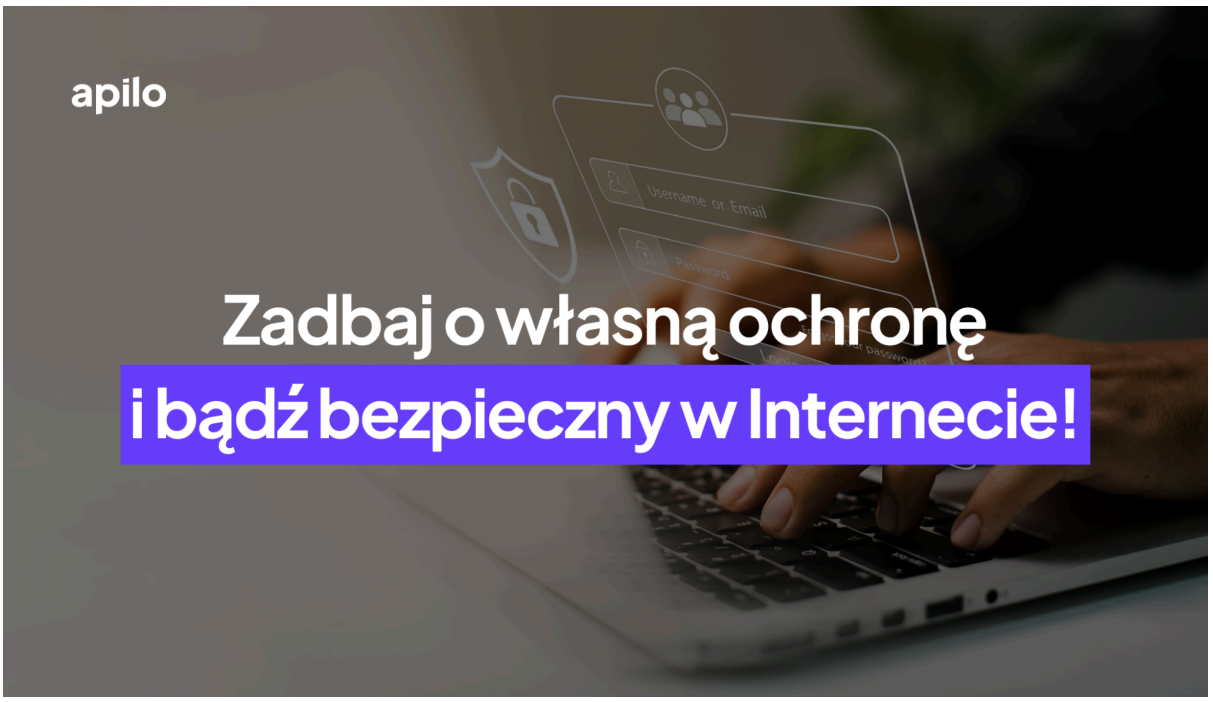

Prowadzisz biznes e-commerce? Starasz się z pewnością sprzedawać produkty z zachowaniem najwyższych standardów bezpieczeństwa. Czy tak samo jest z Twoimi danymi? Cyberprzestępcy czekają na błąd – **brak ochrony własnych kont to prosta droga do strat wizerunkowych i finansowych. Co możesz zrobić, aby Twój biznes był bezpieczny w Internecie?**

Poznaj sprawdzone sposoby na zwiększenie bezpieczeństwa kont

Z pewnością wiesz, że wrażliwe dane należy chronić za wszelką cenę, a ich utrata bądź wyciek wiąże się z szeregiem konsekwencji. Zwróć uwagę na **sprawdzone sposoby, które umożliwią Ci zwiększyć bezpieczeństwo**. Środki te dotyczą między innymi: logowania, szyfrowania danych, tworzenia odpowiednich haseł, czy… wzmożonej ostrożności w codziennych czynnościach. Poniżej znajdziesz **metody na zwiększenie bezpieczeństwa własnych kont w Internecie.**

Używaj silnych i unikalnych haseł

Pierwszym i najważniejszym punktem przy tworzeniu konta na jakiejkolwiek platformie jest **stworzenie silnego hasła**. Jest ono pierwszą linią obrony przed cyberprzestępcami, którzy czyhają na wykradnięcie danych osobowych.

