

SCENARIUSZ LEKCJI

Menedżer haseł i logowanie dwuskładnikowe

Cyberbezpieczeństwo

Klasy VII i VIII

45 minut

Lekcja otwarta

Uczeń tworzy jedno mocne hasło główne, rozumie zasadę działania menedżera haseł i potrafi opisać, przed czym chroni drugi składnik logowania.

Czego uczy ta lekcja

Budowa hasła głównego i rola menedżera

Umiesz ułożyć jedno długie hasło główne i wyjaśnić, dlaczego pozostałych haseł nie musisz już pamiętać.

Drugi składnik logowania

Wiesz, czym jest kod z aplikacji lub klucz sprzętowy i przed jakim atakiem Cię chroni, gdy hasło wycieknie.

Potrzebny sprzęt

laptopy szkolne z przeglądarką, po jednym na ucznia lub na parę, projektor lub monitor do pokazu, kartki i długopisy do zapisania hasła głównego, kostki do gry lub generator losowy do metody słów losowych

Podstawa programowa

Informatyka, Szkoła podstawowa, klasy VII i VIII

Cele kształcenia, wymagania ogólne

- III. Posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi, w tym znajomość zasad działania urządzeń cyfrowych i sieci komputerowych oraz wykonywania obliczeń i programów.
- V. Przestrzeganie prawa i zasad bezpieczeństwa. Respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych.

Treści nauczania, wymagania szczegółowe

- V.1. opisuje kwestie etyczne związane z wykorzystaniem komputerów i sieci komputerowych, takie jak: bezpieczeństwo, cyfrowa tożsamość, prywatność, własność intelektualna, równy dostęp do informacji i dzielenie się informacją; (Podstawa dla wątku o cyfrowej tożsamości i prywatności. Punkt nie wymienia menedżera haseł ani logowania dwuskładnikowego, wymienia bezpieczeństwo, cyfrową tożsamość i prywatność jako kwestie etyczne, które uczeń opisuje.)
- V.2. postępuje etycznie w pracy z informacjami; (Dopasowanie częściowe, dotyczy postawy w pracy z informacjami.)
- III.3. poprawnie posługuje się terminologią związaną z informatyką i technologią. (Dopasowanie częściowe: poprawne posługiwanie się terminologią, uzasadnia wprowadzenie pojęć hasło główne, menedżer haseł, drugi składnik logowania.)

NOWA PODSTAWA PROGRAMOWA, DZ.U. 2026 POZ. 378

5.1. chroni hasła, używa menedżera haseł oraz świadomie zarządza informacjami o sobie udostępnianymi w Internecie;

5.3. rozpoznaje próby wyłudzenia danych i stosuje działania zapobiegawcze;

ODNIESIENIE DO SZKOŁY PONADPODSTAWOWEJ, ZAKRES PODSTAWOWY

Ta sama lekcja w liceum lub technikum realizuje poniższe wymagania, Dz.U. 2018 poz. 467.

V.3. stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji; (Do wykorzystania, gdy lekcję prowadzimy w liceum lub technikum.)

Podstawa prawna: Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej, Dz.U. 2017 poz. 356.

Brzmienie: Załącznik nr 2 do Dz.U. 2017 poz. 356 w brzmieniu nadanym przez Dz.U. 2024 poz. 996, część KLASZ VII i VIII

Lista kontrolna przed lekcją

Do odhaczenia dzień wcześniej i 10 minut przed dzwonkiem.

- ☐ Dzień wcześniej: wydrukujcie listę 36 słów ponumerowanych od 11 do 66 (dziesiątki i jedności tylko od 1 do 6), po jednej na parę uczniów, oraz kartę pracy dla każdego ucznia. Sprawdźcie, że w słowach nie ma imion, nazw marek ani nazw z gier.
- ☐ Dzień wcześniej: przygotujcie kostki do gry, po jednej na parę. Jeśli ich brakuje, wydrukujcie tabelę losową albo użyjcie generatora liczb w przeglądarce bez logowania.

- ☐ Dzień wcześniej: spiszcie pięć haseł do etapu Sprawdzenie: dwa długie z losowych słów i trzy krótkie ze znakami specjalnymi, na przykład Ala2011!, P@sswOrd, Burek1234.
- ☐ Dzień wcześniej: sprawdźcie na szkolnym laptopie, gdzie w ustawieniach przeglądarki leży lista zapisanych haseł, i upewnijcie się, że nie ma tam żadnych prawdziwych haseł nauczycieli ani uczniów. Jeśli są, usuńcie je przed lekcją.
- ☐ Dzień wcześniej: przygotujcie do pokazu ekran logowania z prośbą o kod z aplikacji na własnym koncie testowym albo zrzut ekranu takiego kroku. Uczniowie nie logują się do niczego.
- ☐ 10 minut przed lekcją: włączcie projektor i otwórzcie prezentację, sprawdźcie, że laptopy uczniów startują i mają przeglądarkę.
- ☐ 10 minut przed lekcją: rozłóżcie na ławkach kartki na hasło główne, kostki i listę słów, karty pracy trzymajcie do etapu Praca uczniów.
- ☐ 10 minut przed lekcją: zapiszcie na tablicy zasadę na dziś: prawdziwych haseł nie wpisujemy na szkolnym sprzęcie i nie logujemy się do własnych kont.

