

Podaj dalej wiedzę, nie podawaj danych!

Mistrzowie

bezpiecznych haseł!



CELE OGÓLNE

- Kształtowanie wiedzy z zakresu bezpieczeństwa w sieci
- Wprowadzenie w zagadnienie bezpieczeństwa haseł
- Rozwijanie świadomości dotyczącej znaczenia bezpiecznych haseł internetowych

CELE SZCZEGÓŁOWE: UCZEŃ:

- Zna zasady tworzenia i potrafi stworzyć silne hasło zabezpieczające
- Odróżnia hasła silne od słabych
- Zna i rozumie zagrożenia związane z korzystaniem z haseł
- Sprawdza swoją wiedzę o hasłach
- Rozwiązując quiz, analizuje i ocenia praktyki internetowe na podstawie studium przypadku

DO 30 OSÓB 45 MINUT

SALA LEKCYJNA, ŚWIETLICA

UCZNIOWIE SZKOŁY PODSTAWOWEJ

ŚRODKI DYDAKTYCZNE:

- Tablice do pisania odpowiedzi (lub kartki papieru) dla uczniów
- Tablica do zaznaczania odpowiedzi i liczenia punktów dla nauczyciela
- Markery/długopisy
- Ekran/projektor do wyświetlania prezentacji z pytaniami oraz filmików

METODY PRACY:

Problemowa: analiza treści
Utrwalająca: quiz
Gra dydaktyczna

FORMY PRACY:

Grupowa
Indywidualna
Zespołowa



Amelia

Zalecamy, by nauczyciel odczytywał wszystkie treści pytań i odpowiedzi w grze dydaktycznej — niezależnie od wieku uczniów

Realizowane w scenariuszu punktu podstawy programowej VII.5.1. VII.5.2. VII.5.3.

Słowniczek pojęć

Menedżer haseł

Menedżer haseł to narzędzie, które bezpiecznie przechowuje i zarządza Twoimi hasłami, automatycznie wypełniając je podczas logowania.

Nadanie zdalnego dostępu do komputera

Rozwiązanie, które pozwala innym użytkownikom na kontrolowanie i korzystanie z komputera przez internet za pomocą specjalnego oprogramowania.

"2FA" (dwuskładnikowe uwierzytelnianie)

"2FA" to dodatkowa warstwa zabezpieczeń, która wymaga potwierdzenia tożsamości za pomocą dwóch różnych metod logowania, np. hasła i kodu z telefonu. Przykładowo, logowanie metodą 2FA może wyglądać następująco: najpierw podajesz login (adres email) oraz hasło, a następnie otrzymujesz na swój telefon kod, który należy wprowadzić na stronie logowania. Z tego typu zabezpieczeń korzystamy np. przy logowaniu do kont bankowych.

CEL GRY:

Gra ma na celu zapoznanie uczniów z zagadnieniem tworzenia silnych haseł oraz ochrony swoich danych w internecie. Uczniowie dowiedzą się również, jak unikać zagrożeń związanych z hasłami i dlaczego bezpieczeństwo w sieci jest ważne.

PRZYGOTOWANIE:

- Zapoznaj się z zasadami gry i treściami pytań przed rozpoczęciem zajęć.
- Przygotuj tablice lub kartki do odpowiedzi dla uczniów, markery i ekran/projektor do wyświetlania filmów lub obrazków oraz tablicę do zapisywania punktacji zespołów.
- Upewnij się, że masz dostęp do przykładów haseł oraz krótkiego filmu/scenki, która będzie przedstawiać sytuację związaną z prośbą o hasło.