Zwróć uwagę na to, że wykorzystanie haseł o słabej mocy jest jednym z najpopularniejszych powodów utraty dostępu do własnego konta.

Zwróć uwagę na kilka elementów składających się na moc szyfru. Na co należy położyć nacisk, aby zapewnić Twojemu kontu najwyższy poziom bezpieczeństwa?

- **Długość**: powinno zawierać co najmniej 12 znaków, jednak idealnym wyborem będą te, które posiadają między 14 a 16 znaków. Należy przyjąć zasadę, że im dłuższe, tym trudniejsze jest do złamania przez hakerów.
- **Różnorodność znaków**: wykorzystuj różne kombinacje, takie jak wielkie i małe litery, liczby, czy symbole. Pamiętaj, aby dane sekwencje nie powtarzały się.
- **Przeznaczenie**: pamiętaj, aby każde hasło było przeznaczone wyłącznie do tworzonego konta. Ma to zapobiec eskalacji w przypadku złamania zabezpieczeń na którymkolwiek portalu.
- **Tajemniczość**: skuteczne hasło nie powinno być oparte na podstawie łatwo dostępnych informacji. Zwróć szczególną uwagę, aby nie było słowem ze słownika – to prosta droga do złamania go metodą brute-force.

Wyciek haseł, tak jak wspominamy wyżej, **wynika najczęściej ze słabej mocy zastosowanego szyfru**. Według CERT (*przyp.*Centralny Ośrodek Reagowania na Incydenty Komputerowe), najczęściej łamanymi są m.in.: *123456, qwerty, zaq12wsx, polska, password, komputer,* czy *111111*.

Wśród haseł dostępnych z baz wycieku danych znajdziemy także schematy ich budowy – najczęściej słabe hasła bazują na dodaniu liczby, aby spełniło narzucone wymagania usługodawców.

Włącz dwuetapowe logowanie

Zakładając konto na jakiejkolwiek platformie, należy zwrócić uwagę na **bezpieczeństwo danych** – w szczególności hasła. Jeśli wymyślono je zgodnie z przyjętymi normami lub zostało wygenerowane – powinno być bardzo trudne do złamania.

Hasło, które zawiera: 12-16 znaków, wielkie i małe litery, liczby i znaki specjalne jest niemalże niemożliwe do złamania. Przy metodzie brute-force proces ten będzie trwać co najmniej kilkanaście tysięcy lat.

Warto wiedzieć, że **nie jest to jedyna metoda na odparcie ataków**, bowiem możesz zwiększyć bezpieczeństwo Twojego konta poprzez weryfikację logowania z innych urządzeń. Wiele platform umożliwia wykorzystanie dodatkowych zabezpieczeń, a jednym z nich jest **dwuetapowe logowanie**, w skrócie nazywane **2FA**.

Metoda ta działa na zasadzie weryfikacji zewnętrznej – po wprowadzeniu prawidłowych danych, system prosi o ich uwierzytelnienie. Najczęściej wykorzystuje się **wiadomości SMS**, którymi można przekazać kod, i **aplikacje będącymi generatorami kluczy autentyfikacyjnych**. Zwróć uwagę, że przekazany szyfr jest aktywny przez określony czas – w przypadku aplikacji trwa to od 10 do 30 sekund.
Metoda dwustopniowego logowania jest sprawdzonym i skutecznym sposobem na ochronę własnego konta. Przyjmijmy hipotetyczną sytuację – dochodzi do wycieku danych, w którym hakerzy uzyskali Twoje dane logowania. **W przypadku posiadania włączonej metody 2FA, będą musieli zatwierdzić działanie poprzez wykorzystanie klucza weryfikacyjnego. Ten natomiast znajduje się na Twoim urządzeniu, co znacząco utrudnia – niemal uniemożliwia – atak**. Dzięki temu masz pełną kontrolę nad działaniami Twojego konta.