Rozgrzewka na start

BEZ SPRZĘTU, 3 MIN

Zapisać na tablicy dwa hasła: Ala2011! oraz sople wiadro grzmot lampa. Poproście uczniów o wybór ręką do góry, które hasło jest trudniejsze do złamania, i o jedno słowo uzasadnienia od dwóch osób z każdej strony.

Czego się spodziewać: Większość wskaże pierwsze hasło ze względu na wykrzyknik i cyfry. Chodzi o to, żeby ta intuicja padła na głos, bo cała lekcja ją rozbiera: liczy się długość i nieprzewidywalność, nie znak specjalny. Nie rozstrzygajcie jeszcze, wróćcie do tych dwóch haseł w etapie Sprawdzenie.

Przebieg lekcji

Pięć etapów, razem 45 minut.

1

Wejście, 5 min

Nauczyciel prosi, żeby każdy policzył w głowie, na ilu stronach i w ilu aplikacjach ma konto, i pokazał liczbę na palcach lub zapisał na kartce. Potem pyta, ile różnych haseł tam używa. Zestawienie tych dwóch liczb zwykle mówi wszystko: kont jest kilkanaście, haseł dwa albo trzy. Nauczyciel nie komentuje tego jeszcze oceniająco, tylko zapisuje obie liczby na tablicy.

2

Pokaz, 10 min

Nauczyciel tłumaczy, na czym polega ponowne użycie tego samego hasła: gdy jeden serwis traci bazę haseł, ktoś próbuje tej samej pary adres i hasło w innych serwisach. Potem pokazuje metodę hasła głównego z losowych słów: cztery lub pięć przypadkowych, niepowiązanych słów, wylosowanych kostką albo losowaniem z listy, zapisanych razem. Wyjaśnia, dlaczego długość bije skomplikowanie, i dlaczego imię psa oraz rok urodzenia odpadają. Następnie pokazuje menedżer haseł wbudowany w przeglądarkę i wolne narzędzie Bitwarden, omawiając zasadę: menedżer pamięta wszystkie hasła, uczeń pamięta jedno. Na końcu pokazuje ekran logowania z kodem z aplikacji i mówi, co dzieje się, gdy ktoś zna hasło, ale nie ma telefonu ucznia.

3

Praca uczniów, 20 min

Uczniowie pracują z kartą pracy, która ma pięć zadań. Pierwsze: losują kostką cztery słowa z listy ponumerowanej od 11 do 66 i układają z nich własne hasło główne, zapisują je na kartce, którą zabierają do domu, i nie pokazują nikomu w sali. Drugie: porządkują pięć kont z listy podanej w karcie (poczta, dziennik elektroniczny, konto w grze, sklep internetowy, komunikator) od najważniejszego do najmniej ważnego pod względem ochrony i uzasadniają pierwsze miejsce. Trzecie: na laptopie sprawdzają w ustawieniach przeglądarki, gdzie znajduje się lista zapisanych haseł, i wypisują trzy rzeczy, które zrobi ktoś, kto dostanie się do niezablokowanego komputera z taką listą. Czwarte i piąte zadanie (różnica między kodem z aplikacji a SMS oraz plan pracy domowej) uczniowie wykonują, jeśli zostanie czas, w innym wypadku kończą je w domu. Nauczyciel pilnuje, żeby nikt nie wpisywał prawdziwych haseł na szkolnym sprzęcie i żeby uczniowie nie logowali się do własnych kont.

4

Sprawdzenie, 5 min

Nauczyciel czyta pięć przykładowych haseł przygotowanych wcześniej, w tym dwa długie z losowych słów i trzy krótkie ze znakami specjalnymi. Klasa głosuje, które jest najtrudniejsze do złamania, a nauczyciel wyjaśnia wynik przez długość i nieprzewidywalność, nie przez obecność znaku specjalnego. Potem sprawdza na dwóch przykładach, czy uczniowie poprawnie wskazali konta priorytetowe.

