

KOMPLET 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.

W tym pliku są wszystkie materiały do lekcji: scenariusz z kluczem do karty pracy i kryteriami oceny, prezentacja, karta pracy, materiały dla ucznia, kartka dla rodzica oraz quiz w wersji dla ucznia i z odpowiedziami.

Co znajdziecie w środku

1. Scenariusz lekcji
2. Prezentacja na tablicę
3. Karta pracy do druku
4. Materiały dla ucznia
5. Kartka dla rodzica
6. Quiz dla ucznia
7. Quiz z odpowiedziami

SCENARIUSZ LEKCJI

Menedżer haseł i logowanie dwuskładnikowe

Cel lekcji

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 sopol 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.

PREZENTACJA NA TABLICĘ

Menedżer haseł i logowanie dwuskładnikowe

Slajdów: 8. Notatka pod slajdem jest dla nauczyciela, uczniowie nie widzą jej na tablicy.

SLAJD 1

Ile masz kont, ile masz haseł

- Kont zwykle kilkanaście
- Haseł zwykle dwa lub trzy
- Ta różnica jest całym problemem

NOTATKA DLA NAUCZYCIELA

Zacznijcie od liczb zebranych od klasy. Własna liczba działa lepiej niż każda statystyka z zewnątrz.

SLAJD 2

Jak działa wyciek

- Serwis traci bazę danych logowania
- Ktoś próbuje tej pary w innych serwisach
- To samo hasło otwiera kolejne konta

NOTATKA DLA NAUCZYCIELA

Wyjaśnijcie mechanizm bez straszenia. Uczeń ma zrozumieć łańcuch, a nie się przestraszyć.

SLAJD 3

Hasło z czterech losowych słów

- Losuj słowa, nie wybieraj ich
- Długość bije wykrzykniki i cyfry
- Co najmniej 16 znaków razem

NOTATKA DLA NAUCZYCIELA

Losujcie na żywo kostką. Uczniowie zapamiętują metodę lepiej, gdy ją widzą.

SLAJD 4

Czego nie robimy z hasłem

- Nie używamy imion, dat i nazw z gier
- Nie zamieniamy liter na podobne cyfry
- Nie wklejamy hasła do stron sprawdzających

NOTATKA DLA NAUCZYCIELA

Trzeci punkt powtórzcie osobno, bo uczniowie sami chcą przetestować swoje prawdziwe hasło.

SLAJD 5

Do czego służy menedżer

- Pamięta hasła do wszystkich kont
- Ty pamiętasz jedno hasło główne
- Sam wypełnia pola logowania

NOTATKA DLA NAUCZYCIELA

Wystarczy pokazać menedżer wbudowany w przeglądarkę oraz jedno wolne narzędzie, na przykład Bitwarden.

SLAJD 6

Drugi składnik logowania

- Coś, co wiesz, i coś, co masz
- Kod z aplikacji albo klucz sprzętowy
- Samo hasło przestaje wystarczać

NOTATKA DLA NAUCZYCIELA

Pokażcie ekran logowania proszący o kod i opiszcie, co widzi ktoś, kto zna tylko hasło.

SLAJD 7

Od którego konta zacząć

- Najpierw poczta
- Potem konta z płatnościami

- Na końcu reszta serwisów

NOTATKA DLA NAUCZYCIELA

Uzasadnijcie kolejność: przez pocztę odzyskuje się dostęp do wszystkich pozostałych kont.

SLAJD 8**Trzy zasady na dziś**

- Jedno hasło główne, menedżer na resztę
- Inne hasło do każdego serwisu
- Drugi składnik najpierw na poczcie

NOTATKA DLA NAUCZYCIELA

Poproście uczniów o przepisanie tych trzech zdań do zeszytu przed dzwonkiem.

KARTA PRACY DO DRUKU

Menedżer haseł i logowanie dwuskładnikowe

Imię ucznia: Klasa: Data:

Dziś ułożysz jedno hasło, które będziesz pamiętać, i zdecydujesz, które z Twoich kont wymaga dodatkowej ochrony najbardziej. Prawdziwych haseł nie wpisujesz dziś nigdzie na szkolnym komputerze.

1

Wylosuj cztery słowa i zapisz z nich swoje hasło główne. Policz i wpisz, ile ma znaków.

Wskazówka: Rzuć kostką dwa razy na każde słowo: pierwszy rzut to cyfra dziesiątek, drugi jedności, numer od 11 do 66 wskazuje słowo na liście. Nie wybieraj słów samodzielnie. Celuj w co najmniej 16 znaków razem.

2

Uporządkuj pięć kont od najważniejszego do najmniej ważnego pod względem ochrony: poczta, dziennik elektroniczny, konto w grze, sklep internetowy, komunikator. Uzasadnij pierwsze miejsce jednym zdaniem.

Wskazówka: Zastanów się, przez które konto da się odzyskać hasła do pozostałych.

3

Wypisz trzy rzeczy, które może zrobić osoba, która usiądzie przy Twoim niezablokowanym, zalogowanym komputerze.

Wskazówka: Pomyśl o zapisanych hasłach w przeglądarce, o poczcie i o możliwości zmiany hasła na innych kontach.

