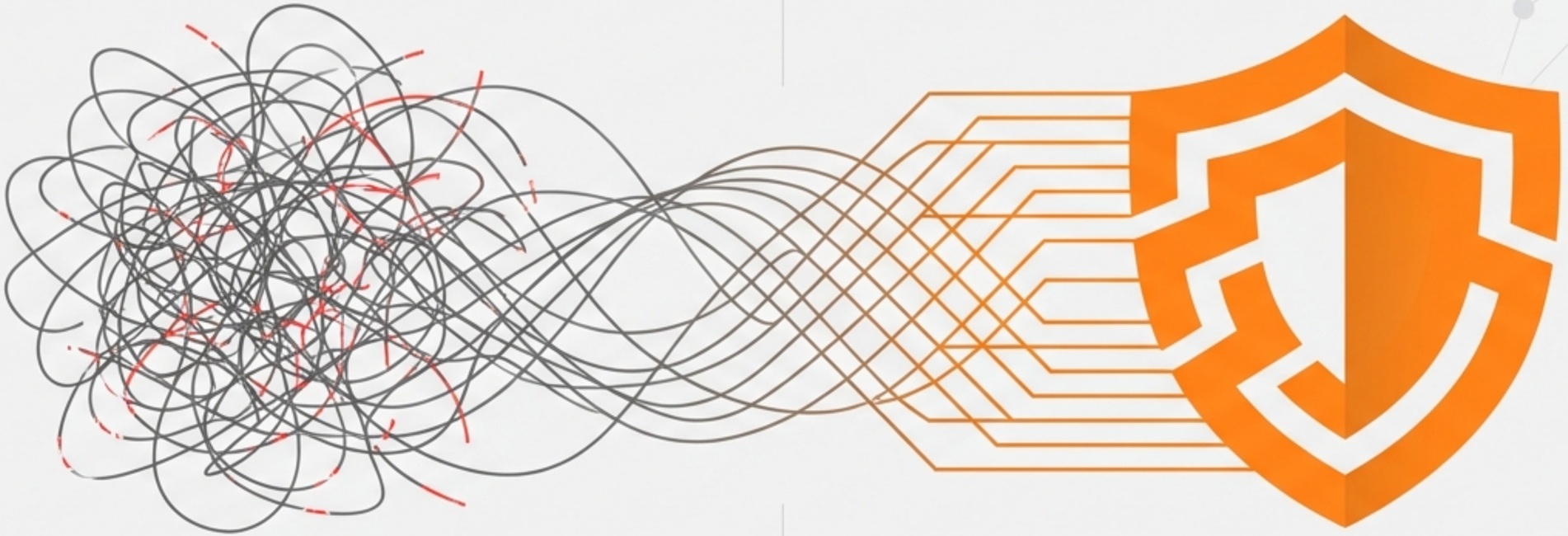


Od Słabości do Fortecy

Nowoczesna strategia ochrony Twoich finansów w sieci.

Wygoda ma swoją cenę.

Bankowość elektroniczna stała się standardem. Dostęp do naszych finansów z dowolnego miejsca i o każdej porze jest niezwykle wygodny. **Jednak ta sama technologia, która ułatwia nam życie, otworzyła nowe drzwi dla przestępców.**

„Skala zagrożeń przestępczością w bankowości elektronicznej będzie wciąż rosła wraz z nieuniknionym, dalszym rozpowszechnianiem się usług bankowości elektronicznej.” – Komisja Nadzoru Finansowego.

Stare zasady bezpieczeństwa już nie działają.

Przez lata uczono nas, że „silne” hasło to takie, które jest skomplikowane i pełne znaków specjalnych. Niestety, takie podejście często prowadzi do tworzenia haseł, które są łatwe do złamania dla komputerów, a trudne do zapamiętania dla ludzi.

„Stara szkoła”

123456
qwerty
haslo1
Pa55word!

Przewidywalne schematy, łatwe do złamania metodą słownikową.

„Rezultat”

Konta są bardziej narażone na atak, niż nam się wydaje.

Studium przypadku #1: Inżynieria społeczna.

