

Idea: let's **encrypt** all of the passwords with a super secret key!

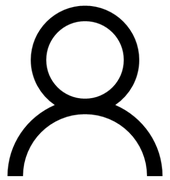
username	encrypted password
user1	9RKqnxPz
user2	IFIy6wk
user3	EycgaHJ0
bob	ImgT6gJz
user5	zFaS9qdg
user6	kSY78tW
user7	5t4Mrc8b
user8	262uaI2w

Attempt 2: encrypting

Idea: let's **encrypt** all of the passwords with a super secret key!

username	encrypted password
user1	9RKqnxPz
user2	IFIy6wk
user3	EycgaHJ0
bob	ImgT6gJz
user5	zFaS9qdg
user6	kSY78tW
user7	5t4Mrc8b
user8	262uaI2w

can i log into teams please?



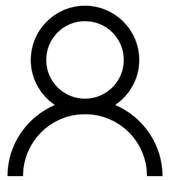
`username: bob`

`password: iambob`

Attempt 2: encrypting

Idea: let's **encrypt** all of the passwords with a super secret key!

username	encrypted password
user1	9RKqnxPz
user2	IFIy6wk
user3	EycgaHJ0
bob	ImgT6gJz
user5	zFaS9qdg
user6	kSY78tW
user7	5t4Mrc8b
user8	262uaI2w



can i log into teams please?

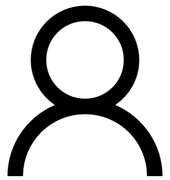
`username: bob`

`password: iambob`

Attempt 2: encrypting

Idea: let's **encrypt** all of the passwords with a super secret key!

username	encrypted password
user1	9RKqnxPz
user2	IFIy6wk
user3	EycgaHJ0
bob	ImgT6gJz
user5	zFaS9qdg
user6	kSY78tW
user7	5t4Mrc8b
user8	262uaI2w



can i log into teams please?

`username: bob`

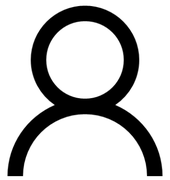
`password: iambob`

check if **decrypt(🔑, ImgT6gJz)** == `iambob`

Attempt 2: encrypting

Idea: let's **encrypt** all of the passwords with a super secret key!

username	encrypted password
user1	9RKqnxPz
user2	IFIy6wk
user3	EycgaHJ0
bob	ImgT6gJz
user5	zFaS9qdg
user6	kSY78tW
user7	5t4Mrc8b
user8	262uaI2w



can i log into teams please?

`username: bob`

`password: iambob`

✅

check if **decrypt(🔑, ImgT6gJz)** == `iambob`

Attempt 2: encrypting

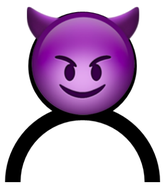
Idea: let's **encrypt** all of the passwords with a super secret key!

username	encrypted password
user1	9RKqnxPz
user2	IFIy6wk
user3	EycgaHJ0
bob	ImgT6gJz
user5	zFaS9qdg
user6	kSY78tW
user7	5t4Mrc8b
user8	262uaI2w

Attempt 2: encrypting

Idea: let's **encrypt** all of the passwords with a super secret key!

username	encrypted password
user1	9RKqnxPz
user2	IFIy6wk
user3	EycgaHJ0
bob	ImgT6gJz
user5	zFaS9qdg
user6	kSY78tW
user7	5t4Mrc8b
user8	262uaI2w

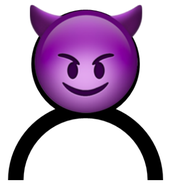


i have bob's encrypted password! it's ***ImgT6gJz***

Attempt 2: encrypting

Idea: let's **encrypt** all of the passwords with a super secret key!

username	encrypted password
user1	9RKqnxPz
user2	IFIy6wk
user3	EycgaHJ0
bob	ImgT6gJz
user5	zFaS9qdg
user6	kSY78tW
user7	5t4Mrc8b
user8	262uaI2w



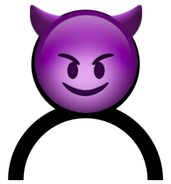
i have bob's encrypted password! it's ***ImgT6gJz***

Can the attacker get Bob's password?

Attempt 2: encrypting

Idea: let's **encrypt** all of the passwords with a super secret key!

username	encrypted password
user1	9RKqnxPz
user2	IFIy6wk
user3	EycgaHJ0
bob	ImgT6gJz
user5	zFaS9qdg
user6	kSY78tW
user7	5t4Mrc8b
user8	262uaI2w



i have bob's encrypted password! it's ***ImgT6gJz***

Can the attacker get Bob's password?