4

Napisz, czym różni się kod z aplikacji od kodu przysłanego SMS i który wybierzesz.

Wskazówka: Zwróć uwagę na to, że numer telefonu można przejąć u operatora, a aplikacja działa na Twoim urządzeniu bez sieci komórkowej.

5

Zaplanuj pracę domową: wpisz nazwę jednego konta, na którym razem z rodzicem włączysz drugi składnik, i termin.

Wskazówka: Zaczynaj od konta pocztowego, bo to ono odblokowuje odzyskiwanie pozostałych.

MATERIAŁY DLA UCZNIA

Menedżer haseł i logowanie dwuskładnikowe

Czego się nauczysz

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.

Masz prawdopodobnie kilkanaście kont w różnych serwisach i dwa albo trzy hasła na wszystkie. Ta różnica jest całym problemem bezpieczeństwa Twoich kont. Z tego materiału dowiesz się, jak zbudować jedno hasło, które naprawdę zapamiętasz, oddać pamiętanie reszty programowi i dołożyć drugi składnik logowania, który ratuje konto nawet wtedy, gdy hasło wycieknie.

Dlaczego to samo hasło w kilku serwisach to jeden problem, a nie kilka

Serwisy internetowe czasem tracą swoje bazy danych logowania. Dzieje się to niezależnie od Ciebie i nie masz na to wpływu. Po takim zdarzeniu pary adres i hasło trafiają w obce ręce, a potem ktoś próbuje tej samej pary w innych popularnych serwisach: w poczcie, w sklepie, w komunikatorze, w grze. Ta metoda nie wymaga zgadywania ani łamania czegokolwiek, bo hasło jest już znane.

Jeśli używasz jednego hasła w dziesięciu miejscach, wyciek z najsłabszego, najmniej ważnego serwisu otwiera pozostałe dziewięć. Twoje bezpieczeństwo jest wtedy równe bezpieczeństwu najgorzej chronionej strony, na której się kiedykolwiek zarejestrowałeś. To dlatego wyciek z forum o grach potrafi skończyć się utratą poczty.

Odwrotnie działa zasada osobnego hasła do każdego serwisu. Wyciek zostaje wtedy zamknięty w jednym miejscu i kosztuje Cię zmianę jednego hasła, a nie odzyskiwanie całego cyfrowego życia. Problem w tym, że dziesięciu różnych, długich haseł nie zapamiętasz. I właśnie po to istnieje menedżer haseł.

SPRÓBUJ SAM

Wypisz na kartce wszystkie serwisy, w których masz konto. Przy każdym postaw znak, jeśli używasz tam tego samego hasła co gdzie indziej. Potem policz, ile kont straciłbyś naraz, gdyby wyciekło jedno z tych powtórzonych haseł. Ta liczba jest Twoim realnym zasięgiem pojedynczego wycieku.

Hasło główne z losowych słów, czyli dlaczego długość bije wykrzykniki

Popularne przekonanie mówi, że mocne hasło to takie, które ma wielką literę, cyfrę i znak specjalny. To za mało. Hasło typu Kasia2011! spełnia wszystkie te warunki i jest słabe, bo składa się z przewidywalnych elementów: imienia, roku i wykrzyknika na końcu. Zamiana litery a na cyfrę 4 albo o na zero też nie pomaga, bo ta sztuczka jest powszechnie znana i uwzględniana przy łamaniu haseł.

To, co naprawdę robi różnicę, to długość i nieprzewidywalność. Metoda czterech albo pięciu losowych słów daje jedno i drugie naraz. Losujesz słowa, na przykład kostką z ponumerowanej listy, i zapisujesz je obok siebie. Powstaje coś w rodzaju „sopel wiadro grzmot lampa”: ponad dwadzieścia znaków, żadnego związku między słowami, a przy tym łatwe do zapamiętania, bo mózg dobrze radzi sobie z dziwnymi obrazami.

Słowo losowanie jest tu kluczowe. Jeśli wybierzesz słowa sam, prawie na pewno wybierzesz je z jednego kręgu skojarzeń: imiona z rodziny, nazwy z ulubionej gry, słowa z jednego przedmiotu w szkole. Wybór człowieka jest przewidywalny, losowanie nie jest. Takie hasło ustawiasz jako hasło główne, czyli to jedno jedyne, którego naprawdę musisz się nauczyć.

SPRÓBUJ SAM

Weź kostkę do gry i listę słów ponumerowaną od 11 do 66. Rzuć dwa razy na każde słowo: pierwszy rzut daje cyfrę dziesiątek, drugi jedności. Wylosuj w ten sposób cztery słowa i zapisz je razem. Policz znaki. Jeśli wyszło mniej niż 16, dolosuj piąte słowo.

Co dokładnie robi menedżer haseł

Menedżer haseł to program, który przechowuje wszystkie Twoje hasła w zaszyfrowanej postaci i odblokowuje je jednym hasłem głównym. Szyfrowanie oznacza, że bez tego hasła zapis jest nieczytelny ciąg znaków, także dla firmy, która menedżer dostarcza. Menedżer potrafi też sam wygenerować nowe, długie i losowe hasło do każdego serwisu i sam je wpisać przy logowaniu, więc nigdy nie musisz go widzieć ani pamiętać.