- Pan Robert odbiera telefon od osoby **podającej się za pracownika banku**.
- W trakcie rozmowy, pod pretekstem **„zwiększenia bezpieczeństwa”**, jest proszony o podanie **loginu i fragmentów hasła**.
- Otrzymuje SMS z **kodem** do „testowego przelewu”. Tytuł i kwota (10 000 PLN) zgadzają się z tym, co mówi oszust.
- Pan Robert podaje kod, autoryzując **kradzież** własnych pieniędzy.

Zapamiętaj! Żaden bank nigdy, pod żadnym pozorem nie prosi o podawanie żadnych danych logowania do bankowości internetowej (...) telefonicznie, czy poprzez pocztę elektroniczną

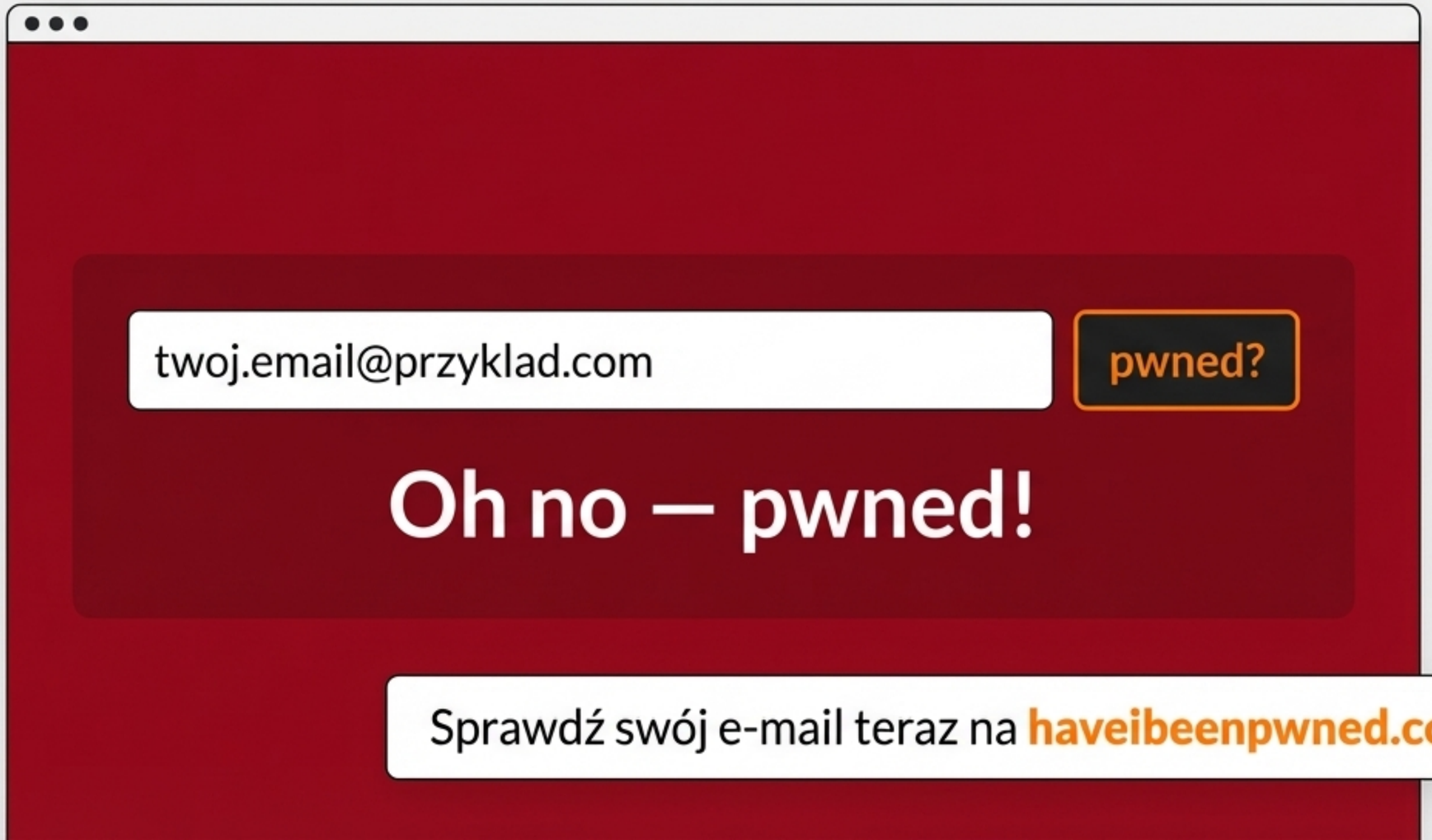
Studium przypadku #2: Złośliwe oprogramowanie.

