

Program “Klikaj z głową - edukacja cyfrowa ZS3”



BEZPIECZNE HASŁA OCHRONA TWOICH KONT

**Komisja Przedmiotów Informatycznych
S. P-N.**

ILE KONT MASZ ONLINE?

- E-dziennik
- Instagram, TikTok, Snapchat
- Discord, Messenger
- Gry online (Steam, Epic Games, PlayStation Network)
- E-mail
- Netflix, Spotify, YouTube
- Sklepy online
- I wiele, wiele innych...

Średnio jedna osoba ma ponad 100 kont online!

PROBLEM

KAŻDY MOŻE ZOSTAĆ ZHAKOWANY

To nie jest kwestia "czy", ale "kiedy".

Cyberprzestępcy atakują WSZYSTKICH:

- Nie musisz być sławny
- Nie musisz mieć dużo pieniędzy
- Nie musisz być "ważny"

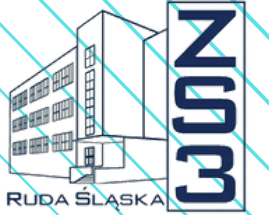
Hakerzy atakują masowo – ich programy sprawdzają miliony kont dziennie.

STATYSTYKI

Zagrożenie w liczbach:

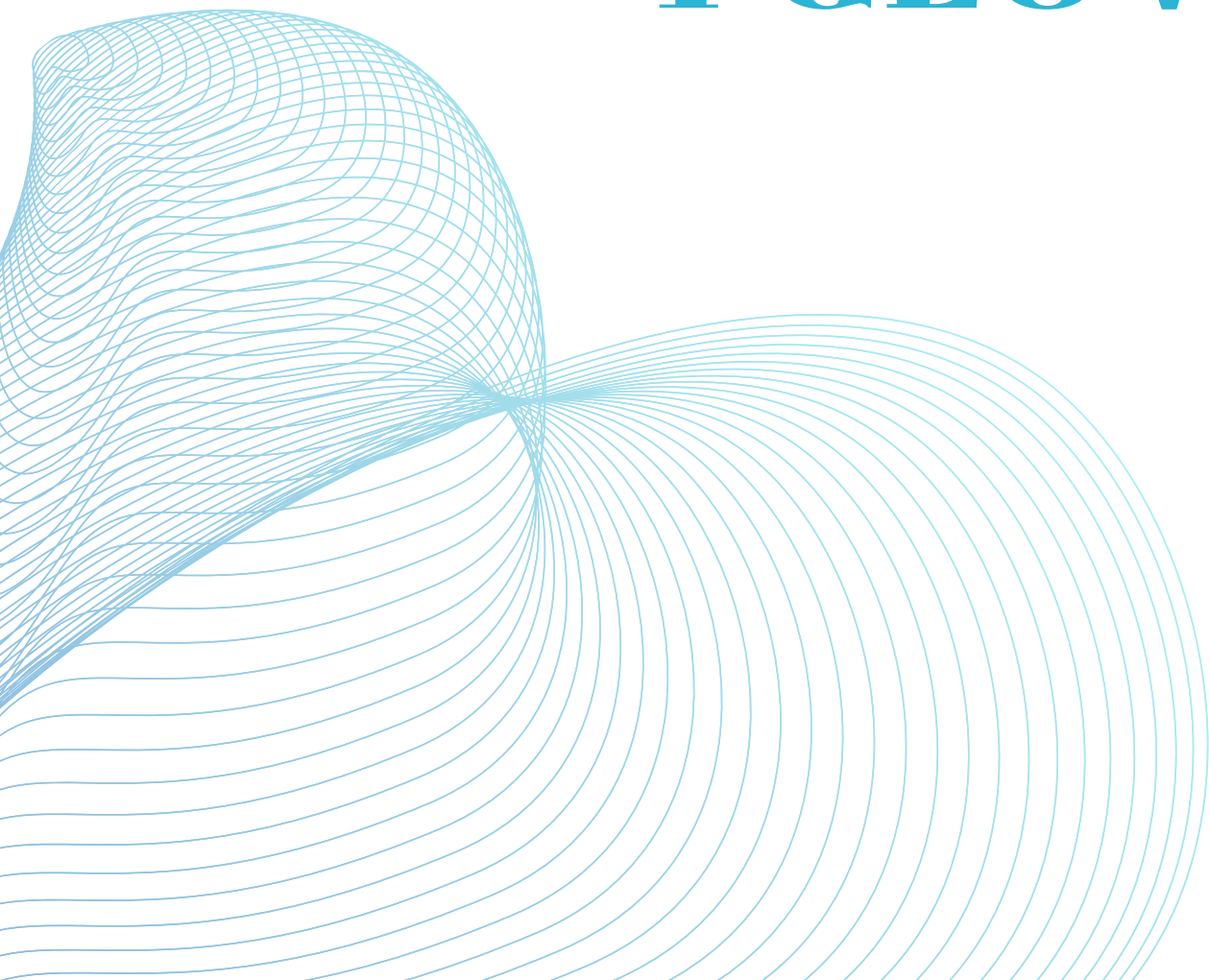
- 72% Polaków pada ofiarą prób wyłudzenia danych rocznie
- 83% włamań wynika z użycia słabych lub skradzionych haseł
- Słabe hasło zostaje złamane w mniej niż 1 sekundę
- 5 na 10 młodych ludzi doświadczyło cyberprzemocy lub nękania online