To odwraca sytuację z pierwszej sekcji. Zamiast dziesięciu kont z jednym hasłem masz dziesięć kont, z których każde ma inne, mocne hasło, a Ty pamiętasz jedno. Menedżerem może być osobne narzędzie, na przykład Bitwarden, albo funkcja wbudowana w przeglądarkę. Zasada działania jest ta sama.

Jest jeden warunek, o którym łatwo zapomnieć. Menedżer jest odblokowany tak długo, jak długo Twój komputer jest odblokowany i zalogowany. Kto usiądzie przy Twoim niezablokowanym laptopie, ten ma dostęp do zapisanych haseł, do poczty i do przycisku zmiany hasła w pozostałych serwisach. Dlatego blokowanie ekranu przy odchodzeniu od komputera jest częścią tej samej ochrony, nie osobnym drobiazgiem.

Druga rzecz do zapamiętania: hasła głównego nikt Ci nie przypomni. Skoro dostawca go nie zna, nie ma go skąd odzyskać. Przy pierwszym ustawieniu zapisuje się je na kartce i trzyma w domu w znanym sobie miejscu, razem z kodami zapasowymi.

SPRÓBUJ SAM

Otwórz w przeglądarce ustawienia i znajdź miejsce z zapisanymi hasłami. Nie wpisuj tam ani nie sprawdzaj żadnego prawdziwego hasła, zwłaszcza na szkolnym komputerze. Zamiast tego wypisz trzy konkretne rzeczy, które mogłaby zrobić osoba, która usiądzie przy tym komputerze, gdy zostawisz go odblokowany na dziesięć minut.

Drugi składnik logowania, czyli co ratuje konto po wycieku

Hasło jest czymś, co wiesz. Drugi składnik to coś, co masz przy sobie. Gdy oba są wymagane, sama znajomość hasła przestaje wystarczać do zalogowania. Ktoś, kto zdobył Twoje hasło z wycieku albo z podrobionej strony logowania, zatrzyma się na prośbie o kod, którego nie ma jak zdobyć, bo urządzenie z kodem leży u Ciebie w kieszeni.

Drugi składnik występuje w kilku odmianach i nie są one równorzędne. Kod z aplikacji na telefonie zmienia się co kilkadziesiąt sekund i powstaje na Twoim urządzeniu, bez udziału sieci komórkowej. Klucz sprzętowy to małe urządzenie podłączane do komputera lub przykładane do telefonu, a jego dodatkową zaletą jest to, że potwierdza także adres strony, więc nie zadziała na podrobionej witrynie. Kod przysłany SMS jest najłabszy z tej trójki, bo numer telefonu można przejąć, podszywając się pod Ciebie u operatora.

Ważne, żeby nie mylić drugiego składnika z mocniejszym hasłem. To dwie różne warstwy. Drugi składnik nie chroni przed słabym hasłem, a mocne hasło nie chroni przed wyciekiem z serwisu. Dopiero razem dają sens: hasło zamyka drzwi, a drugi składnik sprawia, że skradziony klucz sam w sobie nic nie otwiera. Przy włączaniu drugiego składnika serwis pokazuje kody zapasowe. Zapisz je od razu na kartce, bo to Twoje wejście awaryjne, gdy zgubisz telefon.

SPRÓBUJ SAM

Wybierz jeden ze swoich serwisów i sprawdź w jego ustawieniach bezpieczeństwa, jakie drugie składniki oferuje. Wypisz je i ustaw w kolejności od najbezpieczniejszego do najłabszego, a przy każdym dopisz jedno zdanie uzasadnienia. Samego włączenia nie rób w szkole, tylko w domu z rodzicem.

Od którego konta zacząć

Nie wszystkie konta są równie ważne i nie musisz zabezpieczać wszystkich naraz. Jest jedna kolejność, która ma sens w niemal każdej sytuacji, i zaczyna się od poczty. Powód jest mechaniczny: prawie każdy serwis odzyskuje hasło, wysyłając link na adres pocztowy. Kto ma Twoją pocztę, ten może po kolei przejmować pozostałe konta, nie znając do nich ani jednego hasła.

Drugie w kolejności są konta, w których zapisana jest metoda płatności albo Twoje dane osobowe: sklepy, serwisy z zakupami w grach, bank, jeśli już go masz. Dopiero na końcu reszta, czyli fora, komunikatory i serwisy rozrywkowe, w których utrata dostępu jest kłopotem, ale nie katastrofą.

Jeśli kiedykolwiek zastanawiasz się, jak ważne jest jakieś konto, zadaj sobie jedno pytanie: co jeszcze otwiera to konto. Poczta otwiera wszystko, więc dostaje ochronę pierwszą. Konto w grze otwiera tylko tę grę, chyba że użyłeś w nim tego samego hasła co w poczcie, a wtedy właśnie sam połączyłeś oba konta w jedno ryzyko.

SPRÓBUJ SAM

Wypisz pięć swoich kont i uszereguj je od najważniejszego do najmniej ważnego pod względem ochrony. Przy pierwszym miejscu dopisz jedno zdanie, co jeszcze da się otworzyć przez to konto. Na tej liście zaznacz to jedno, na którym włączysz drugi składnik jako pierwsze.