- Pan Wojciech otrzymuje e-mail z fałszywym „ostatecznym wezwaniem do zapłaty”.
- Wiadomość napisana jest łamaną polszczyzną, ale presja czasu i obawa o firmę skłaniają go do działania.
- Otwiera zainfekowany załącznik, ignorując ostrzeżenia programu antywirusowego.
- Wirus po cichu instaluje się na jego komputerze. Przez kolejne dni, gdy Pan Wojciech wykonuje przelewy do swoich kontrahentów, oprogramowanie podmienia numery kont odbiorców.
- Rezultat: utrata wszystkich środków z konta firmowego.

Wniosek: Przestępcy atakują najsłabsze ogniwo – często niedostatecznie zabezpieczone komputery użytkowników.

Twoje dane prawdopodobnie już krążą w sieci.

Ataki nie zawsze są celowane w Ciebie osobiście. Częściej Twoje dane – e-mail i hasła – wyciekają w wyniku wyniku masowych włamań na serwisy, z których korzystasz. **Jak to sprawdzić?**



Narzędzie: "Have I Been Pwned?"

Opis: Serwis stworzony przez eksperta ds. cyberbezpieczeństwa, Troya Hunta. Gromadzi dane z setek ujawnionych publicznie wycieków.

Jak to działa: Wpisz swój adres e-mail, a serwis sprawdzi, czy znajduje się w znanych bazach skradzionych danych.

Czas na nową filozofię haseł: Długość jest ważniejsza niż złożoność.

Zapomnij o skomplikowanych, ale krótkich hasłach. Współczesne komputery potrafią je złamać w kilka sekund. Kluczem do bezpieczeństwa jest długość i losowość.

Nowa rekomendacja: “Metoda „trzech losowych słów”. Połącz ze sobą trzy (lub więcej) przypadkowe, niezwiązane ze sobą słowa.

Słabe

M@gd@1991!

