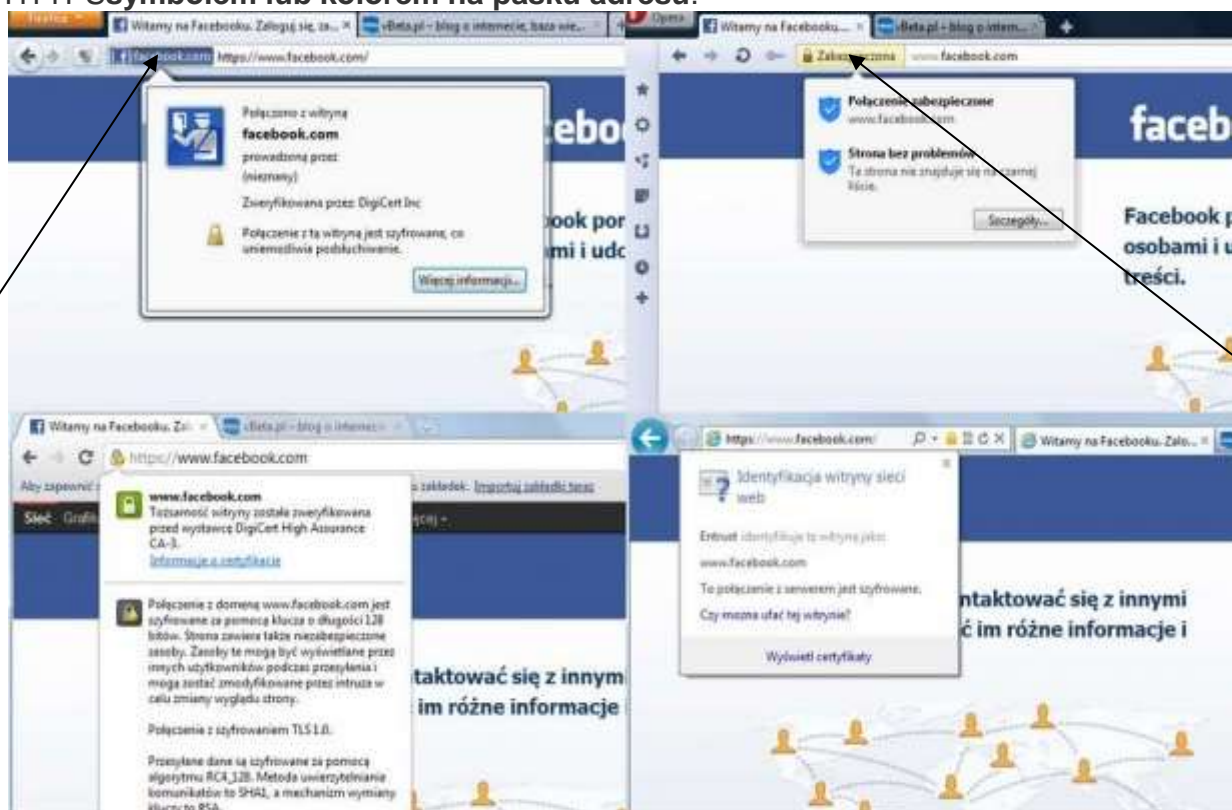


Skutki przejęcia naszego konta na Facebooku mogą być opłakane. Obrażeni znajomi, zdjęcia przeznaczone dla przyjaciół krążące gdzieś w Sieci i wykradzione dane osobowe to prawdziwy kataklizm. W jaki sposób można zwiększyć bezpieczeństwo konta na Facebooku?

## Włącz HTTPS

Korzystanie z protokołu HTTPS zamiast HTTP oznacza, że **szyfrujesz komunikację** pomiędzy Twoim komputerem a serwerem. Potencjalny szkodnik nie jest w stanie przechwycić i modyfikować tak przesyłanych informacji.