Attempt 3: hashing

Attempt 3: hashing

A **hash function** *(Hash-Funktion)* is a function with a few **special properties:**

Attempt 3: hashing

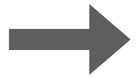
A **hash function** *(Hash-Funktion)* is a function with a few **special properties:**

`mygreatpassword`

input: text of any length

Attempt 3: hashing

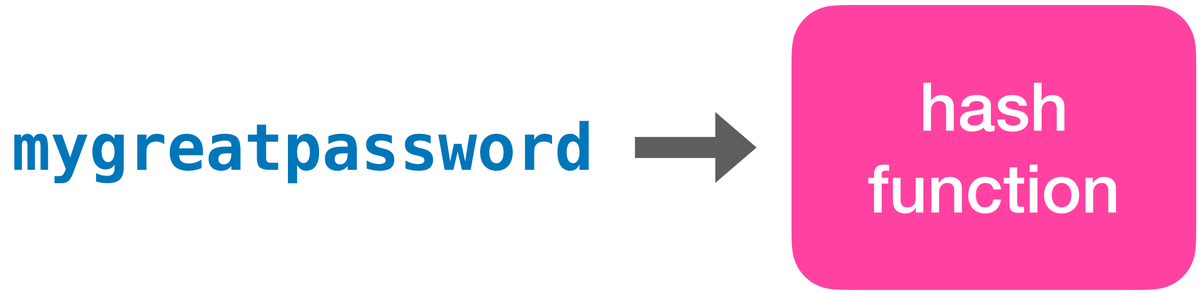
A **hash function** *(Hash-Funktion)* is a function with a few **special properties:**

`mygreatpassword` 

input: text of any length

Attempt 3: hashing

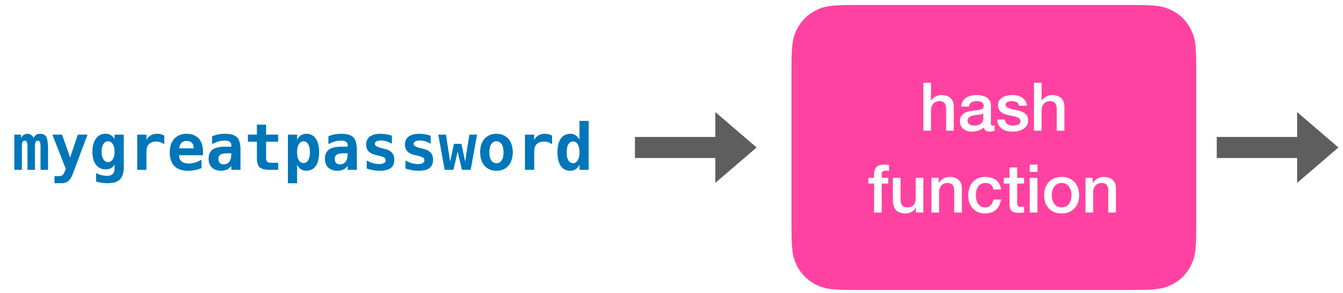
A **hash function** *(Hash-Funktion)* is a function with a few **special properties:**



input: text of any length

Attempt 3: hashing

A **hash function** *(Hash-Funktion)* is a function with a few **special properties:**



input: text of any length

Attempt 3: hashing

A **hash function** *(Hash-Funktion)* is a function with a few **special properties:**

input: text of any length

output: fixed-length string

(the “hash”)

Attempt 3: hashing

A **hash function** *(Hash-Funktion)* is a function with a few **special properties:**

input: text of any length

output: fixed-length string

(the “hash”)

Hash functions are **one-way —** it is virtually impossible to get the original back

Attempt 3: hashing

A **hash function** *(Hash-Funktion)* is a function with a few **special properties:**

input: text of any length

output: fixed-length string

(the “hash”)

Hash functions are **one-way —** it is virtually impossible to get the original back

Hash functions are **collision-resistant —** two different things should not have the same hash

Attempt 3: hashing

Idea: we don’t need to see the password, we just need proof that Bob knows it

username	password
user1	adfjsksshfds
user2	vcncxmnskfh
bob	iambob
user3	qwpeeruwrew

Attempt 3: hashing

Idea: we don’t need to see the password, we just need proof that Bob knows it

username	password
user1	adfjsksshfds
user2	vcncxmnskfh
bob	iambob
user3	qwpeeruwrew

*Apply a **hash function** to the stored passwords (z.B. SHA256, MD5)*

Attempt 3: hashing

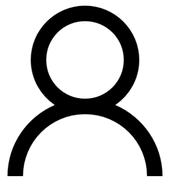
Idea: we don’t need to see the password, we just need proof that Bob knows it

username	hashed password
user1	52d47bc53a257971797b43164be2378193cb1f85c4f2036c56c8b44fb69abd75
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user3	5860faf02b6bc6222ba5aca523560f0e364ccd8b67bee486fe8bf7c01d492ccb

Attempt 3: hashing

Idea: we don’t need to see the password, we just need proof that Bob knows it

username	hashed password
user1	52d47bc53a257971797b43164be2378193cb1f85c4f2036c56c8b44fb69abd75
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user3	5860faf02b6bc6222ba5aca523560f0e364ccd8b67bee486fe8bf7c01d492ccb



can i log into teams please?

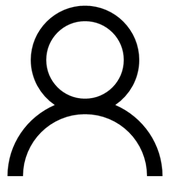
username: bob

password: iambob

Attempt 3: hashing

Idea: we don’t need to see the password, we just need proof that Bob knows it

username	hashed password
user1	52d47bc53a257971797b43164be2378193cb1f85c4f2036c56c8b44fb69abd75
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user3	5860faf02b6bc6222ba5aca523560f0e364ccd8b67bee486fe8bf7c01d492ccb



can i log into teams please?