Długość: 9 znaków

Czas złamania: < 1 minuta

Silne

jasnyNiebieskiGarnekPapryka

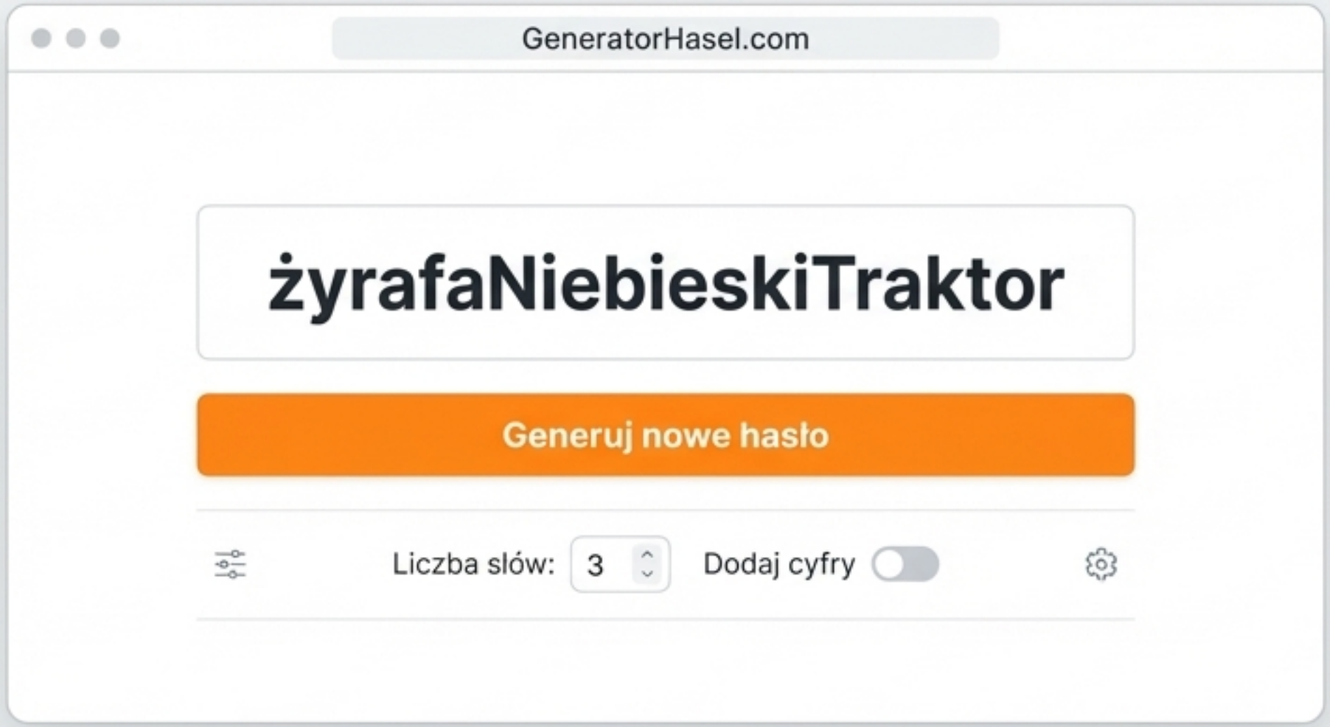
Długość: 26 znaków

Czas złamania: Tysiące lat

Wniosek: Hasło łatwe do zapamiętania dla Ciebie, ale praktycznie niemożliwe do odgadnięcia dla maszyny.

Twojenie nowe, kluczowe narzędzie: GeneratorHasel.com

Jak tworzyć naprawdę losowe i długie hasła bez wysiłku? Użyj dedykowanego narzędzia. GeneratorHasel.com tworzy silne, łatwe do zapamiętania frazy hasłowe oparte na losowych słowach, zgodnie z najlepszymi praktykami bezpieczeństwa.



Prostota: Jedno kliknięcie, by stworzyć nowe, silne hasło.

Bezpieczeństwo: Generowanie odbywa się po stronie Twojej przeglądarki, hasła nie są nigdzie zapisywane ani przesyłane.

Elastyczność: Dostosuj długość i rodzaj hasła do swoich potrzeb.

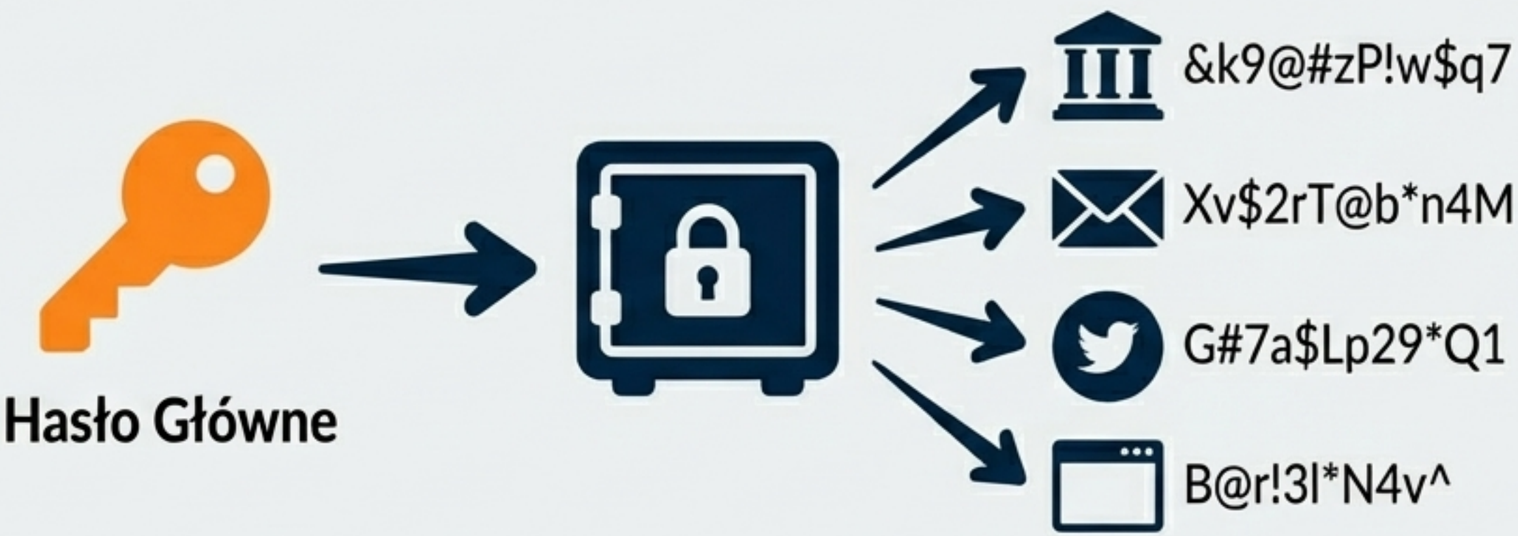
Stwórz swoje nowe hasło główne. To będzie klucz do Twojej cyfrowej fortecy.