Korzystaj z menedżerów haseł

Kolejną metodą na zwiększenie bezpieczeństwa i wdrożenia różnorodności haseł stosowanych na każdej platformie są **menedżery haseł**. Są to narzędzia umożliwiające zarządzaniem, uzupełnianiem i generowaniem haseł. Ich zadania są dostosowywane w zależności od aktualnych potrzeb:

- W przypadku **zapisywania haseł** – zbiera je do bezpiecznej bazy danych zabezpieczonej przed dostępem osób niepowołanych. Najczęściej chronione są biometrią, odciskiem palca, czy… hasłem.
- **Generowanie hasła** za pomocą menedżera hasła umożliwia tworzenie unikalnych szyfrów, których zadaniem jest uniemożliwienie złamania ich przez najpopularniejsze metody. Ich ciąg wynosi najczęściej 16 i więcej znaków. Są one najczęściej losowe.
- Jeśli potrzebujemy **uzupełnić hasło** – taki menedżer wprowadzi dane do pola logowania automatycznie. Co ważne, możesz w każdej chwili zmienić login i hasło, jeśli te wcześniej zapisane są nieprawidłowe bądź nieaktualne wskutek różnych wydarzeń.

Pamiętaj, że **takie programy można używać z dowolnej liczby kont**, a synchronizacja danych zapewni Ci nieprzerwany dostęp do danych logowania, gdziekolwiek jesteś.

> Hasła generowane przez menedżery wyróżniają się ciągiem znaków, które najczęściej są niemożliwe do złamania. Co więcej, jeśli dojdzie do wycieku, jego zmiana jest dosłownie chwilą – wygeneruje nowe, tak samo silne hasło.

Zainstaluj odpowiednie oprogramowanie antywirusowe

Cyberprzestępcy nigdy nie śpią, bowiem działają nieustannie, aby pozyskać nielegalnie Twoje dane. W tym celu tworzą różne programy i rozszerzenia – są to przykładowo wirusy, trojany, pluskwy. Jeśli nie zostaną wykryte – będą szkodzić systemowi i zbierać dane. Taka sytuacja może dotyczyć i Ciebie, dlatego warto zabezpieczyć system operacyjny **oprogramowaniem antywirusowym**. **Antywirus stanowi jeden z najważniejszych elementów ochrony i prewencji przed poważnymi skutkami ich działań.**

Jego zadaniem jest **wykrywanie szkodliwych programów i rozszerzeń** poprzez skanowanie komputera. Praca antywirusa opiera się na algorytmach – wyszukuje sekwencje sygnatur oznaczających odpowiednie oprogramowanie. Jeśli zostanie wychwycony – informuje użytkownika o wykryciu zainfekowanego pliku. Jego **nieustanna praca zapewnia stałą ochronę także poprzez monitorowanie zadań zachodzących w systemie.**

Bardzo ważne są **nieustanne aktualizacje oprogramowania antywirusowego**. Najczęściej z tą możliwością można spotkać się w licencjonowanych wersjach programów. Z drugiej strony są one traktowane priorytetowo, posiadając natychmiast wprowadzane zmiany. Mimo że wiążą się z opłatami, tak na cyberbezpieczeństwie nie należy oszczędzać. **Koszt antywirusa jest niczym w porównaniu do szkód, jakie mogą wywołać wirusy i inne szkodliwe programy**.

> W przypadku domowych urządzeń najczęściej wystarczy wbudowany Windows Defender, który zabezpiecza system przed szkodliwymi oprogramowaniami.

Zachowaj zdrowy rozsądek

Warto przyjąć założenie, że **Internet jest miejscem, w którym czyha na Ciebie wiele niebezpieczeństw**. Oszuści i cyberprzestępcy zwracają uwagę na ludzkie słabości wynikające z braku wiedzy, nieuwagi, czy naiwności. Nie oznacza to jednak, że jesteśmy bezradni. W tym celu **zachowaj zdrowy rozsądek** – nie ufaj we wszystko co widzisz.

Zwróć uwagę, że wielu niebezpieczeństw możesz uniknąć dzięki własnym działaniom. W jaki sposób? Przykładowo, w celu ochrony przed phishingiem sprawdź, czy przedstawione informacje lub wskazana strona są zgodne ze stanem rzeczywistym. Kieruj się jak kierowca, zasadą ograniczonego zaufania – jeśli wiadomość jest niezgodna bądź strona jest nieprawidłowa – zgłoś to administratorowi strony i odpowiednim służbom, takim jak CERT.

Phishing to rodzaj cyberprzestępstwa polegający na podszyciu się pod zaufane firmy i instytucje w celu wyłudzenia danych, takich jak: login, hasło, numery konta bankowego i karty kredytowej.