ZASADY GRY:

- Nauczyciel dzieli grupę na zespoły, maksymalnie po 5 uczniów w zespole. W grze może brać udział maksymalnie 6 zespołów.
- Uczniowie pracują w zespołach i odpowiadają na pytania, które zadaje nauczyciel. Gdy upłynie czas na udzielenie odpowiedzi, każdy z zespołów unosi kartkę z zapisaną odpowiedzią. Na prośbę nauczyciela zespoły kolejno odczytują swoje odpowiedzi.
- Po każdej rundzie nauczyciel przyznaje punkty za poprawne odpowiedzi. Wyniki może zapisywać na tablicy szkolnej.
- Po odczytaniu wszystkich pytań, nauczyciel podsumowuje punktację. Zespół, który zdobędzie najwięcej punktów, wygrywa.

PODSUMOWANIE:

Na koniec nauczyciel podkreśla najważniejsze zasady dotyczące silnych haseł: **długość, złożoność i bezpieczeństwo przechowywania**. Wskazuje, że nie należy nikomu podawać swoich haseł poza opiekunami.

SYSTEM PUNKTACJI:

- Za każdą poprawną odpowiedź zespoły otrzymują 10 punktów.
- W rundzie na szybkość, zespół, który jako pierwszy podniesie tablicę z poprawną odpowiedzią, zdobywa dodatkowe 5 punktów.
- W rundzie praktycznej za stworzenie poprawnego, silnego hasła każdy zespół otrzymuje 20 punktów.
- Za niepoprawne odpowiedzi zespół otrzymuje 0 punktów.

Co to jest hasło?

Wprowadzenie
do gry dydaktycznej

10 minut



Czy znacie opowieści, w których wejścia do skarbcza lub ukrytej komnaty broni zaklęcie?

Abrakadabra,
sezamie otwórz się,
przyjacielu wejdź?

Te baśniowe zaklęcia to nic
innego jak Wasze hasła.



Hasło

- Twoje magiczne zaklęcie

- Hasło to Twoja tajemnica. Nie może być znane nikomu poza Tobą. To tajna kombinacja składająca się z minimum 10 znaków: liter, cyfr i symboli, która chroni nasze dane w internecie.
- Dzięki hasłu tylko Ty masz dostęp do swoich: gier, e-maila, a nawet do telefonów.

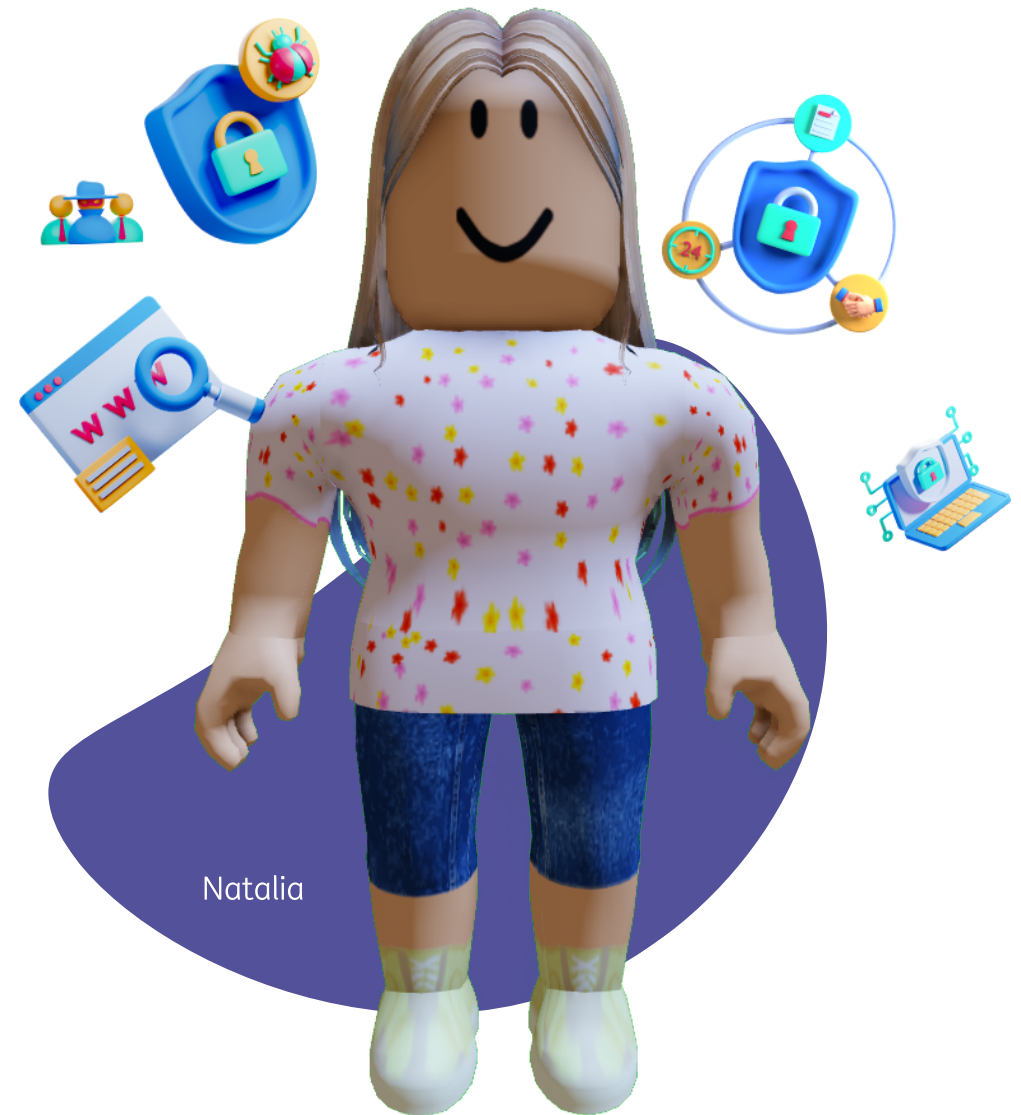
Ale czy wszystkie hasła są tak samo bezpieczne?