`username: bob`

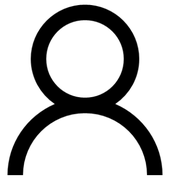
`password: iambob`

check if **hash(**`iambob`**)** == `8299a9...24c9`

Attempt 3: hashing

Idea: we don’t need to see the password, we just need proof that Bob knows it

username	hashed password
user1	52d47bc53a257971797b43164be2378193cb1f85c4f2036c56c8b44fb69abd75
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user3	5860faf02b6bc6222ba5aca523560f0e364ccd8b67bee486fe8bf7c01d492ccb



can i log into teams please?

`username: bob`

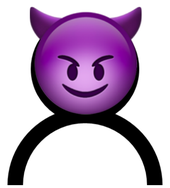
`password: iambob`

check if **hash(**`iambob`**)** == `8299a9...24c9`

Attempt 3: hashing

Idea: we don’t need to see the password, we just need proof that Bob knows it

username	hashed password
user1	52d47bc53a257971797b43164be2378193cb1f85c4f2036c56c8b44fb69abd75
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user3	5860faf02b6bc6222ba5aca523560f0e364ccd8b67bee486fe8bf7c01d492ccb



can i log into teams please?

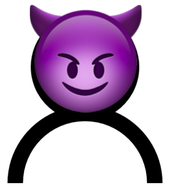
username: bob

password: NotBob

Attempt 3: hashing

Idea: we don’t need to see the password, we just need proof that Bob knows it

username	hashed password
user1	52d47bc53a257971797b43164be2378193cb1f85c4f2036c56c8b44fb69abd75
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user3	5860faf02b6bc6222ba5aca523560f0e364ccd8b67bee486fe8bf7c01d492ccb



can i log into teams please?

username: bob

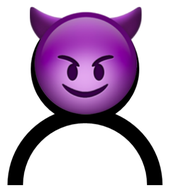
password: NotBob

check if **hash(NotBob)** == 8299a9...24c9

Attempt 3: hashing

Idea: we don’t need to see the password, we just need proof that Bob knows it

username	hashed password
user1	52d47bc53a257971797b43164be2378193cb1f85c4f2036c56c8b44fb69abd75
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user3	5860faf02b6bc6222ba5aca523560f0e364ccd8b67bee486fe8bf7c01d492ccb



can i log into teams please?

username: bob

password: NotBob

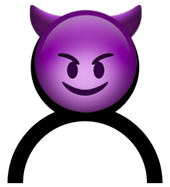
check if **hash(NotBob)** == 8299a9...24c9

hash(NotBob) ➡️ 3008aa...689d

Attempt 3: hashing

Idea: we don’t need to see the password, we just need proof that Bob knows it

username	hashed password
user1	52d47bc53a257971797b43164be2378193cb1f85c4f2036c56c8b44fb69abd75
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user3	5860faf02b6bc6222ba5aca523560f0e364ccd8b67bee486fe8bf7c01d492ccb



can i log into teams please?

`username: bob`

`password: NotBob`

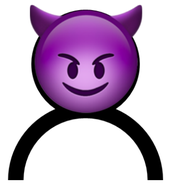
check if **hash(NotBob)** == `8299a9...24c9`

hash(NotBob) ➡️ `3008aa...689d`

Attempt 3: hashing

Idea: we don’t need to see the password, we just need proof that Bob knows it

username	hashed password
user1	52d47bc53a257971797b43164be2378193cb1f85c4f2036c56c8b44fb69abd75
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user3	5860faf02b6bc6222ba5aca523560f0e364ccd8b67bee486fe8bf7c01d492ccb



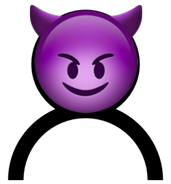
*i have bob’s hashed password! it’s **8299a…4c9***

Can the attacker get Bob’s password?

Attempt 3: hashing

Idea: we don't need to see the password, we just need proof that Bob knows it

username	hashed password
user1	52d47bc53a257971797b43164be2378193cb1f85c4f2036c56c8b44fb69abd75
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user3	5860faf02b6bc6222ba5aca523560f0e364ccd8b67bee486fe8bf7c01d492ccb



*i have bob's hashed password! it's **8299a…4c9***

Can the attacker get Bob's password?

*No! Because hashes are **one way***

Attempt 3: hashing (problems)

username	hashed password
user1	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user3	5860faf02b6bc6222ba5aca523560f0e364ccd8b67bee486fe8bf7c01d492ccb

Attempt 3: hashing (problems)

username	hashed password
user1	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user3	5860faf02b6bc6222ba5aca523560f0e364ccd8b67bee486fe8bf7c01d492ccb

What if user1's password is also "`iambob`"?

Attempt 3: hashing (problems)

username	hashed password
user1	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	8299a97e9883d91c7be01c536d4fc7bd8fa02d308f027da7d3f084e0565424c9
user3	5860faf02b6bc6222ba5aca523560f0e364ccd8b67bee486fe8bf7c01d492ccb

What if user1's password is also "`iambob`"?

Attempt 3: hashing (problems)

Attempt 3: hashing (problems)

Most passwords are **bad**, and hash functions can be computed **quickly**.