W praktyce oznacza to pewność, że dane, które otrzymujesz, są rzeczywiście danymi wysłanymi przez serwer. Przeglądarki zazwyczaj sygnalizują korzystanie z protokołu HTTPS symbolem lub kolorem na pasku adresu.



Aby Facebook łączył się z Tobą za pomocą **bezpiecznego protokołu**, trzeba aktywować odpowiednią opcję. Kliknij kolejno Konto / Ustawienia konta / Zabezpieczenia konta. Zaznacz pole Bezpieczne przeglądanie (https).

Funkcja ta może nie działać podczas korzystania z zewnętrznych aplikacji (np. gier) na Facebooku.

**Zabezpieczenia konta** ukryj

Określ swoje ustawienia dotyczące bezpieczeństwa przeglądania i logowania się

**Bezpieczne przeglądanie (https)**

Gdy tylko jest to możliwe, przeglądaj zawartość serwisu w trybie połączenia szyfrowanego (https).

**Wiadomości dotyczące logowania**

Gdy nieznanemu komputerowi lub innemu urządzeniu próbuje uzyskać dostęp do mojego konta:

Chcę otrzymać wiadomość e-mail

**Zatwierdzanie logowania** [?]

Gdy nieznanemu komputerowi lub innemu urządzeniu próbuje uzyskać dostęp do mojego konta:

Wymagaj wprowadzania kodu bezpieczeństwa wysłanego na mój numer telefonu

**Zapisz**

**Aktywność na koncie**

Zobacz ostatnią aktywność na koncie. Jeśli zauważysz nieznaną lokalizację lub urządzenie, kliknij polecenie „zakończ aktywność”.

*Uwaga: Lokalizacje i typy urządzeń są oparte na naszych szacunkach dokonywanych w oparciu o*

