MATERIAŁY DLA UCZNIA

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 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 nieczytelnym ciągiem 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 najsłabszy 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 najsłabszego, 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 pierwsza. 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 zmyślone.
- 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 sopel 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 potwierdzane 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, dolosuj 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 najsłabszego 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.