Attempt 3: hashing (problems)

Most passwords are **bad**, and hash functions can be computed **quickly**.

password	hashed password
123456	
password	
123456789	
12345	
12345678	
qwerty	
iloveyou	

Attempt 3: hashing (problems)

Most passwords are **bad**, and hash functions can be computed **quickly**.

password	hashed password
123456	ba3253876aed6bc22d4a6ff53d8406c6ad864195ed144ab5c87621b6c233b548baeae6956df346ec8c17f5e
password	bc547750b92797f955b36112cc9bdd5cddf7d0862151d03a167ada8995aa24a9ad24610b36a68bc02da2414
123456789	d9e6762dd1c8eaf6d61b3c6192fc408d4d6d5f1176d0c29169bc24e71c3f274ad27fcd5811b313d681f7e55
12345	3627909a29c31381a071ec27f7c9ca97726182aed29a7ddd2e54353322cfb30abb9e3a6df2ac2c20fe23436
12345678	fa585d89c851dd338a70dcf535aa2a92fee7836dd6aff1226583e88e0996293f16bc009c652826e0fc5c706
qwerty	0dd3e512642c97ca3f747f9a76e374fbda73f9292823c0313be9d78add7cdd8f72235af0c553dd26797e78e
iloveyou	50e0dc4455bcb1ee80adb942d153c6b0eb17b31d603b017fa77f60f60f68fd7d0565cb486783f29cea21031

Attempt 3: hashing (problems)

Most passwords are **bad**, and hash functions can be computed **quickly**.

password	hashed password
123456	ba3253876aed6bc22d4a6ff53d8406c6ad864195ed144ab5c87621b6c233b548baeae6956df346ec8c17f5e
password	bc547750b92797f955b36112cc9bdd5cddf7d0862151d03a167ada8995aa24a9ad24610b36a68bc02da2414
123456789	d9e6762dd1c8eaf6d61b3c6192fc408d4d6d5f1176d0c29169bc24e71c3f274ad27fcd5811b313d681f7e55
12345	3627909a29c31381a071ec27f7c9ca97726182aed29a7ddd2e54353322cfb30abb9e3a6df2ac2c20fe23436
12345678	fa585d89c851dd338a70dcf535aa2a92fee7836dd6aff1226583e88e0996293f16bc009c652826e0fc5c706
qwerty	0dd3e512642c97ca3f747f9a76e374fbda73f9292823c0313be9d78add7cdd8f72235af0c553dd26797e78e
iloveyou	50e0dc4455bcb1ee80adb942d153c6b0eb17b31d603b017fa77f60f60f68fd7d0565cb486783f29cea21031

username	hashed password
user1	ba3253876aed6bc22d4a6ff53d8406c6ad864195ed144ab5c87621b6c233b548baeae6956df346ec8c17f5ea
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	3627909a29c31381a071ec27f7c9ca97726182aed29a7ddd2e54353322cfb30abb9e3a6df2ac2c20fe234363
user3	0dd3e512642c97ca3f747f9a76e374fbda73f9292823c0313be9d78add7cdd8f72235af0c553dd26797e78e1

Attempt 3: hashing (problems)

Most passwords are **bad**, and hash functions can be computed **quickly**.

password	hashed password
123456	ba3253876aed6bc22d4a6ff53d8406c6ad864195ed144ab5c87621b6c233b548baeae6956df346ec8c17f5e
password	bc547750b92797f955b36112cc9bdd5cddf7d0862151d03a167ada8995aa24a9ad24610b36a68bc02da2414
123456789	d9e6762dd1c8eaf6d61b3c6192fc408d4d6d5f1176d0c29169bc24e71c3f274ad27fcd5811b313d681f7e55
12345	3627909a29c31381a071ec27f7c9ca97726182aed29a7ddd2e54353322cfb30abb9e3a6df2ac2c20fe23436
12345678	fa585d89c851dd338a70dcf535aa2a92fee7836dd6aff1226583e88e0996293f16bc009c652826e0fc5c706
qwerty	0dd3e512642c97ca3f747f9a76e374fbda73f9292823c0313be9d78add7cdd8f72235af0c553dd26797e78e
iloveyou	50e0dc4455bcb1ee80adb942d153c6b0eb17b31d603b017fa77f60f60f68fd7d0565cb486783f29cea21031

username	hashed password
user1	ba3253876aed6bc22d4a6ff53d8406c6ad864195ed144ab5c87621b6c233b548baeae6956df346ec8c17f5ea
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	3627909a29c31381a071ec27f7c9ca97726182aed29a7ddd2e54353322cfb30abb9e3a6df2ac2c20fe234363
user3	0dd3e512642c97ca3f747f9a76e374fbda73f9292823c0313be9d78add7cdd8f72235af0c553dd26797e78e1

Attempt 3: hashing (problems)

Most passwords are **bad**, and hash functions can be computed **quickly**.