Program “Klikaj z głową - edukacja cyfrowa ZS3”



JAK HAKERZY ŁAMIĄ HASŁA?

4 GŁÓWNE METODY ATAKÓW



METODA 1

Zaawansowane programy testują:

- Popularne hasła ("haslo123", "qwerty", "password")
- Słowa ze słownika
- Typowe kombinacje (imię+rok urodzenia)

Szybkość: nawet 1000 kombinacji na sekundę

Najpopularniejsze hasła 2025:

1. 123456
2. password
3. qwerty123
4. admin
5. haslo123 T

Te hasła zostają złamane NATYCHMIAST

METODA 2

WYCIEKI BAZ DANYCH

Co się dzieje?

1. Serwis internetowy zostaje zhakowany (stara gra, forum, sklep)
2. Przestępcy wykradają miliony haseł
3. Jeśli używasz tego samego hasła wszędzie...
4. ...mają dostęp do WSZYSTKICH Twoich kont

PRZYKŁAD: Hasło z gry sprzed 5 lat = hasło do Instagrama = hasło do e-maila → DRAMAT

METODA 3

PHISHING – WYŁUDZANIE DANYCH

Fałszywe wiadomości i strony internetowe:

- "🎁 Gratulacje! Wygrałeś iPhone 15! Kliknij tutaj i zaloguj się!"
- "⚠️ Twoje konto zostanie zablokowane! Zaloguj się natychmiast!"
- "🎮 Darmowe V-Bucksy! Podaj login i hasło!"

Strona wygląda jak prawdziwa, ale... → wpisujesz hasło → przestępcy je mają

METODA 4

SOCJOTECHNIKA I ODGADYWANIE

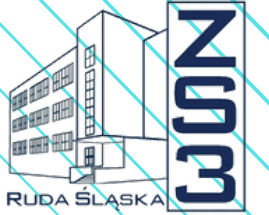
Używają publicznie dostępnych informacji o Tobie:

- Imię i nazwisko (z Instagrama)
- Data urodzenia (z Facebooka)
- Nazwa szkoły
- Ulubiona drużyna
- Imię psa/kota

Typowe hasło: Anna2008 lub Reksio123

Te hasła można odgadnąć w kilka prób!

Program “Klikaj z głową - edukacja cyfrowa ZS3”



CO MOGĄ ZROBIĆ Z TWOIM KONTEM?

KONSEKWENCJE WŁAMANIA



KONSEKWENCJE

REALNE ZAGROŻENIA:

- 🔓 Kradzież prywatnych zdjęć i wiadomości
- 👤 Podszywanie się pod Ciebie – oszukiwanie znajomych i rodziny
- 🎮 Utrata postępów w grach (setki godzin pracy!)
- 💳 Nieautoryzowane zakupy (jeśli masz podpiętą kartę)
- 🚫 Zmiana hasła – całkowita blokada WŁASNEGO konta
- 😱 Publikowanie kompromitujących treści w Twoim imieniu
- ⚠️ Szantaż i wymuszenia

PRZYKŁADY

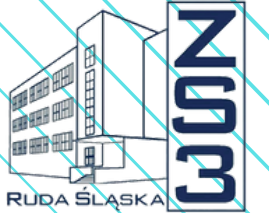
"Ktoś przejął moje konto na Instagramie i wysyłał moim znajomym linki do wyłudzenia pieniędzy.

Wszyscy myśleli, że to ja!"

"Straciłem konto w grze, w którą grałem przez 3 lata. Wszystkie skiny, poziomy, osiągnięcia –
wszystko zniknęło."

"Haker wszedł na moje konto Snapchat i groził, że opublikuje moje prywatne zdjęcia,
jeśli nie zapłacę."

