

# Bezpieczne Hasła i Uwierzytelnianie

Warsztaty

Prowadzący: prof. dr hab. Maciej Rybczyński

# Dlaczego hasła są ważne?

1. Hasła zabezpieczają nasze konta przed nieautoryzowanym dostępem.
2. Słabe hasła mogą być łatwo złamane przez hakerów.
3. Wiele osób używa tych samych haseł w różnych serwisach.
4. Silne hasło znacząco utrudnia ataki brute-force i inne metody łamania zabezpieczeń.

# Jakie ataki są stosowane przeciwko hasłom?

**Atak brute-force** – systematyczne sprawdzanie wszystkich możliwych kombinacji.

**Atak słownikowy** – używanie listy najczęściej stosowanych haseł.

**Phishing** – kradzież haseł poprzez fałszywe strony i e-maile.

**Ataki na wycieki danych** – wykorzystanie haseł ujawnionych w naruszeniach bezpieczeństwa.

# Jak stworzyć silne hasło?

1. Minimum 12-16 znaków.
2. Używaj kombinacji wielkich i małych liter, cyfr oraz znaków specjalnych.
3. Unikaj łatwych do odgadnięcia fraz (np. '123456', 'qwerty').
4. Każde konto powinno mieć unikalne hasło.

# TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

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	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

<https://www.hivesystems.io/password>



## Using ChatGPT hardware to brute force your password in 2023

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	instantly	instantly	instantly
8	instantly	instantly	instantly	instantly	1 sec
9	instantly	instantly	4 secs	21 secs	1 min
10	instantly	instantly	4 mins	22 mins	1 hour
11	instantly	6 secs	3 hours	22 hours	4 days
12	instantly	2 mins	7 days	2 months	8 months
13	instantly	1 hour	12 months	10 years	47 years
14	instantly	1 day	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

Source: hivesystems.io



<https://www.hivesystems.io/password>



Security Awareness Episode 1: Passwords

<https://www.youtube.com/watch?v=0Wd3JoUHXno&list=PL7QHbjPSF0r6qJonaROIxVaMLzwDnZyOL>

# Menedżery haseł – czy warto ich używać?

1. Przechowują i generują silne hasła.
2. Eliminują potrzebę zapamiętywania wielu skomplikowanych haseł.
3. Zmniejszają ryzyko ponownego użycia tego samego hasła.
4. Przykłady menedżerów haseł: Bitwarden, KeePass, 1Password, LastPass.



# Uwierzytelnianie dwuskładnikowe (2FA) – jak to działa?

**Co to jest 2FA?** – dodatkowa warstwa zabezpieczeń konta.

## **Rodzaje 2FA:**

- Kody SMS (mniej bezpieczne).
- Aplikacje uwierzytelniające (np. Google Authenticator, Authy).
- Klucze sprzętowe (np. YubiKey).

# Interaktywne zadanie: Tworzenie silnych haseł

Wygeneruj bezpieczne hasło za pomocą menedżera haseł

Przetestuj jego siłę na stronie

<https://howsecureismypassword.net>

Porównaj swoje obecne hasła i sprawdź, czy są wystarczająco silne

# Podsumowanie i pytania

Twórz silne, unikalne hasła dla każdego konta.

Korzystaj z menedżera haseł, aby ułatwić sobie zarządzanie danymi.

Włącz uwierzytelnianie dwuskładnikowe tam, gdzie to możliwe.  
Jakie masz pytania?