Jedno hasło, by rządzić wszystkimi. Ale nie to samo.

Używanie tego samego hasła w wielu serwisach to jedno z największych zagrożeń. Jeśli wycieknie w jednym miejscu, wszystkie Twoje konta są zagrożone (tzw. *credential stuffing*).

Rozwiązanie: Menedżer haseł.

- To cyfrowy, zaszyfrowany sejf na wszystkie Twoje hasła.
- Chroni go jedno, silne **hasło główne** (to, które stworzyłeś w poprzednim kroku).
- Automatycznie generuje i zapamiętuje unikalne, bardzo trudne hasła dla każdej strony, z której korzystasz.



Rekomendowane narzędzia
(Open Source)

Bitwarden
(synchronizacja w chmurze)

KeePassXC
(plik przechowywany lokalnie)

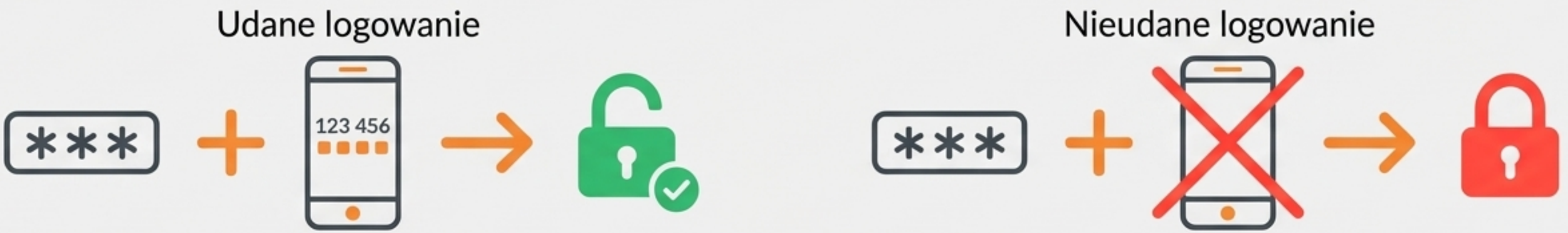
ProtonPass

Drugi zamek do Twojej fortecy: Uwierzytelnianie dwuskładnikowe (2FA).

Co, jeśli ktoś mimo wszystko zdobędzie Twoje hasło? Uwierzytelnianie dwuskładnikowe (2FA) to dodatkowa warstwa zabezpieczeń, która skutecznie go powstrzyma.

Jak to działa? Prosta zasada:

1. Czegoś, co wiesz -> Twoje hasło.
2. Czegoś, co masz -> Twój telefon generujący jednorazowy kod.



Wniosek: Nawet jeśli przestępca ukradnie Twoje hasło, bez fizycznego dostępu do Twojego telefonu nie zaloguje się na konto.

Rodzaje 2FA: Od SMS do aplikacji uwierzytelniających.

Nie każda metoda 2FA jest tak samo bezpieczna. Warto znać różnice.