Program “Klikaj z głową - edukacja cyfrowa ZS3”



JAK STWORZYĆ NAPRAWDĘ BEZPIECZNE HASŁO?

3 SPRAWDZONE METODY



METODA 1

ZDANIE - HASŁO

1. Wymyśl absurdalne, łatwe do zapamiętania zdanie "Mój pies Reksio zjadł 7 pizz w poniedziałek!"
2. Weź pierwsze litery + cyfry + znaki M p R z 7 p w p !
3. Gotowe hasło MpRz7pwp!

METODA 2

KLOCKI (4-5 losowych słów + cyfry + znaki)

Połącz niepowiązane słowa z cyframi i znakami:

1. Dinozaur#Gitara92!Balon@Ketchup
2. Tramwaj&Słońce88#Klawiatura@Herbata
3. Parasol!Czekolada77\$Monitor@Pizza

METODA 3

MENEDŻER HASEŁ

Co to jest?

Program, który:

- Generuje super-silne hasła (np. g7#mK9\$pL2@xR5!)
- Bezpiecznie je przechowuje
- Automatycznie wpisuje za Ciebie
- Musisz zapamiętać tylko JEDNO główne hasło!

Popularne menedżery:

- Bitwarden (darmowy)
- 1Password
- LastPass
- Keeper

ZŁOTE ZASADY

ZŁOTE ZASADY BEZPIECZNYCH HASEŁ:

- MINIMUM 12 ZNAKÓW (najlepiej 15-20)
- WIELKIE i małe litery + cyfry + znaki specjalne (!@#\$%^&*)
- RÓŻNE hasło do KAŻDEGO konta (szczególnie: e-mail, media społecznościowe, bankowość)
- WŁĄCZ weryfikację dwuetapową (2FA) wszędzie gdzie możesz
- NIGDY nie udostępniaj hasła nikomu (nawet bliskim)
- Regularnie ZMIENIAJ hasła do ważnych kont (co 3-6 miesięcy)

CZEGO UNIKAĆ?

NIGDY NIE UŻYWAJ:

- Swojego imienia lub nazwiska
- Daty urodzenia
- Nazwy szkoły, ulicy, miasta
- Słowa "hasło" lub "password"
- Ciągów cyfr: 12345, 11111, 2008
- Nazwy ulubionej gry, drużyny, zespołu
- Imienia zwierzaka
- Klawiatury: qwerty, asdfgh

Te hasła zostają złamane w SEKUNDY.

WERYFIKACJA DWUETAPOWA



WERYFIKACJA DWUETAPOWA (2FA) to dodatkowa warstwa ochrony.

Jak działa?

1. Wpisujesz hasło
2. Dostajesz kod SMS lub z aplikacji
3. Wpisujesz kod
4. Dopiero teraz jesteś zalogowany.

Nawet jeśli ktoś ukradnie Twoje hasło, to bez kodu z Twojego telefonu NIE wejdzie na konto!

PRAKTYCZNE PORADY

DODATKOWE PORADY:

- Sprawdź, czy Twoje dane wyciekły: www.haveibeenpwned.com
- NIE zapisuj haseł w:
 - Notatkach w telefonie
 - Plikach Word/Excel
 - Zdjęciach → Użyj menedżera haseł!
- Zmień NATYCHMIAST hasło jeśli:
 - Podejrzewasz, że ktoś je zna
 - Wpisałeś je na podejrzanej stronie
 - Dostałeś powiadomienie o nieautoryzowanym logowaniu
- Nigdy nie loguj się na:
 - Cudzych komputerach
 - Publicznych WiFi bez VPN
 - Podejrzanych stronach

POTRZEBUJESZ POMOCY?

Jeśli padłeś ofiarą włamania:

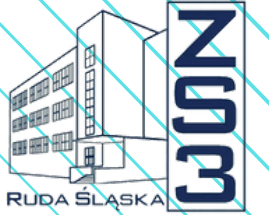
- Natychmiast zmień hasła
- Zgłoś incydent do administratorów serwisu
- Powiadom znajomych
- Zgłoś na Policję (jeśli poważne konsekwencje)
- Porozmawiaj z rodzicem/nauczycielem

☎ Telefon zaufania dla dzieci i młodzieży: 116 111

💬 W szkole porozmawiaj z: wychowawcą klasy, nauczycielem informatyki, pedagogiem szkolnym.

Nie wstydź się! To może spotkać każdego.

Program “Klikaj z głową - edukacja cyfrowa ZS3”



DZIĘKUJEMY ZA UWAGĘ