5

Podsumowanie, 5 min

Nauczyciel podsumowuje trzy zasady do zapisania: jedno hasło główne i menedżer na resztę, różne hasło do każdego serwisu, drugi składnik na koncie pocztowym w pierwszej kolejności, bo przez pocztę odzyskuje się pozostałe konta. Zadaje pracę domową: włączyć drugi składnik na jednym własnym koncie razem z rodzicem i zapisać, ile to zajęło minut.

Do powiedzenia na głos

„Jeżeli używasz tego samego hasła w kilku miejscach, to wyciek u jednego dostawcy otwiera wszystkie Twoje konta naraz.”

„Twoje zadanie to zapamiętać jedno hasło. Resztę pamięta menedżer i robi to lepiej niż Ty.”

„Długość jest ważniejsza niż wykrzykniki na końcu. Cztery losowe słowa biją zamianę litery o na zero.”

„Drugi składnik to warunek, żeby sam skradziony ciąg znaków przestał komukolwiek wystarczać do wejścia na Twoje konto.”

Typowe błędy uczniów i co z nimi zrobić

- Uczniowie układają hasło z bliskich sobie słów, na przykład z imion z jednej rodziny albo nazw z jednej gry. Przypomnijcie, że słowa mają być losowane, a nie wybierane, bo wybór zawsze jest przewidywalny.
- Uczniowie uważają, że zamiana litery na cyfrę robi z hasła mocne hasło. Pokażcie, że taka zamiana jest powszechnie znana i nie dokłada trudności.
- Uczniowie chcą przetestować prawdziwe hasło w narzędziu sprawdzającym siłę haseł. Zabrońcie tego wprost i wyjaśnijcie, że prawdziwego hasła nie wkleja się nigdzie poza ekranem logowania.
- Uczniowie traktują kod SMS jak najbezpieczniejszy drugi składnik. Wyjaśnijcie, że kod z aplikacji albo klucz sprzętowy jest lepszy, bo numer telefonu da się przejąć przez podszycie się pod właściciela u operatora, a aplikacja i klucz działają na urządzeniu ucznia i od numeru nie zależą.
- Uczniowie zapisują hasło główne w pliku na komputerze szkolnym. Ustalcie, że hasło główne idzie na kartkę do domu albo do pamięci, nigdy do wspólnego sprzętu.

Warianty lekcji

Bez sprzętu i internetu

Cała lekcja działa na kartkach i kostkach do gry. Uczniowie losują słowa z przygotowanej przez nauczyciela listy ponumerowanej od 11 do 66 (pierwszy rzut daje cyfrę dziesiątek, drugi jedności), układają hasło główne i zapisują je na kartce, której nikomu nie pokazują. Rolę menedżera odgrywa zamknięta koperta z kartkami hasel do kilku wymyślonych kont; klasa ustala do niej wspólne, wymyślone na lekcji hasło główne, żadne prawdziwe ani osobiste hasło nie pada na głos. Drugi składnik ćwiczy się scenką: jeden uczeń zna kartkę z hasłem do koperty, drugi trzyma kartonik z kodem zmieniającym się co rundę, i klasa sprawdza, czy sam znawca hasła otworzy kopertę bez kodu.

Dla szybszych uczniów

Uczeń opisuje w pięciu zdaniach, co dokładnie dzieje się przy logowaniu na podrobionej stronie, jeśli ofiara ma włączony kod z aplikacji, i wskazuje, dlaczego klucz sprzętowy albo klucz dostępu radzi sobie w tej sytuacji lepiej niż kod przepisywany ręcznie.

Przy trudnościach

Uczeń układa hasło z trzech wylosowanych słów zamiast czterech i korzysta z gotowego wzoru zdania do uzupełnienia. W zadaniu o priorytetach dostaje trzy konta zamiast pięciu i wybiera to jedno, na którym drugi składnik jest najważniejszy, wraz z uzasadnieniem wybranym z dwóch podanych.

Kryteria oceny

Trzy poziomy dla każdej umiejętności. Opis mówi, co uczeń pokazuje, a nie ile punktów dostaje.