password	hashed password
123456	ba3253876aed6bc22d4a6ff53d8406c6ad864195ed144ab5c87621b6c233b548baeae6956df346ec8c17f5e
password	bc547750b92797f955b36112cc9bdd5cddf7d0862151d03a167ada8995aa24a9ad24610b36a68bc02da2414
123456789	d9e6762dd1c8eaf6d61b3c6192fc408d4d6d5f1176d0c29169bc24e71c3f274ad27fcd5811b313d681f7e55
12345	3627909a29c31381a071ec27f7c9ca97726182aed29a7ddd2e54353322cfb30abb9e3a6df2ac2c20fe23436
12345678	fa585d89c851dd338a70dcf535aa2a92fee7836dd6aff1226583e88e0996293f16bc009c652826e0fc5c706
qwerty	0dd3e512642c97ca3f747f9a76e374fbda73f9292823c0313be9d78add7cdd8f72235af0c553dd26797e78e
iloveyou	50e0dc4455bcb1ee80adb942d153c6b0eb17b31d603b017fa77f60f60f68fd7d0565cb486783f29cea21031

username	hashed password
user1	ba3253876aed6bc22d4a6ff53d8406c6ad864195ed144ab5c87621b6c233b548baeae6956df346ec8c17f5ea
user2	vcncxmnsf88e939e9b2c837eb6b3b67ae1b932ab4a03a3548a2d2ab867cb6aa4a28cf94ekfh
bob	3627909a29c31381a071ec27f7c9ca97726182aed29a7ddd2e54353322cfb30abb9e3a6df2ac2c20fe234363
user3	0dd3e512642c97ca3f747f9a76e374fbda73f9292823c0313be9d78add7cdd8f72235af0c553dd26797e78e1

Rainbow table attack

Attempts 4 and 5: salting and slow hashes

Salting: add a random value to your password before hashing it

Attempts 4 and 5: salting and slow hashes

Salting: add a random value to your password before hashing it

`iambob`

`iambob`

`password`

Attempts 4 and 5: salting and slow hashes

Salting: add a random value to your password before hashing it

`iambob` + `vsg2rkr39`

`iambob` + `xz8dhas7h`

`password` + ***`salt`***

Attempts 4 and 5: salting and slow hashes

Salting: add a random value to your password before hashing it

`iambob` + `vsg2rkr39` →

`iambob` + `xz8dhas7h` →

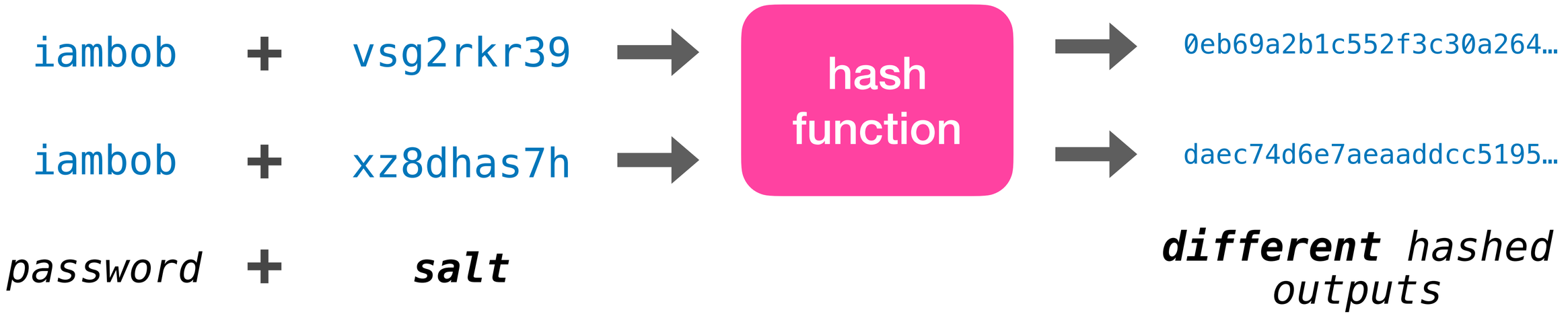
`password` + ***`salt`***

Attempts 4 and 5: salting and slow hashes

Salting: add a random value to your password before hashing it

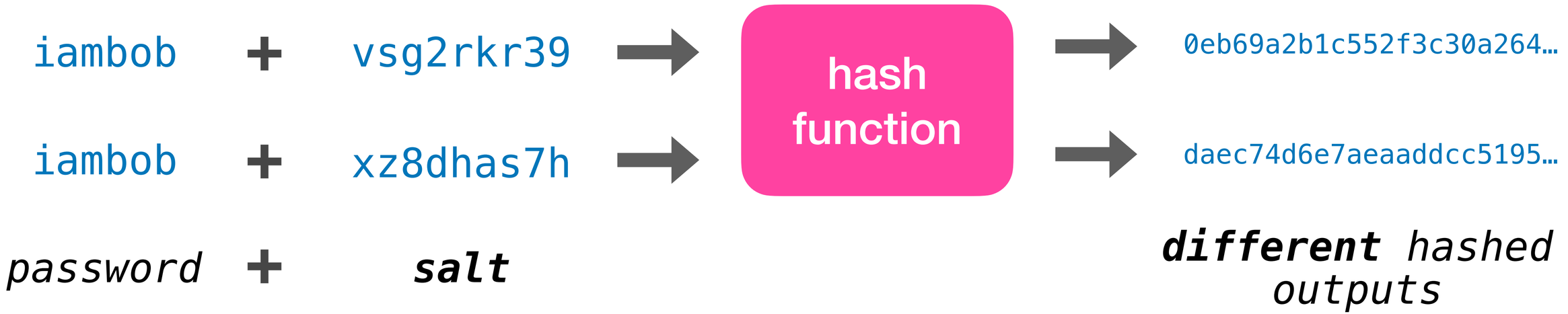
Attempts 4 and 5: salting and slow hashes