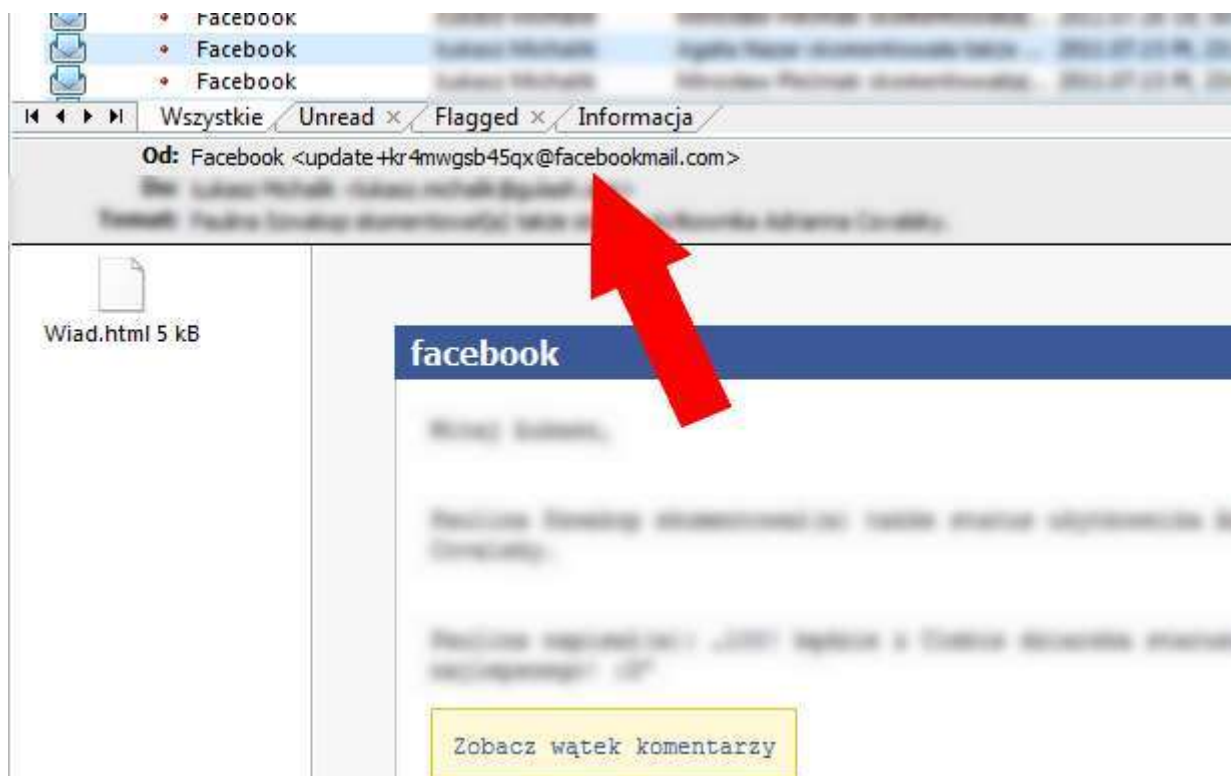
## Korzystaj z dwuetapowego logowania

Włączenie tej opcji może budzić sprzeciw osób dbających o swoją prywatność. Aby aktywować dwuetapowe logowanie, trzeba **podać numer telefonu**. Od tego momentu Twoje konto chronione jest zarówno wpisywanym przez Ciebie hasłem, jak i kodem, który dostajesz za pomocą SMS-a.

W przypadku łączenia się z Facebookiem z nowego miejsca lub komputera system zapyta o kod. Jeśli aktywujesz tę opcję, a ktoś pozna Twoje hasło, **nie skorzysta z niego** – podczas próby logowania zostanie zapytany o kod przesłany na Twoją komórkę.

## Nie pozwól na wyłudzenie informacji

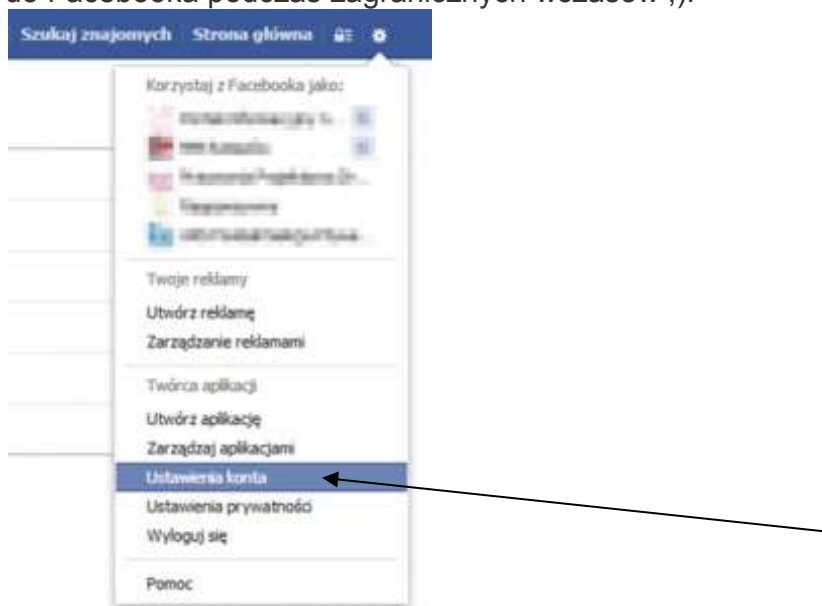
“Łamałem ludzi, nie hasła” – podtytuł książki [Kevina Mitnicka](#) powinien być przestrożą dla osób lekceważących zagrożenie ze strony **phishingu i scamu**. Nie klikaj linków, które zostały opublikowane np. na Twojej tablicy bez sprawdzenia, do czego prowadzą. Sądzisz, że ta rada to oczywistość? Gdyby tak było, przestępcy nie zajmowaliby się phishingiem ;) Ze szczególną uwagą traktuj również maile z linkami, nadesłane – rzekomo – przez Facebooka. Korespondencja pochodząca od serwisu społecznościowego zawsze wysyłana jestz **domeny facebookmail.com**.