Słowniczek

hasło główne

Jedyne hasło, które musisz pamiętać samodzielnie, bo odblokowuje menedżer przechowujący całą resztę.

menedżer haseł

Program, który przechowuje hasła w zaszyfrowanej postaci, generuje nowe i wpisuje je za Ciebie przy logowaniu.

wyciek danych

Sytuacja, w której serwis traci swoją bazę danych logowania i pary adres oraz hasło trafiają w obce ręce.

drugi składnik logowania

Dodatkowe potwierdzenie przy logowaniu oparte na czymś, co masz przy sobie, a nie na tym, co wiesz.

kod z aplikacji

Kilkucyfrowy kod zmieniający się co kilkadziesiąt sekund, generowany na Twoim urządzeniu bez udziału sieci komórkowej.

klucz sprzętowy

Małe urządzenie potwierdzające logowanie, które sprawdza także adres strony, więc nie zadziała na podrobionej witrynie.

kody zapasowe

Jednorazowe kody wydawane przy włączaniu drugiego składnika, służące do wejścia na konto po utracie telefonu.

szyfrowanie

Zamiana danych w nieczytelny ciąg znaków, który da się odczytać tylko przy pomocy właściwego hasła lub klucza.

Częste pomyłki

- Układanie hasła z bliskich sobie słów, na przykład z imion domowników albo nazw z jednej gry. Taki zestaw wygląda na losowy, ale jest wybrany, więc jest przewidywalny. Słowa trzeba losować, nie wybierać.
- Wklejanie prawdziwego hasła do stron sprawdzających jego siłę. Prawdziwego hasła nie wpisuje się nigdzie poza ekranem logowania właściwego serwisu. Jeśli chcesz coś sprawdzić, testuj hasło podobnej długości, ale zmyślane.
- Uznawanie kodu SMS za najbezpieczniejszy drugi składnik. Numer telefonu da się przejąć u operatora przez podszycie się, a kod z aplikacji i klucz sprzętowy nie zależą od numeru.
- Zapisywanie hasła głównego w pliku na komputerze, zwłaszcza szkolnym albo wspólnym. Hasło główne idzie na kartkę trzymaną w domu albo do pamięci, nigdy do wspólnego sprzętu.

Sprawdź, czy rozumiesz

1. Ktoś zdobył Twoje hasło do poczty z wycieku ze sklepu internetowego, w którym używałeś tego samego hasła. Wypisz po kolei, co może zrobić dalej, i wskaż moment, w którym włączony drugi składnik przerywa ten łańcuch.
2. Dwa hasła: pierwsze to Tr0ub4dur!, drugie to sopol wiadro grzmot lampa. Które jest trudniejsze do złamania i którą cechą to tłumaczysz, skoro tylko pierwsze ma znak specjalny?
3. Menedżer haseł trzyma wszystkie Twoje hasła w jednym miejscu, co brzmi ryzykownie. Czym ta sytuacja jest lepsza od jednego hasła użytego w dziesięciu serwisach i co musiałoby się stać, żeby była gorsza?

Wyzwanie dla chętnych

PONAD PROGRAM

Sprawdź w ustawieniach bezpieczeństwa jednego swojego serwisu (razem z rodzicem, w domu), czy oferuje klucz dostępu, czyli logowanie bez hasła potwierdzone odblokowaniem telefonu albo kluczem sprzętowym. Opisz w pięciu zdaniach, co różni klucz dostępu od hasła plus kod z aplikacji i dlaczego klucz dostępu nie zadziała na podrobionej stronie logowania.

Jak sprawdzisz, że Ci wyszło: Wyszło Ci, jeśli w opisie pada, że klucz dostępu jest przypisany do prawdziwego adresu serwisu i nie da się go przepisać ręcznie na inną stronę, oraz jeśli potrafisz powiedzieć, co się stanie z takim logowaniem po zgubieniu telefonu i po co wtedy kody zapasowe.

Zadanie do domu na trzy poziomy

Wybierz jeden poziom. Możesz zacząć od łatwego i wrócić po trudniejszy.

POZIOM: ŁATWE

Wylosuj kostką cztery słowa z listy z lekcji, zapisz je razem jako hasło główne, policz znaki i schowaj kartkę w domu w miejscu, które zapamiętasz. Jeśli wyszło mniej niż 16 znaków, dołosuj piąte słowo.

POZIOM: ŚREDNIE

Zrób zadanie łatwe, a potem razem z rodzicem włącz drugi składnik na jednym własnym koncie, najlepiej pocztowym, wybierając kod z aplikacji zamiast SMS. Zapisz, ile minut to zajęło i gdzie schowaliście kody zapasowe.

POZIOM: TRUDNE

Zrób zadanie średnie, a potem sprawdź w tym samym koncie, jakie jeszcze drugie składniki serwis oferuje, uszereguj je od najbezpieczniejszego do najslabszego z jednym zdaniem uzasadnienia przy każdym i wyjaśnij rodzicowi, dlaczego kod SMS jest na końcu tej listy.

Samoocena

Zaznacz, co już potrafisz. To tylko dla Ciebie, nikt tego nie ocenia.