UMIEJĘTNOŚĆ	PODSTAWOWY	DOBRY	BARDZO DOBRY
-------------	------------	-------	--------------

UMIEJĘTNOŚĆ	PODSTAWOWY	DOBRY	BARDZO DOBRY
Budowa hasła głównego i rola menedżera	Uczeń układa hasło główne z czterech wylosowanych słów, liczy jego znaki i mówi, że menedżer haseł pamięta pozostałe hasła, a on pamięta jedno.	Uczeń dodatkowo wyjaśnia, dlaczego losowanie jest lepsze od wybierania słów, i wskazuje w podanym hasle typu Ala2011! elementy, które czynią je przewidywalnym.	Uczeń wyjaśnia, dlaczego to samo hasło w wielu serwisach zamienia jeden wyciek w utratę wielu kont, opisuje, co dzieje się z hasłami w menedżerze (szyfrowanie hasłem głównym, którego dostawca nie zna) i tłumaczy, dlaczego hasła głównego nie da się odzyskać.
Drugi składnik logowania	Uczeń mówi, że drugi składnik to coś, co ma przy sobie, i że po jego włączeniu samo hasło nie wystarcza do zalogowania.	Uczeń dodatkowo wskazuje pocztę jako pierwsze konto do zabezpieczenia i uzasadnia to odzyskiwaniem haseł przez pocztę, a także odróżnia kod z aplikacji od kodu SMS i nazywa słabość SMS.	Uczeń opisuje na przykładzie z życia, w którym momencie drugi składnik przerywa atak po wycieku hasła, wyjaśnia, dlaczego klucz sprzętowy działa na podrobionej stronie lepiej niż kod przepisywany ręcznie, i wie, do czego służą kody zapasowe.

Pytania do dyskusji

Na podsumowanie lekcji. Nie mają jednej poprawnej odpowiedzi, chodzi o uzasadnienie.

1. Menedżer haseł trzyma wszystkie hasła w jednym miejscu. Kiedy taka koncentracja jest siłą, a kiedy staje się słabością, i co musiałoby się stać, żeby była gorsza od jednego hasła powtórzonego w dziesięciu serwisach?
2. Drugi składnik logowania dokłada kilka sekund do każdego logowania. Na których kontach ten koszt jest wart zapłacenia, a na których Waszym zdaniem nie, i jak byście to uzasadnili rodzicom?
3. Serwis internetowy stracił bazę haseł swoich użytkowników. Kto tu ponosi odpowiedzialność za skutki: serwis, użytkownik, który powtarzał hasło, czy obaj, i czy odpowiedź zmienia się, gdy użytkownik ma trzynaście lat?

Częste pytania uczniów

Czy menedżer haseł jest bezpieczny, skoro trzyma wszystko w jednym miejscu?

Trzyma je zaszyfrowane i odblokowuje jednym hasłem głównym, którego sam dostawca nie zna. Alternatywa, czyli to samo hasło w dziesięciu serwisach, jest wyraźnie gorsza, bo tam wystarczy jeden wyciek.

Co, jeśli zapomnę hasła głównego?

W dobrze zrobionym menedżerze nie odzyskasz dostępu, bo nikt poza Tobą tego hasła nie zna. Dlatego przy pierwszym ustawieniu zapisuje się je na kartce i trzyma w domu w znanym sobie miejscu, razem z kodami zapasowymi.

Po co drugi składnik, skoro moje hasło jest długie i nikt go nie zgadnie?

Bo hasła nie zawsze się zgaduje. Czasem wycieka z serwisu albo wpisujesz je na podrobionej stronie. Drugi składnik sprawia, że sam ciąg znaków przestaje wystarczać.

Mini projekt na kolejne lekcje

Na 2 do 3 kolejne lekcje albo na kółko. Buduje na tym, co uczniowie zrobili na tej lekcji.

Instrukcja bezpiecznego logowania dla rodziny

Uczniowie w parach tworzą krótką, papierową instrukcję dla swojej rodziny: jak ułożyć hasło główne z losowych słów, jak zacząć korzystać z menedżera wbudowanego w przeglądarkę i jak włączyć drugi składnik na poczcie. Projekt buduje na tej lekcji i zajmuje dwie do trzech kolejnych lekcji albo dwa spotkania kółka. Instrukcja ma zadziałać u osoby, która nie była na lekcji.

1. Lekcja 1: para spisuje trzy zasady z tej lekcji własnymi słowami i sprawdza je nawzajem z inną parą, czy są zrozumiałe dla kogoś, kto nie zna słów menedżer i drugi składnik.
2. Lekcja 2: para przygotowuje listę 36 słów do losowania i opisuje krok po kroku, jak wylosować cztery słowa kostką, potem układa listę pytań kontrolnych: co zrobić, gdy zgubię telefon, gdzie trzymać kody zapasowe, kiedy blokować ekran.
3. Lekcja 3: para składa instrukcję na jednej kartce A4 w wersji do druku (czarny tekst na białym tle, numerowane kroki, bez informacji przekazywanych samym kolorem) i testuje ją na innej parze, która wykonuje kroki dosłownie i zaznacza miejsca niezrozumiałe.
4. W domu: uczeń przechodzi instrukcję razem z rodzicem na jednym prawdziwym koncie rodzica albo własnym i wraca z informacją, który krok wymagał poprawy.

Co powstaje na końcu: Jednostronicowa instrukcja bezpiecznego logowania, przetestowana na innej parze i w domu, oraz lista poprawek po teście. Najlepsze instrukcje można wywiesić w pracowni albo dołączyć do gazetki szkolnej.