Salting: add a random value to your password before hashing it



Attempts 4 and 5: salting and slow hashes

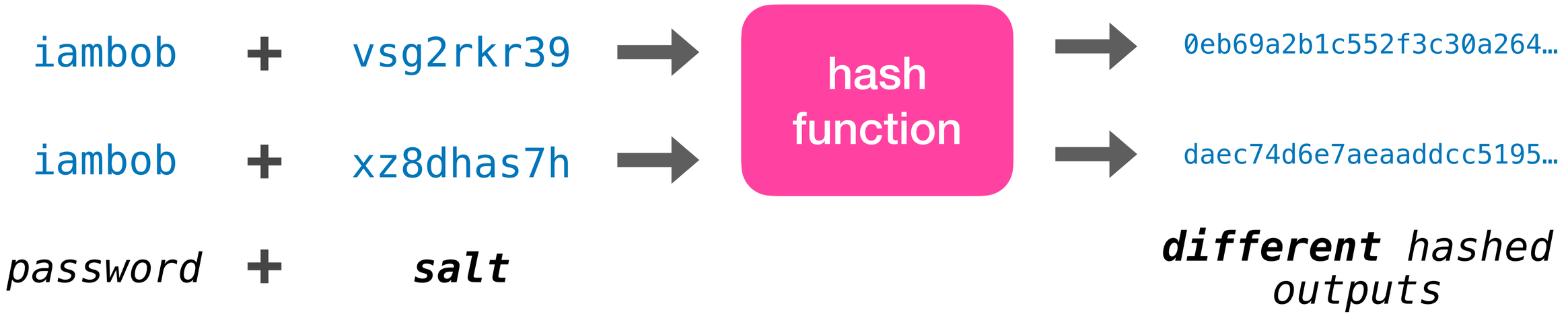
Salting: add a random value to your password before hashing it