- ☐ Potrafię ułożyć hasło główne z czterech wylosowanych słów i wyjaśnić, dlaczego losowanie jest lepsze od wybierania słów.
- ☐ Potrafię wytłumaczyć, po co jest menedżer haseł i dlaczego pamiętam wtedy tylko jedno hasło.
- ☐ Potrafię powiedzieć, przed czym chroni drugi składnik logowania, gdy moje hasło wycieknie z serwisu.
- ☐ Potrafię wskazać, na którym koncie włączyć drugi składnik jako pierwsze, i uzasadnić to jednym zdaniem.

KARTKA DLA RODZICA

Menedżer haseł i logowanie dwuskładnikowe

Szanowni Rodzice, dziecko miało dziś lekcję z Cyfrowej Pracowni. Poniżej w dwóch zdaniach, czego się nauczyło, i jedno pytanie, które możecie zadać przy kolacji.

Czego dziecko nauczyło się na tej lekcji

Wasze dziecko potrafi ułożyć jedno długie hasło główne z czterech wylosowanych słów i wie, że pozostałe hasła może pamiętać za nie menedżer haseł, także ten wbudowany w przeglądarkę. Wie też, że drugi składnik logowania (kod z aplikacji albo klucz sprzętowy) zatrzymuje osobę, która zna hasło, i że w pierwszej kolejności włącza się go na poczcie.

Pytanie na kolację

Gdyby wyciekło Twoje hasło ze sklepu internetowego, do których jeszcze kont ktoś mógłby się nim zalogować i co go zatrzyma, jeśli włączysz drugi składnik?

Uwaga o bezpieczeństwie

Praca domowa polega na włączeniu drugiego składnika na jednym koncie dziecka razem z Wami: zróbcie to na domowym urządzeniu, kody zapasowe zapiszcie na kartce i schowajcie w domu, a kartki z hasłem głównym dziecka nie fotografujcie ani nie przesyłajcie nikomu, bo hasła głównego nie da się odzyskać od dostawcy menedżera.

Zadanie domowe do wyboru

Dziecko wybiera jeden poziom. Każdy jest do zrobienia bez pomocy nauczyciela.

POZIOM: ŁATWE

Wylosuj kostką cztery słowa z listy z lekcji, zapisz je razem jako hasło główne, policz znaki i schowaj kartkę w domu w miejscu, które zapamiętasz. Jeśli wyszło mniej niż 16 znaków, dołosuj piąte słowo.

POZIOM: ŚREDNIE

Zrób zadanie łatwe, a potem razem z rodzicem włącz drugi składnik na jednym własnym koncie, najlepiej pocztowym, wybierając kod z aplikacji zamiast SMS. Zapisz, ile minut to zajęło i gdzie schowaliście kody zapasowe.

POZIOM: TRUDNE

Zrób zadanie średnie, a potem sprawdź w tym samym koncie, jakie jeszcze drugie składniki serwis oferuje, uszereguj je od najbezpieczniejszego do najslabszego z jednym zdaniem uzasadnienia przy każdym i wyjaśnij rodzicowi, dlaczego kod SMS jest na końcu tej listy.

QUIZ DLA UCZNIA

Menedżer haseł i logowanie dwuskładnikowe

Zaznacz jedną odpowiedź w każdym pytaniu. Wynik nigdzie się nie zapisuje.

1. Które hasło będzie najtrudniejsze do złamania?

1 Z 10, POZIOM PODSTAWOWY

- ☐ A. Ala2011!
- ☐ B. sopel wiadro grzmot lampa
- ☐ C. P@sswOrd

2. Po co w ogóle używać menedżera haseł?

2 Z 10, POZIOM PODSTAWOWY

- ☐ A. Żeby móc używać tego samego hasła szybciej
- ☐ B. Żeby hasła były krótsze i łatwiejsze do wpisania
- ☐ C. Żeby pamiętać jedno hasło główne i mieć inne hasło w każdym serwisie

3. Hasło do Twojego konta wyciekło z serwisu. Masz włączony kod z aplikacji. Co się stanie, gdy ktoś spróbuje się zalogować?

3 Z 10, POZIOM ROZSZERZONY

- ☐ A. Wejdzie bez przeszkód, bo zna hasło
- ☐ B. Zatrzyma się na prośbie o kod, którego nie ma na swoim urządzeniu
- ☐ C. Konto zostanie natychmiast skasowane
- ☐ D. Hasło zmieni się samo na nowe

4. Na którym koncie warto włączyć drugi składnik w pierwszej kolejności?

4 Z 10, POZIOM PODSTAWOWY

- ☐ A. Na koncie pocztowym
- ☐ B. Na koncie w grze, w którą grasz najczęściej
- ☐ C. Na dowolnym, kolejność nie ma znaczenia

5. Który drugi składnik jest najbardziej odporny na podszycie się pod Ciebie u operatora telefonii?

5 Z 10, POZIOM PODSTAWOWY

- ☐ A. Kod przysłany SMS
- ☐ B. Kod podyktowany przez telefon przez osobę podającą się za pracownika serwisu
- ☐ C. Klucz sprzętowy albo kod z aplikacji na Twoim urządzeniu

6. Twój kolega mówi: „Moje hasło Kacper2012 zmieniłem na K4cper2012!, teraz jest mocne”. Co mu odpowiesz?

6 Z 10, POZIOM ROZSZERZONY

- ☐ A. Ma rację, cyfra zamiast litery i wykrzyknik wystarczą
- ☐ B. Hasło jest nadal słabe, bo imię i rok są przewidywalne, a zamiana a na 4 jest powszechnie znana
- ☐ C. Wystarczy dodać jeszcze jedną cyfrę na końcu
- ☐ D. Hasło jest mocne, bo ma więcej niż 8 znaków

7. Wylosowałeś kostką słowa: mydło, rakietę, stół, burza. Twoja siostra mówi, że lepiej wziąć słowa, które coś dla Ciebie znaczą, bo łatwiej je zapamiętać. Które hasło główne jest lepsze?