Pamiętaj, najbezpieczniej jest korzystać z różnych haseł. Nie powtarzaj wszędzie tego samego!



Jakie hasło jest bezpieczne?

- Długie
(przynajmniej 10 znaków)
- Trudne
(mieszanka liter, cyfr i symboli)
- Bez danych osobistych
(np. imię, data urodzenia)



Co chroni Twoje hasło?

- Dwustopniowa weryfikacja (2FA)
- Niezapisywanie haseł w publicznych miejscach (np. na komputerach w szkole)
- Nieudostępnianie swojego hasła innym



Czy to hasło jest bezpieczne?

Pytania TAK / NIE

ok. 5 min



Czy to hasło jest bezpieczne? Zasady.

- Zaraz zobaczycie różne przykłady haseł, a Waszą misją będzie zdecydować, czy hasło jest bezpieczne, czy nie.
- Aby udzielić odpowiedzi, podnieście tabliczkę lub kartkę z napisem 'Tak' lub 'Nie'.
- Na każdą odpowiedź dostaniecie 30 sekund.
- Za każdą poprawną odpowiedź otrzymacie po 10 pkt.



Czy to hasło jest bezpieczne?

12345

00:30

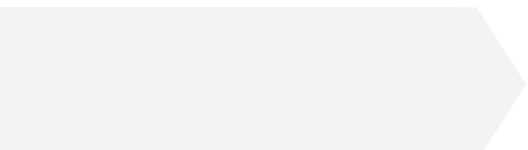
Czy to hasło jest bezpieczne?

NIE

12345

NIE

Czy to hasło jest bezpieczne?



kot123

00:30

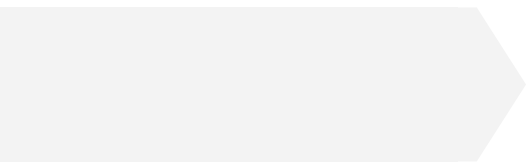
Czy to hasło jest bezpieczne?