Metoda (z ikoną)	Bezpieczeństwo	Wygoda	Opis
 **Kod SMS**	Średnie	Wysoka	Kod jednorazowy przychodzi w wiadomości SMS. Wygodne, ale podatne na ataki typu 'SIM swapping' (przejęcie numeru telefonu).
 **Aplikacja uwierzytelniająca**	★ **Wysokie (Rekomendowane)**	Wysoka	Aplikacja (np. Google Authenticator, Authy, Duo Mobile) generuje kody co 30 sekund. Działa offline.
 **Klucz sprzętowy (U2F)**	Bardzo wysokie	Średnia	Fizyczne urządzenie (np. YubiKey), które podłączasz do komputera. Najwyższy poziom ochrony, stosowany w krytycznych systemach.

Nasza rekomendacja: Dla większości użytkowników najlepszym balansem między bezpieczeństwem a wygodą są **aplikacje uwierzytelniające**.

Twoja nowa strategia bezpieczeństwa: Checklista

1 

Krok 1: Stwórz hasło główne.

Użyj GeneratorHasel.com, aby stworzyć długą frazę z 3-4 losowych słów. Zapamiętaj ją lub zapisz w BARDZO bezpiecznym miejscu.

2 

Krok 2: Zainstaluj menedżer haseł.

Wybierz narzędzie (np. Bitwarden, KeePassXC), zainstaluj je i zabezpiecz swoim nowym hasłem głównym.

3 

Krok 3: Wymień stare hasła.

Stopniowo, zaczynając od najważniejszych kont (e-mail, bank), użyj menedżera do wygenerowania i zapisania nowych, unikalnych haseł dla każdej usługi.

4 

Krok 4: Włącz 2FA wszędzie, gdzie to możliwe.

Skonfiguruj uwierzytelnianie dwuskładnikowe, preferując aplikację uwierzytelniającą nad SMS.

5 

Krok 5: Sprawdź historię swoich danych.

Wejdź na haveibeenpwned.com, sprawdź swoje adresy e-mail i włącz powiadomienia o przyszłych wyciekach.

A co, jeśli pieniądze znikną z konta?

Mimo najlepszych starań, możesz paść ofiarą przestępstwa. Najważniejsze to działać szybko, ale spokojnie.

1 

Natychmiast poinformuj bank.

Zadzwoń na infolinię, aby zablokować dostęp do konta lub zastrzec kartę. Wiele banków oferuje tę opcję 24/7.

2 

Złóż oficjalną reklamację w banku.

Wskaż transakcje, których nie autoryzowałeś.

3 

Zgłoś sprawę na policję. w banku.

Złóż zawiadomienie o podejrzeniu popełnienia przestępstwa. Zachowaj potwierdzenie zgłoszenia.

4 

Skorzystaj z procedury charge-back.

Jeśli transakcja została dokonana kartą (kredytową lub debetową), bank może pomóc odzyskać środki w ramach tej procedury.

(źródło: KNF)

Bezpieczeństwo to proces, a nie produkt.

Technologie i narzędzia się zmieniają, ale fundamentalne zasady pozostają te same. Twoja cyfrowa forteca nie opiera się na jednym, idealnym rozwiązaniu, ale na świadomej strategii, dobrych nawykach i regularnej weryfikacji.

Unikalność

Każde konto, własne hasło

Wielowarstwowość

Zawsze używaj 2FA

Długość

Hasła-zdania zamiast haseł-słów

Wiedza

Bądź na bieżąco z zagrożeniami i regularnie sprawdzaj stan swoich zabezpieczeń.

Wiarygodność i źródła.

Przedstawione informacje i rekomendacje zostały opracowane na podstawie materiałów i wytycznych czołowych instytucji i ekspertów w dziedzinie cyberbezpieczeństwa.

Główne źródła:

- Komisja Nadzoru Finansowego: Poradnik „Bezpieczeństwo finansowe w bankowości elektronicznej”.
- Portal Rzeczypospolitej Polskiej (Gov.pl): Baza wiedzy o cyberbezpieczeństwie.
- Projekt „Have I Been Pwned?” autorstwa Troya Hunta.