Jakie mogą być przykłady oszustw w Internecie? Cyberprzestępcy szukają nowych metod, które skutecznie umożliwią pozyskanie danych. Nie inaczej jest z niektórymi elementami. Zwróć szczególnie uwagę na:

- **Bramki płatnicze** – należy sprawdzić, czy witryna posiada zabezpieczenia związane z bezpieczeństwem transakcji i jest odpowiednio szyfrowana poprzez protokół SSL. Zweryfikować to możesz poprzez sprawdzenie paska przeglądarki – przed adresem strony powinna znajdować się zielona kłódka.
- **Protokoły HTTPS** – czy strona internetowa posiada odpowiedni poziom zabezpieczeń
- **Załączniki** –zwróć uwagę, czy w wiadomości z załącznikiem znasz nadawcę, a także czy treść wzbudza jakąkolwiek wiarygodność. Jeśli są podejrzane – nie otwieraj ich, nawet jeśli są od znajomej osoby.
- **Źródła informacji** – weryfikuj dane i nie dawaj wprowadzać się w dezinformację, której celem może być pozyskanie od Ciebie wrażliwych danych.

Bardzo ważne jest, aby regularnie dokształcać się w zakresie cyberbezpieczeństwa. Jeśli masz możliwość – odświeżaj wiedzę, dokonuj audytu bezpieczeństwa i udoskonalaj techniki zabezpieczające przed zagrożeniem cyberprzestępców.

Pamiętaj! Jeśli widzisz coś niezgodnego – nie wykonuj żadnej czynności. Jeśli nie masz pewności, czy strona jest prawidłowa – również nie wykonuj żadnej czynności. Zgłoś to odpowiednim organom.

Nieustannie aktualizuj oprogramowanie i zabezpieczenia

Stosujesz się do powyższych porad? Jesteś z pewnością dobrze zabezpieczony przed czyhającymi zagrożeniami. Zwróć szczególną uwagę, że nawet najskuteczniejszy program może być po dłuższym czasie nieaktualny. Przestaje tym samym spełniać oczekiwania. Dołóż wszelkich starań, aby **każde zabezpieczenie było zawsze aktualne gotowe do działania.**

Nawet produkty największych firm technologicznych posiadają luki. W 2024 roku odkryto niedokładne zabezpieczenie w Microsoft Outlook, która umożliwiała manipulowanie wiadomościami e-mail. Producent wydał poprawkę zabezpieczeń.

Wykorzystuj wszelkie aktualizacje i nowości od producentów oprogramowania. Znajdziesz je zawsze na stronie producenta bądź po włączeniu programu – poinformuje o dostępności nowej wersji. Brak wykonania tej czynności zwiększa ryzyko przeprowadzenia ataku na Twoje konto.

Zabezpiecz urządzenie przed dostępem niepowołanych osób

Bezpieczeństwo danych dotyczy nie tylko Internetu, bowiem niespodziewane mogą być także ataki od… pobliskich Ciebie osób. Zwróć uwagę na urządzenia – często przechowują informacje, które nie powinny trafiać do osób trzecich. **Wiele incydentów bezpieczeństwa wynika z braku odpowiednich procedur i zasad.**
Sztandarowym przykładem naruszenia danych osobowych są… wścibscy. Może to być Twój współpracownik, a także bliska osoba. **Zwracaj szczególną uwagę na to, aby przy wpisywaniu danych logowania nikt nie spoglądał na Ciebie zza ramienia**. Jeśli dostrzeżesz takie działanie – natychmiast przerwij ten proces.

> Pamiętaj, że z pozoru prozaiczne czynności, jak spoglądanie na ekran współpracownika są potencjalnym incydentem bezpieczeństwa. Zapewnij miejscu pracy odpowiednią prywatność, by nie dopuścić do takiej sytuacji.

Dopilnuj, aby **przesyłane dokumenty i przechowywane dane były odpowiednio szyfrowane.** Możesz to wykonać poprzez nadawanie klucza, który jest znany wyłącznie nadawcy i odbiorcy. Przy ustalaniu hasła nie wykorzystuj powszechnie dostępnych danych.
Żelazną zasadą, którą obowiązkowo należy stosować jest **brak możliwości współdzielenia i udostępniania służbowego sprzętu**. Dostęp do urządzeń powinien być wyłącznie dostępny dla powołanych osób – w tym celu nadaj hasło zgodne z wytycznymi. Jeśli pracujesz z domu – pamiętaj, aby wykonywać zadania według procedur. Po zakończeniu pracy schowaj sprzęt w niewidocznym dla innych domowników miejscu.