7 Z 10, POZIOM ROZSZERZONY

- ☐ A. mydło rakietę stół burza, bo losowe słowa nie mają związku ze mną i nikt ich nie zgadnie
- ☐ B. Imiona czterech członków rodziny, bo są łatwe do zapamiętania
- ☐ C. Nazwy czterech postaci z mojej ulubionej gry, bo nikt nie wie, w co gram
- ☐ D. mydło rakietę, bo dwa słowa wystarczą, jeśli są losowe

8. Zapomniałeś hasła głównego do menedżera haseł. Co się stanie?

8 Z 10, POZIOM PODSTAWOWY

- ☐ A. Dostawca menedżera wyśle Ci hasło główne na pocztę
- ☐ B. Nie odzyskasz dostępu, bo dostawca nie zna Twojego hasła głównego, dlatego zapisuje się je na kartce w domu
- ☐ C. Wystarczy zrestartować komputer i hasło się wyczyści

9. Dostajesz SMS: „Twoje konto zostanie zablokowane. Zaloguj się tutaj”, z linkiem do strony, która wygląda jak Twoja poczta. Wpisujesz hasło i kod z aplikacji. Który drugi składnik zatrzymałby ten atak nawet po wpisaniu hasła na tej stronie?

9 Z 10, POZIOM ROZSZERZONY

- ☐ A. Kod SMS, bo przychodzi na Twój numer
- ☐ B. Kod z aplikacji, bo zmienia się co 30 sekund
- ☐ C. Dłuższe hasło główne
- ☐ D. Klucz sprzętowy, bo sprawdza adres strony i nie zadziała na podrobionej witrynie

10. Włączasz drugi składnik na pocztę i serwis pokazuje Ci listę dziesięciu kodów zapasowych. Co z nimi zrobić?

10 Z 10, POZIOM ROZSZERZONY

- ☐ **A.** Zignorować, bo mam przecież telefon z aplikacją
- ☐ **B.** Wysłać je sobie na tę samą pocztę, żeby zawsze były pod ręką
- ☐ **C.** Zapisać na kartce i schować w domu, bo to wejście awaryjne po utracie telefonu
- ☐ **D.** Ustawić je jako nowe hasło do poczty

QUIZ Z ODPOWIEDZIAMI

Menedżer haseł i logowanie dwuskładnikowe

Wersja dla nauczyciela. Poprawna odpowiedź jest zaznaczona, pod każdym pytaniem jest wyjaśnienie.

1. Które hasło będzie najtrudniejsze do złamania?

1 Z 10, POZIOM PODSTAWOWY

- ☐ A. Ala2011!
- ☒ B. sopel wiadro grzmot lampa
- ☐ C. P@sswOrd

Poprawna odpowiedź: B.

Cztery losowe, niepowiązane słowa dają ponad dwadzieścia znaków i brak związku między nimi, a to liczy się najbardziej. Ala2011! to imię, rok i wykrzyknik, czyli same przewidywalne elementy. P@sswOrd to znane słowo z powszechnie znaną zamianą liter na podobne znaki, która nie dokłada trudności.

Umiejętność: Budowa hasła głównego i rola menedżera

2. Po co w ogóle używać menedżera haseł?

2 Z 10, POZIOM PODSTAWOWY

- ☐ A. Żeby móc używać tego samego hasła szybciej
- ☐ B. Żeby hasła były krótsze i łatwiejsze do wpisania
- ☒ C. Żeby pamiętać jedno hasło główne i mieć inne hasło w każdym serwisie

Poprawna odpowiedź: C.

Menedżer istnieje po to, żeby każde konto miało własne, długie hasło, a Ty pamiętasz tylko jedno hasło główne. Pierwsza odpowiedź jest odwrotnością celu, bo menedżer ma właśnie skończyć z powtarzaniem hasła. Druga też jest błędna, bo menedżer generuje hasła dłuższe, nie krótsze, i sam je wpisuje, więc ich długość Ci nie przeszkadza.

Umiejętność: Budowa hasła głównego i rola menedżera

3. Hasło do Twojego konta wyciekło z serwisu. Masz włączony kod z aplikacji. Co się stanie, gdy ktoś spróbuje się zalogować?

3 Z 10, POZIOM ROZSZERZONY

- ☐ A. Wejdzie bez przeszkód, bo zna hasło
- ☒ B. Zatrzyma się na prośbie o kod, którego nie ma na swoim urządzeniu

- ☐ C. Konto zostanie natychmiast skasowane
- ☐ D. Hasło zmieni się samo na nowe

Poprawna odpowiedź: B.