NIE

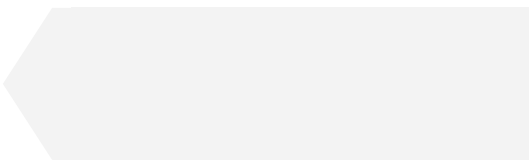
kot123

NIE

Czy to hasło jest bezpieczne?



M@l1ny2024



00:30

Czy to hasło jest bezpieczne?

TAK

M@l1ny2024

TAK

Czy to hasło jest bezpieczne?

haslo123

00:30

Czy to hasło jest bezpieczne?

NIE

haslo123

NIE

Czy to hasło jest bezpieczne?

T!grys9LwY

00:30

Czy to hasło jest bezpieczne?

TAK

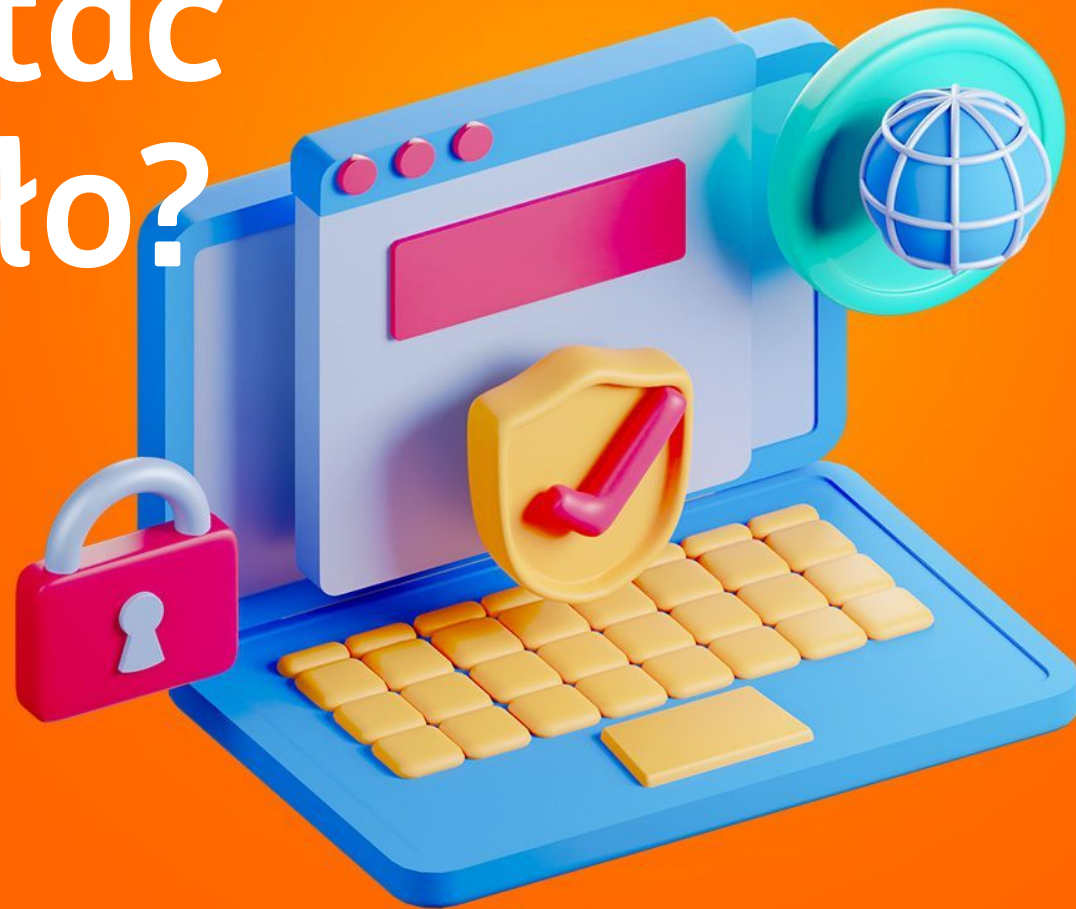
T!grys9LwY

TAK

Jak zapamiętać i chronić hasło?