Co może się stać, gdy stracisz dostęp do konta?

Zabezpieczanie kont to obowiązek, aby nikt nieautoryzowany nie mógł się na nie zalogować. W rzeczywistości wiele osób nie uwzględnia tych zasad. Jest to rażący błąd, ponieważ dochodzi do tzw. incydentu bezpieczeństwa. Co się stanie, gdybyś stracił dostęp do konta? **Najprościej mówiąc – tracisz kontrolę nad własnym biznesem. Hakerzy uzyskali pełny dostęp do Twojego e-commerce.** To z kolei rodzi kolejne potencjalne problemy – mogą oni z poziomu administratora wprowadzić dowolną zmianę. W szczególności dotyczy to takich danych, jak:

- **login i hasło** – hakerzy zyskują bazę klientów, która zawiera każde dane logowania

- **księgowość** – poprzez tę sekcję cyberprzestępcy mogą uzyskać dowolne dane z tego zakresu, a także możliwych wyłudzeń czy wystawienie faktur niemożliwych do rozliczeń
- **adresy klientów**, które uchodzą za dane wrażliwe podlegające ochronie RODO
- **spis produktów** – każdorazowa zmiana zaburza funkcjonowanie biznesu, a brak zgodności ze stanem faktycznym może powodować błędy w księgowości

Co więcej, **najczęściej wtedy także dochodzi do przejęcia bazy klientów.** Wśród danych najczęściej znajdują się dane logowania, adresy e-mail, a w poważniejszych przypadkach – adresy, czy numery telefonu.

> W bazach wycieków najczęściej pojawiają się takie dane, jak: dane logowania, PESEL, adresy e-mail i IP, numery telefonu, a w poważniejszych przypadkach dokumenty tożsamości, czy numery kart kredytowych.

Powyższa sytuacja odbija się nie tylko na bezpieczeństwie danych, lecz także na reputację sklepu. Zwróć uwagę, że taka sytuacja jest sygnałem dla klientów, że nie dbasz o ochronę i zabezpieczenia sklepu online. Co więcej, konkurencja będzie z chęcią wykorzystywać tę sytuację do podkopywania zaufania wobec Twojej marki.
Uzyskanie nieuprawnionego dostępu do konta może dotyczyć każdego aspektu Twojej aktywności w Internecie – nie tylko w e-commerce. Nie ma sensu zwlekać z wdrożeniem zasad mających na celu wspieranie codziennego cyberbezpieczeństwa. Zrób to teraz!

Bezpieczeństwo danych zależy wyłącznie od Ciebie!

Nawet najbardziej zaawansowane narzędzia nie zastąpią człowieka, który jest najsłabszym ogniwem w cybernetycznych atakach. **Skuteczność rozwiązań w głównej mierze zależy tylko i wyłącznie od Ciebie.** Wdrożenie powyższych metod z pewnością zwiększy Twoje bezpieczeństwo. Co możesz jeszcze zrobić?
Z pewnością co jakiś czas wykonaj zmianę hasła – możesz wesprzeć się generatorem dostępnym w menedżerze. **W przypadku podejrzeń wycieku danych – bezwzględnie zmień hasło.**

> Możesz w każdej chwili sprawdzić, czy Twoje dane znajdują się w arkuszach wycieków danych. Umożliwia to portal haveibeenpwned.com.

Kolejnym ważnym krokiem jest… **rozwaga**. **Nie udostępniaj wrażliwych danych, a jeśli musisz – opatrz je odpowiednim znakiem wodnym**, który z łatwością nakieruje Cię na wypadek potencjalnego wycieku. Wtedy będziesz wiedzieć, które źródło zawiniło.
Pamiętaj, że ataki cyberprzestępców mogą być opłakane w skutkach, jednak nie jesteś na straconej pozycji. **Dbaj o swoje bezpieczeństwo i nie ryzykuj utratą dostępu do swojego konta, bowiem bierność może Cię drogo kosztować. Twoje dane są przecież najważniejsze, a co ważne – bezcenne.**