Drugi składnik wymaga czegoś, co masz przy sobie, więc osoba znająca hasło zatrzymuje się na prośbie o kod. Nie wejdzie bez przeszkód, bo samo hasło już nie wystarczy. Konto nie kasuje się samo ani hasło nie zmienia się samo, serwis nie robi nic takiego bez Twojej decyzji.

Umiejętność: Drugi składnik logowania

4. Na którym koncie warto włączyć drugi składnik w pierwszej kolejności?

4 Z 10, POZIOM PODSTAWOWY

- ☒ A. Na koncie pocztowym
- ☐ B. Na koncie w grze, w którą grasz najczęściej
- ☐ C. Na dowolnym, kolejność nie ma znaczenia

Poprawna odpowiedź: A.

Przez pocztę odzyskuje się hasła do pozostałych kont, więc jej przejęcie otwiera całą resztę. Konto w grze otwiera tylko tę grę, więc jest mniej ważne. Kolejność ma znaczenie, bo poczta jest kluczem do innych kont, a inne konta nie są kluczem do poczty.

Umiejętność: Drugi składnik logowania

5. Który drugi składnik jest najbardziej odporny na podszycie się pod Ciebie u operatora telefonii?

5 Z 10, POZIOM PODSTAWOWY

- ☐ A. Kod przysłany SMS
- ☐ B. Kod podyktowany przez telefon przez osobę podającą się za pracownika serwisu
- ☒ C. Klucz sprzętowy albo kod z aplikacji na Twoim urządzeniu

Poprawna odpowiedź: C.

Klucz sprzętowy i aplikacja działają na Twoim urządzeniu i nie zależą od numeru telefonu. Kod SMS zależy od numeru, a numer można przejąć u operatora przez podszycie się. Kod podyktowany przez telefon to nie drugi składnik, tylko typowa próba wyłudzenia: prawdziwy serwis nigdy nie dzwoni po Twój kod.

Umiejętność: Drugi składnik logowania

6. Twój kolega mówi: „Moje hasło Kacper2012 zmieniłem na K4cper2012!, teraz jest mocne”. Co mu odpowiesz?

6 Z 10, POZIOM ROZSZERZONY

- ☐ A. Ma rację, cyfra zamiast litery i wykrzyknik wystarczą
- ☒ B. **Hasło jest nadal słabe, bo imię i rok są przewidywalne, a zamiana a na 4 jest powszechnie znana**
- ☐ C. Wystarczy dodać jeszcze jedną cyfrę na końcu
- ☐ D. Hasło jest mocne, bo ma więcej niż 8 znaków

Poprawna odpowiedź: B.

Podstawa hasła to nadal imię i rok, czyli elementy, które ktoś zgadnie jako pierwsze, a zamiana litery na podobną cyfrę to sztuczka uwzględniana przy łamaniu haseł. Znak specjalny i dodatkowa cyfra na końcu nie zmieniają tego, że rdzeń jest przewidywalny. Sama liczba znaków powyżej 8 nie wystarcza, bo liczy się długość razem z nieprzewidywalnością, a tu brakuje tej drugiej. Dobrym wyjściem są cztery wylosowane słowa.

Umiejętność: Budowa hasła głównego i rola menedżera

7. Wylosowałeś kostką słowa: mydło, rakietę, stół, burza. Twoja siostra mówi, że lepiej wziąć słowa, które coś dla Ciebie znaczą, bo łatwiej je zapamiętać. Które hasło główne jest lepsze?

7 Z 10, POZIOM ROZSZERZONY

- ☒ A. **mydło rakietę stół burza, bo losowe słowa nie mają związku ze mną i nikt ich nie zgadnie**
- ☐ B. Imiona czterech członków rodziny, bo są łatwe do zapamiętania
- ☐ C. Nazwy czterech postaci z mojej ulubionej gry, bo nikt nie wie, w co gram
- ☐ D. mydło rakietę, bo dwa słowa wystarczą, jeśli są losowe

Poprawna odpowiedź: A.

Wylosowane słowa są nieprzewidywalne, a mimo to łatwe do zapamiętania, bo tworzą dziwny obraz. Imiona domowników i postacie z gry to słowa wybrane z jednego kręgu skojarzeń, a taki wybór da się odgadnąć, zwłaszcza że wiele osób wie, w co grasz i jak mają na imię Twoi bliscy. Dwa słowa to za mało znaków, celem jest co najmniej 16, dlatego losuje się cztery, a przy krótkich słowach pięć.

Umiejętność: Budowa hasła głównego i rola menedżera

8. Zapomniałeś hasła głównego do menedżera haseł. Co się stanie?**8 Z 10, POZIOM PODSTAWOWY**

- ☐ A. Dostawca menedżera wyśle Ci hasło główne na pocztę
- ☒ B. **Nie odzyskasz dostępu, bo dostawca nie zna Twojego hasła głównego, dlatego zapisuje się je na kartce w domu**
- ☐ C. Wystarczy zrestartować komputer i hasło się wyczyści

Poprawna odpowiedź: B.