Pytania otwarte

ok. 5 min



Jak zapamiętać hasło? Zasady.

- W grupach wymyślcie różne sposoby zapamiętania haseł, bez ich zapisywania w oczywistych miejscach.
Zapiszcie pomysły na tablicy/kartce.
- Na przygotowanie odpowiedzi dostaniecie 3 minuty.
- Za każdą poprawną odpowiedź otrzymacie po 10 pkt.



Jakie są sposoby na zapamiętanie
hasła?

03:00

Przykładowe sposoby na zapamiętanie hasła



Zrobić rymowankę, w której ukryte są słowa z hasła.



Zapamiętać poprzez historię związaną z hasłem.



Można również wspomóc się menedżerem haseł-programem, który przechowuje hasła i pomaga w zarządzaniu nimi



Gdzie najlepiej przechowywać hasło?

Analiza przypadków

ok. 3 min



Gdzie najlepiej przechowywać hasło? Zasady.

- Za chwilę zobaczycie trzy przykłady przechowywania haseł. Zdecydujcie, które miejsce jest najbezpieczniejsze.
- Na przygotowanie odpowiedzi dostaniecie 1 minutę.
- Za każdą poprawną odpowiedź otrzymacie po 10 pkt.



Gdzie najlepiej przechowywać hasło?

Przykłady sytuacji:

1. Zapisanie hasła na kartce przyklejonej do monitora.
2. Powiedzenie hasła koledze.
3. Zapisanie hasła w menedżerze haseł programie, który bezpiecznie przechowuje hasła i pomaga w zarządzaniu nimi, umożliwiając łatwy dostęp do kont przy użyciu jednego głównego hasła.



Gdzie najlepiej przechowywać hasło?

01:00

Gdzie najlepiej przechowywać hasło?

W tajemnicy!

Najbezpieczniejszym sposobem na przechowywanie hasła, jest zapamiętanie go. Możemy wspomóc się menedżerem haseł, który przechowuje Twoje hasła w jednym miejscu.

Pamiętaj! Nigdy nie zapisuj haseł w łatwo dostępnych miejscach!



Co jest najważniejsze w silnym haśle?

Pytania na szybkość
ok. 5 min



Co jest najważniejsze w silnym haśle? Zasady.

- Zaraz zobaczycie pytania, a Waszą misją będzie jak najszybciej podnieść tabliczkę z poprawną odpowiedzią.
- Na każdą odpowiedź dostaniecie 30 sekund.
- Za każdą poprawną odpowiedź dostaniecie 10 punktów.
Zespół, który jako pierwszy podniesie tabliczkę z poprawną odpowiedzią, zdobywa dodatkowe 5 punktów.



Co jest najważniejsze w silnym haśle?

**Czy w haśle powinny
być cyfry?**

00:30

Co jest najważniejsze w silnym haśle?

TAK

**Czy w haśle powinny
być cyfry?**

TAK

Co jest najważniejsze w silnym haśle?

**Czy można używać
swojego imienia jako
hasła?**

00:30

Co jest najważniejsze w silnym haśle?

NIE

**Czy można używać
swojego imienia jako
hasła?**

NIE

Co jest najważniejsze w silnym haśle?

**Czy hasło powinno
być krótkie,
np. 3 znaki?**

00:30

Co jest najważniejsze w silnym haśle?

NIE

**Czy hasło powinno
być krótkie,
np. 3 znaki?**

NIE

Co jest najważniejsze w silnym haśle?

**Czy w haśle mogą być
znaki specjalne,
np. "@"?**

00:30

Co jest najważniejsze w silnym haśle?

TAK

Czy w haśle mogą być
znaki specjalne,
np. "@"?

TAK

Podsumowanie

Bezpieczne hasło powinno się składać z:

- 💡 Przynajmniej 10 znaków.
- 💡 Małych i dużych liter, cyfr i znaków specjalnych (np. !@#\$%^&*()_+-=).
- 💡 Nie opierać się na oczywistych informacjach, takich jak imię czy data urodzenia.