Slow hashing: purposefully slow hash function *(z.B. bcrypt)*

Attempts 4 and 5: salting and slow hashes

Salting: add a random value to your password before hashing it



Slow hashing: purposefully slow hash function *(z.B. bcrypt)*

✅ ✅ ✅

Summary

Attempt 1: plaintext passwords

Attempt 2: encrypted passwords

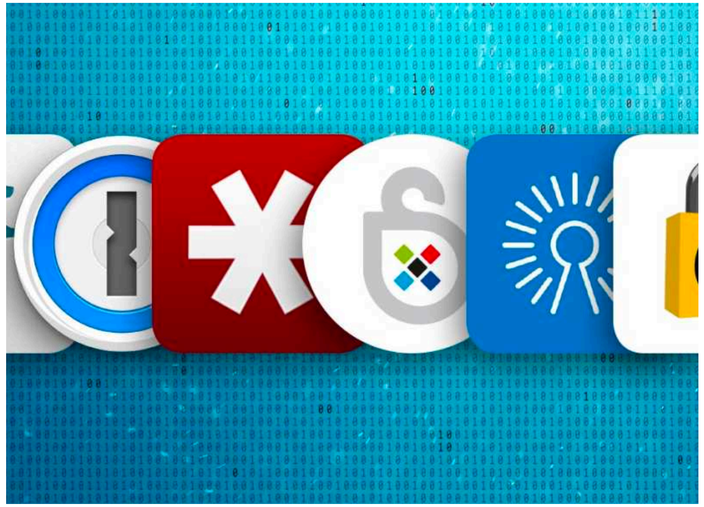
Attempt 3: hashed passwords

Attempt 4: hashed and salted passwords

Attempt 5: hashed and salted passwords, using a *slow hash*

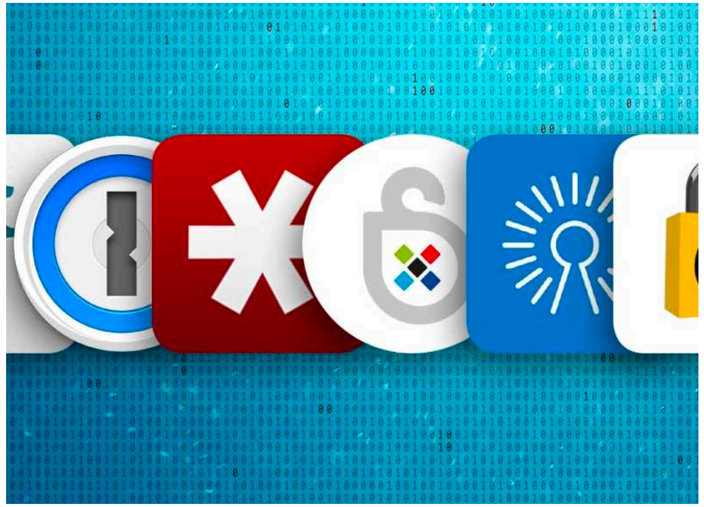
Password advice for *you*

Password advice for *you*

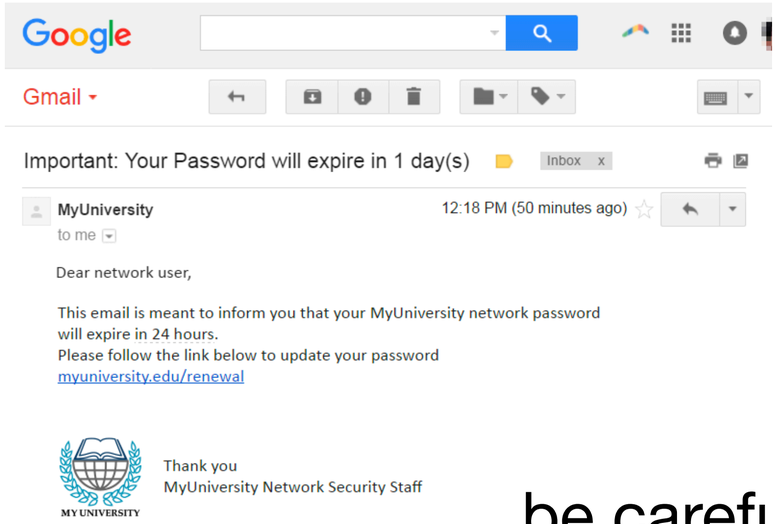


password managers

Password advice for *you*