Sprawdź uważnie domenę nadawcy maila – w tym wypadku jedna litera **robi bardzo dużą różnicę**. Maile z dowolnej innej domeny, których treść sugeruje, że zostały wysłane przez Facebooka, to próba wyłudzenia informacji.

## Włącz powiadomienia o logowaniu

Aktywowanie tej opcji sprawi, że dowiesz się, gdy ktoś zaloguje się na Twoje konto **z nietypowej lokalizacji**. Facebook określi to na podstawie poprzednich logowań. Skuteczność tego mechanizmu możesz sprawdzić, robiąc małą prowokację – zaloguj się do Facebooka podczas zagranicznych wczasów ;).



**Zabezpieczenia konta** ukryj

Określ swoje ustawienia dotyczące bezpieczeństwa przeglądania i logowania się.

**Bezpieczne przeglądanie (https)**

Gdy tylko jest to możliwe, przeglądaj zawartość serwisu w trybie połączenia szyfrowanego (https).

**Powiadomienia dotyczące logowania**

Gdy nieznanemu komputerowi lub innemu urządzeniu próbuje uzyskać dostęp do Twojego konta:

Chcę otrzymać wiadomość e-mail

Chcę otrzymać wiadomość SMS

**Zatwierdzanie logowania**

Gdy nieznanemu komputerowi lub innemu urządzeniu próbuje uzyskać dostęp do Twojego konta:

Wymagam wprowadzania kodu bezpieczeństwa wysłanego na mój numer telefonu

**Zapisz**

**Twoje zaakceptowane urządzenia:**

Nazwa urządzenia	Zapisano czas
------------------	---------------

W zależności od wybranej opcji serwis społecznościowy powiadomi Cię o **podejrzanych logowaniach** mailem lub SMS-em. Powiadomienia możesz włączyć, wybierając Konto / Ustawienia konta / Zabezpieczenia konta.

## Korzystaj z haseł jednorazowych

Facebook udostępnia funkcję znaną z systemów transakcyjnych wielu banków – **hasła jednorazowe**. Dobrym pomysłem jest korzystanie z tej możliwości, gdy logujesz się z publicznie dostępnego komputera.

Po aktywowaniu tej opcji możesz z niej skorzystać, wysyłając SMS-a o treści **otp pod numer 32665**. W odpowiedzi otrzymasz SMS-a z hasłem jednorazowym. Liczące 8 znaków hasło tymczasowe jest ważne przez 20 minut. Aby aktywować usługę, wybierz Konto / Ustawienia konta / Facebook mobile.

## Wyrzuć zbędne aplikacje

Kontroluj, komu i jakie dane na swój temat udostępniasz. Regularnie **sprawdzaj listę aplikacji**, które mają dostęp do Twojego konta, i usuwaj te, z których nie korzystasz. Akceptuj monity o dostęp tylko od aplikacji, o których wiesz, do czego służą.

**Zalecane**

**Ustawienie niestandardowe** ✓

Wzrost i ciężyść ciała (niezobowiązująco)

Poglądy religijne i polityczne

Data urodzenia

Zezwolenie na komentowanie Twoich postów

Miejsca, w których się meldujesz [?]

Informacje kontaktowe

Dostosuj ustawienia ✓

 **Aplikacje i witryny**  
Edytuj ustawienia dotyczące korzystania z aplikacji, gier i witryn internetowych.

 **Listy zablokowanych**  
Edytuj listy zablokowanych osób i aplikacji

 **Kontrola nad udostępnianiem**  
Dowiedz się więcej o udostępnianiu na Facebooku.

Aby sprawdzić aplikacje, kliknij kolejno Menu / Ustawienia prywatności a następnie Edytuj ustawienia (pod napisem Aplikacje i witryny). Pojawi się **lista aplikacji** – możesz wskazać, których chcesz się pozbyć.

Część opcji Facebooka stawia użytkownika przed dylematem znanym z rzeczywistego świata: **wygoda czy bezpieczeństwo**. Co jest dla Ciebie ważniejsze?