Jak stworzyć silne hasło?

Runda praktyczna

ok. 5 min



Jak stworzyć silne hasło? Zasady.

- Wymyślcie dowolne, bezpieczne hasło i zapiszcie je na tablicy/kartce.
- Na przygotowanie silnego hasła dostaniecie 2 minuty.
- Za poprawną odpowiedź dostaniecie po 20 pkt.



Jak stworzyć silne hasło?

02:00

Z czego składa się bezpieczne hasło?



Minimum 10 znaków



Co najmniej jednej litery, jednej cyfry i jednego znaku specjalnego (np. @, !, \$)



Co zrobić, gdy ktoś prosi o hasło?

Analiza scenki

ok. 5 min



Co zrobić, gdy ktoś prosi o hasło?

Zasady.

- Zaraz zapoznacie się ze scenką.
- Po zapoznaniu się ze scenką odpowiadacie na pytania.
- Na każdą odpowiedź dostaniecie 30 sekund.
- Za każdą poprawną odpowiedź otrzymacie po 10 pkt.



**IGOR, PODASZ
MI SWOJE HASŁO
DO GRY?**

**CHCIAŁBYM ZAGRAĆ
NA TWOIM KONCIE!**



Co zrobić, gdy ktoś prosi o hasło?

**Czy powinieneś
podać swoje hasło
koledze?**

00:30

Co zrobić, gdy ktoś prosi o hasło?

NIE

**Czy powinieneś
podać swoje hasło
koledze?**

NIE

Co zrobić, gdy ktoś prosi o hasło?

Co powinieneś zrobić,
gdy ktoś prosi Cię o
hasło?

00:30



Co zrobić, gdy ktoś prosi o hasło?

Co powinieneś zrobić, gdy ktoś prosi Cię o hasło?



Odmówić



Poinformować dorosłego o zaistniałej sytuacji.



Quiz ewaluacyjny ABC

Czy wiesz już wszystko o hasłach?

do 10 min

Runda nieobowiązkowa*



Czy wiesz już wszystko o hasłach?

- Zaraz zobaczycie pytanie i trzy możliwe odpowiedzi.
- Zastanówcie się w zespołach i podnieście tabliczkę lub kartkę z napisem 'A', 'B' lub 'C'.
- Na każdą odpowiedź dostaniecie 30 sekund.
- Za każdą poprawną odpowiedź dostaniecie po 10 pkt.



Nie możesz zainstalować najnowszej gry.

Ktoś w internecie oferuje, że Ci pomoże, ale najpierw musisz mu dać zdalny dostęp do swojego komputera.

Co robisz?

A

Daję dostęp i czekam,
aż naprawi mój problem

B

Nie daję dostępu

C

Daję dostęp tylko do
niektórych funkcji

00:30

Nie możesz zainstalować najnowszej gry.

Ktoś w internecie oferuje, że Ci pomoże, ale najpierw musisz mu dać zdalny dostęp do swojego komputera.

Co robisz?



Daję dostęp i czekam aż
naprawi mój problem

B

Nie daję dostępu



Daję dostęp tylko do
niektórych funkcji

Który z poniższych jest dobrym sposobem
na stworzenie silnego hasła?

A

Użycie swojego imienia
i nazwiska

B

Użycie kombinacji liter,
cyfr i symboli

C

Użycie daty urodzenia

00:30

Który z poniższych jest dobrym sposobem
na stworzenie silnego hasła?



B

Użycie kombinacji liter,
cyfr i symboli



Jakie jest dobre miejsce na przechowywanie haseł?

A

W notesie, w którym
zapisuje wszystkie
ważne rzeczy

B

W serduszk!

C

Bezpieczne, znane tylko
Tobie (na przykład
menedżer haseł)

00:30

Jakie jest dobre miejsce na przechowywanie haseł?