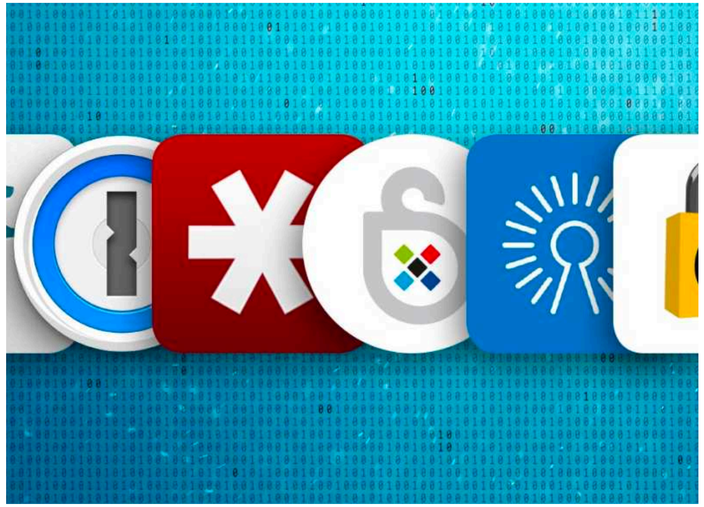


password managers

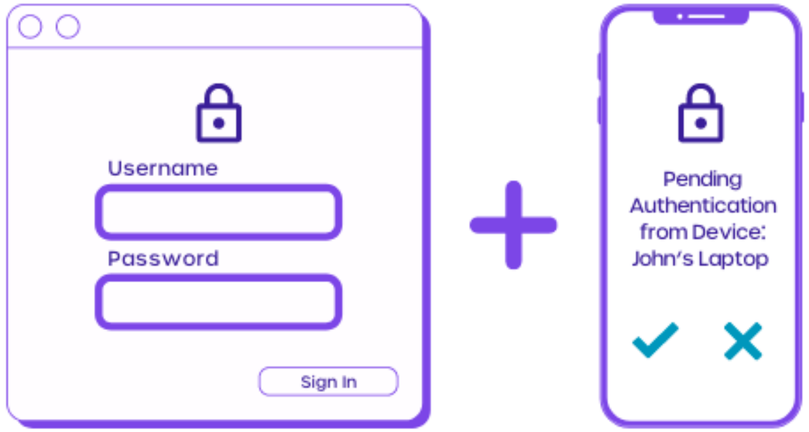


be careful of **phishing**

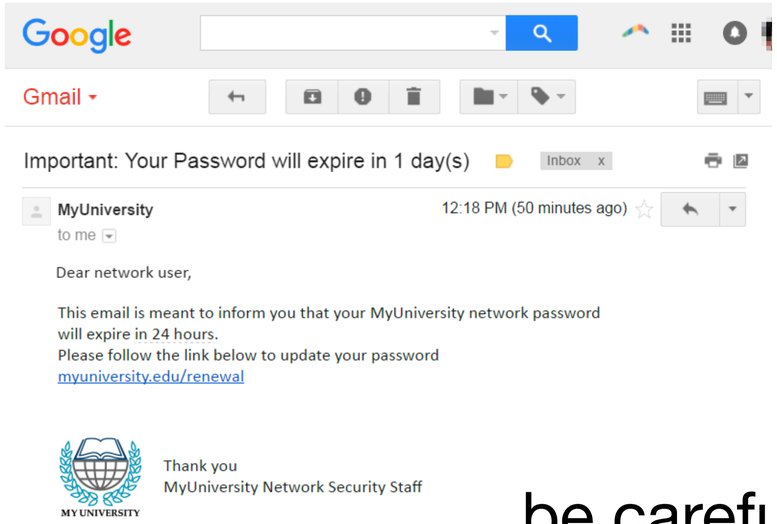
Password advice for *you*



password managers

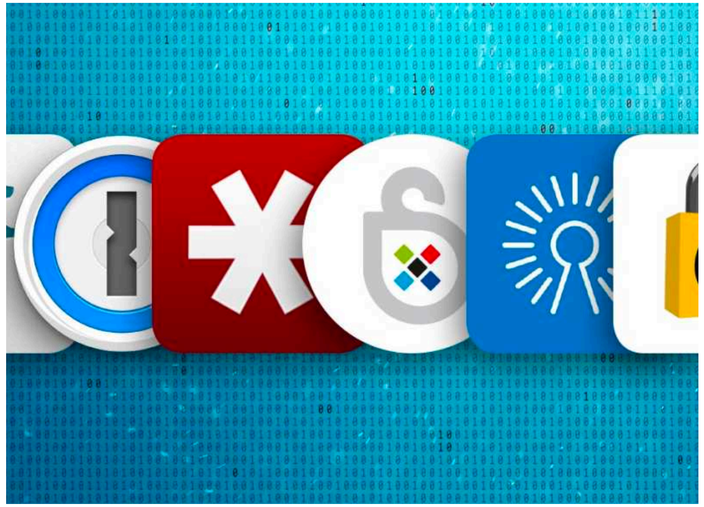


two factor authentication

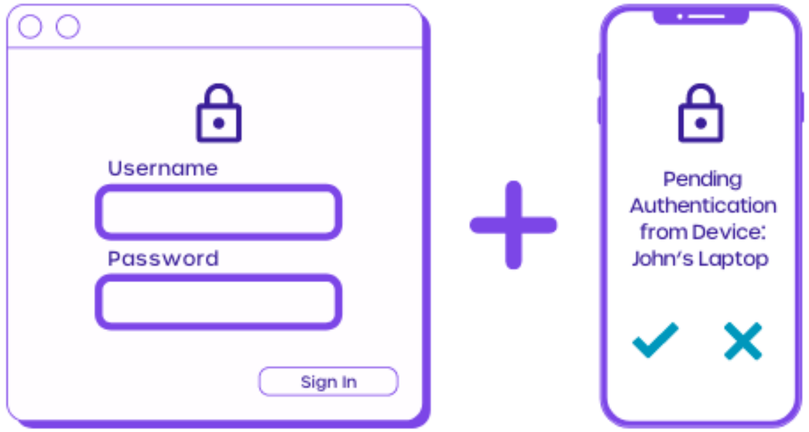


be careful of **phishing**

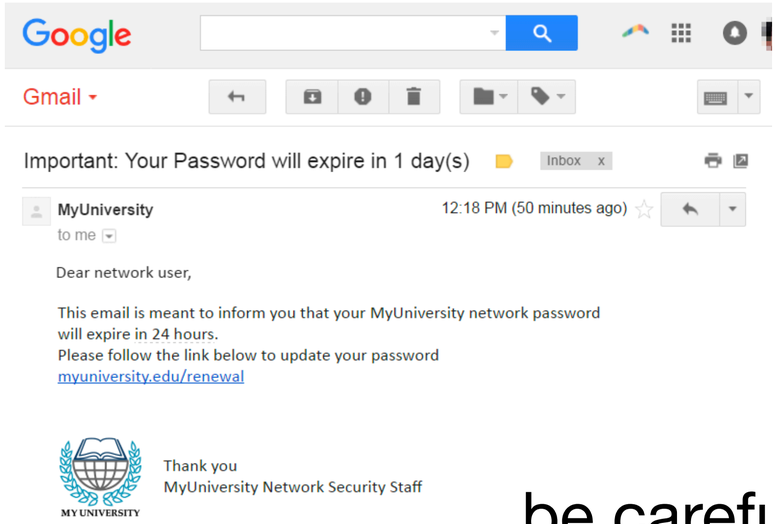
Password advice for *you*



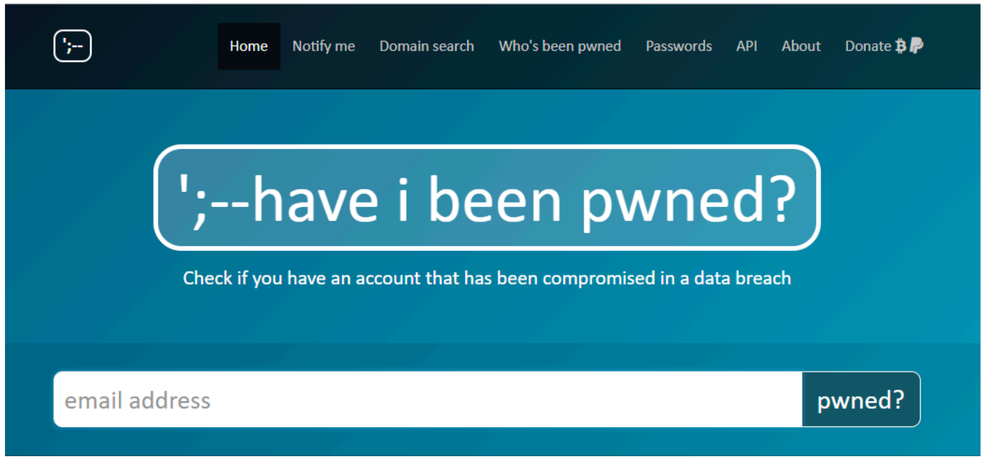
password managers



two factor authentication



be careful of **phishing**



have i been pwned?

Now, for the fun part.

A password cracking activity!

http://tinyurl.com/passwordWG

Thank you!