Hasła są zaszyfrowane hasłem głównym, którego dostawca nie zna, więc nie ma go skąd wysłać. Restart komputera niczego nie wyczyści, bo szyfrowanie nie zależy od tego, czy komputer jest włączony. Dlatego przy pierwszym ustawieniu hasła głównego zapisuje się na kartce i trzyma w domu razem z kodami zapasowymi.

Umiejętność: Budowa hasła głównego i rola menedżera

9. Dostajesz SMS: „Twoje konto zostanie zablokowane. Zaloguj się tutaj”, z linkiem do strony, która wygląda jak Twoja poczta. Wpisujesz hasło i kod z aplikacji. Który drugi składnik zatrzymałby ten atak nawet po wpisaniu hasła na tej stronie?**9 Z 10, POZIOM ROZSZERZONY**

- ☐ A. Kod SMS, bo przychodzi na Twój numer
- ☐ B. Kod z aplikacji, bo zmienia się co 30 sekund
- ☐ C. Dłuższe hasło główne
- ☒ D. **Klucz sprzętowy, bo sprawdza adres strony i nie zadziała na podrobionej witrynie**

Poprawna odpowiedź: D.

Klucz sprzętowy potwierdza logowanie tylko na prawdziwym adresie serwisu, więc na podrobionej stronie nic nie podpisze. Kod SMS i kod z aplikacji przepisujesz ręcznie, więc na podrobionej stronie oddajesz je razem z hasłem, a ktoś może użyć ich natychmiast, zanim kod wygaśnie. Dłuższe hasło nie pomaga, bo sam je wpisałeś na fałszywej stronie.

Umiejętność: Drugi składnik logowania

10. Włączasz drugi składnik na poczcie i serwis pokazuje Ci listę dziesięciu kodów zapasowych. Co z nimi zrobić?**10 Z 10, POZIOM ROZSZERZONY**

- ☐ A. Zignorować, bo mam przecież telefon z aplikacją
- ☐ B. Wysłać je sobie na tę samą pocztę, żeby zawsze były pod ręką

- ☒ **C. Zapisać na kartce i schować w domu, bo to wejście awaryjne po utracie telefonu**
- ☐ **D. Ustawić je jako nowe hasło do poczty**

Poprawna odpowiedź: C.

Kody zapasowe służą do wejścia na konto, gdy zgubisz telefon z aplikacją, więc trzeba je zapisać poza telefonem, najprościej na kartce w domu. Zignorowanie ich oznacza, że utrata telefonu odcina Cię od poczty. Wysłanie ich na tę samą pocztę nie ma sensu, bo bez telefonu nie dostaniesz się do poczty, żeby je odczytać. Kody nie są hasłem, każdy działa tylko raz i tylko jako zastępstwo drugiego składnika.

Umiejętność: Drugi składnik logowania

SKRYPT WIDEO DLA NAUCZYCIELA

Menedżer haseł i logowanie dwuskładnikowe

Nagranie powstaje na podstawie tego skryptu. Do czasu publikacji wideo możecie przeczytać skrypt przed lekcją.

0:00 DO 0:40

Ta lekcja nie kończy się wykładem o bezpieczeństwie, tylko konkretnym wynikiem. Każdy uczeń wychodzi z sali z jednym ułożonym hasłem głównym i z decyzją, na którym koncie włączy drugi składnik. To całe zamierzenie.

0:40 DO 1:40

Zaczynacie od liczb zebranych od klasy. Ile kont, ile haseł. Ta różnica robi robotę lepiej niż jakikolwiek slajd, bo jest o nich. Zapiszcie obie liczby na tablicy i wróćcie do nich na koniec lekcji.

1:40 DO 2:50

Metodę losowych słów pokazujcie na żywo, najlepiej kostkami i listą ponumerowaną od 11 do 66. Kluczowe słowo brzmi losuj, nie wybieraj. Uczeń, który wybiera samodzielnie, weźmie słowa ze swojej ulubionej gry, a to pierwsze miejsce, gdzie ktoś będzie zgadywał.

2:50 DO 3:50

Przy menedżerze haseł wystarczy pokazać zasadę, nie zakładać kont. Menedżer pamięta wszystko, uczeń pamięta jedno hasło. Jeżeli macie na sprzęcie przeglądarkę z wbudowanym menedżerem, pokażcie po prostu, gdzie leży lista zapisanych haseł.

3:50 DO 4:50

Uwaga organizacyjna, ważna. Uczniowie nie wpisują dziś prawdziwych haseł na szkolnym sprzęcie i nie logują się do własnych kont. Hasło główne zapisują na kartce, którą zabierają do domu. Powiedzcie to na głos, zanim otworzą laptopy.

4:50 DO 5:50

Drugi składnik tłumaczcie przez prosty obraz: coś, co wiesz, i coś, co masz. Jeśli uczeń zapyta o SMS, powiedzcie wprost, że jest lepszy niż nic, ale kod z aplikacji lub klucz sprzętowy chroni skuteczniej, bo numeru telefonu można się podszyciem pozbyć.

5:50 DO 6:40

Kolejność włączania ma znaczenie. Najpierw poczta, bo przez pocztę odzyskuje się resztę kont, potem konta z płatnościami, potem cała reszta. Pracę domową ustawcie tak, żeby uczeń robił to razem z rodzicem.