A
X
W notesie, w którym
zapisujesz wszystkie
ważne rzeczy

B
X
W słowniku!

C
Bezpieczne, znane tylko
Tobie (na przykład
menedżer haseł)

Dlaczego nie należy dzielić się swoim hasłem z innymi?

A

Bo ukradną mi pomysł
na fajne hasło

B

Ponieważ mogą uzyskać
dostęp do moich kont i je
wykorzystać

C

Ponieważ hasła są
nudne

00:30

Dlaczego nie należy dzielić się swoim hasłem z innymi?

A
X
Bo ukradł mi pomysł
na fajne hasło

B
Ponieważ mogą uzyskać
dostęp do moich kont i je
wykorzystać

C
X
Ponieważ dostała się
do niego

Co zrobić, jeśli podejrzewasz, że ktoś
poznał twoje hasło?

A

Zmienić hasło
natychmiast

B

Zignorować, bo na
pewno nic się nie stanie

C

Zapytać tę osobę, czy
uważa, że masz fajne
hasło

00:30

Co zrobić, jeśli podejrzewasz, że ktoś poznał twoje hasło?

A

Zmienić hasło
natychmiast

B

Zignorować, bo na
pewno nic z tego nie stanie

C

Zapytać tę osobę, czy
uważa, że masz fajne
hasło

Co to jest menedżer haseł?

A

Program do
przechowywania haseł
w bezpieczny sposób

B

Osoba, która tworzy
hasła dla innych i
dostaje za to wypłatę

C

Postać z kreskówki

00:30

Co to jest menedżer haseł?

A

Program do
przechowywania haseł
w bezpieczny sposób

B

Osoba, która tworzy
hasła dla innych i
dostaje za to wypłatę

C

Postać z kreskówki

Co oznacza skrót "2FA" (dwuskładnikowe uwierzytelnianie)?

A

Dodanie dodatkowej
cyfry do hasła

B

Model samolotu

C

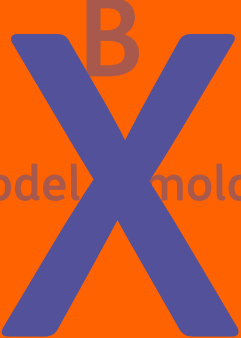
Drugą warstwę
zabezpieczeń, np. kod
SMS lub aplikację do
uwierzytelniania

00:30

Co oznacza skrót "2FA" (dwuskładnikowe uwierzytelnianie)?

A

Dodanie dodatkowej
cyfry do hasła

B

Model samolotu

C
Drugą warstwę
zabezpieczeń, np. kod
SMS lub aplikację do
uwierzytelniania

Które hasło jest najsilniejsze?

A

kot123

B

AbC!897#kOT

C

123456

00:30

Które hasło jest najsilniejsze?

X

B

AbC!897#kOT

X

Dlaczego warto mieć silne hasło?

A

Żeby koledzy zazdrościli

B

Aby było trudne do
odgadnięcia dla innych osób

C

Aby wyglądało ciekawie

00:30

Dlaczego warto mieć silne hasło?



Żeby koleś zazdrościł

B

Aby było trudne do
odgadnięcia dla innych osób



Aby wyglądało ciekawie

Jaki jest dobry sposób na zapamiętanie trudnego hasła?

A

Zamienić trudne hasło
na krótkie i łatwe do
zapamiętania

B

Napisać hasło na ręce
markerem

C

Użyć menedżera haseł

00:30

Jaki jest dobry sposób na zapamiętanie trudnego hasła?



Zamienić trudne hasło
na krótkie i łatwe do
zapamiętania



Napisać hasło na ręce
możemy

C

Użyć menedżera haseł



Dlaczego hasło jest
ważne?



Co robić, gdy ktoś pyta
o nasze hasło?



Jak dodatkowo chronić
swoje hasła?



Jakie hasło jest
bezpieczne?

Mistrzowie

bezpiecznych haseł!

