Jak zabezpieczyć swoje dane w internecie?

Otrzymujesz na swoją skrzynkę mailową informację, że ktoś próbował przejąć twoje konto na Facebooku. Na szczęście próba ataku hakerskiego została przerwana, jednak konieczne jest usunięcie poprzedniego hasła. By odzyskać dostęp do konta, wystarczyło kliknąć w link i postępować zgodnie z instrukcjami. Ale pobrany plik to nie generator nowego hasła, lecz wirus, który może np. usunąć wszystkie dane z komputera.

Inna historia, kobieta odbiera telefon od swojej siostry z pytaniem: „Po co ci te pieniądze?”. Siostra wyjaśniła zaskoczonej dziewczynie, że przecież pisała do niej na Facebooku, że potrzebuje pilnie kilku tysięcy złotych i poprosiła o przelew. Co się wydarzyło? Ktoś włamał się na jej konto społecznościowe i wysyłał do znajomych prośby przelanie pieniędzy. Haker miał ułatwione zadanie: dziewczyna używała tego samego hasła do kilkunastu innych kont w internecie.

Jeszcze inna prawdziwa, i to bardzo częsta historia: dostajesz maila, że twoje konto w banku zostało zablokowane. Konieczne jest kliknięcie w link, który przenosi na stronę wyglądającą identycznie jak tak twojego banku. Po wpisaniu dotychczasowego loginu i hasła masz otrzymać na maila nowe hasło. Wiadomość jednak nigdy nie nadejdzie, a po kilku chwilach pieniądze znikną z Twojego konta bankowego.

W internecie można znaleźć całe morze podobnych historii. Jeden błąd może spowodować utratę pieniędzy i cennych danych.

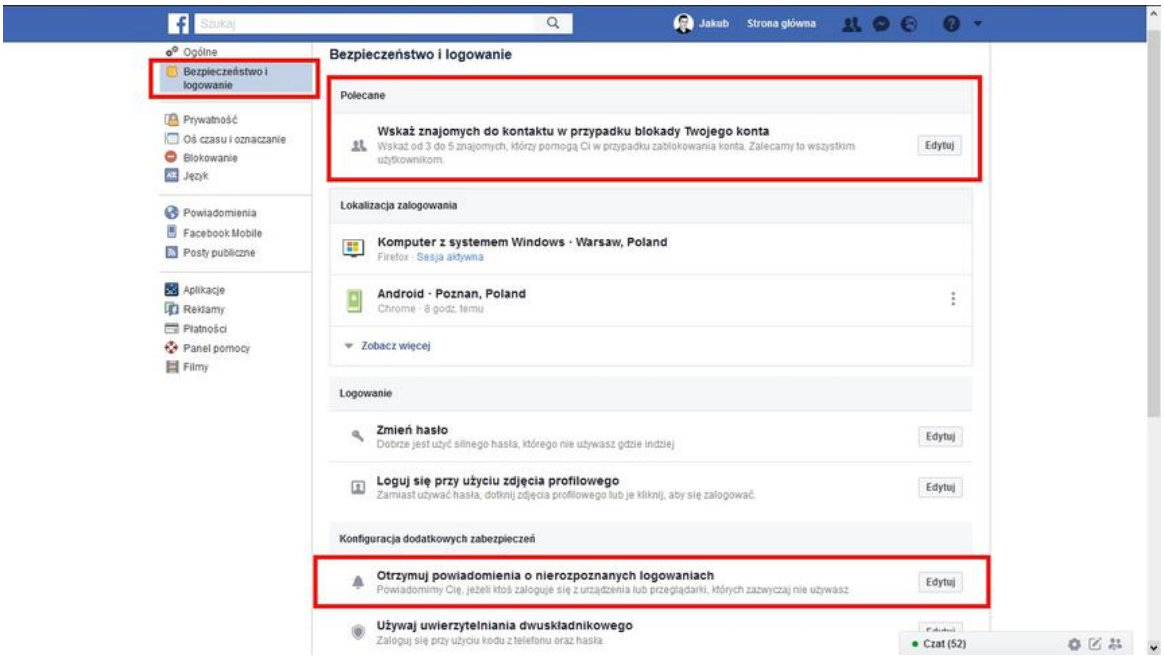
Gigabajty danych

W ciągu jednej sekundy internauci z całego świata pobierają 80 aplikacji, piszą ponad 10 tys. tweetów, przeprowadzą 1 885 rozmów na Skype, 51 tys. razy szukają czegoś w Google i rozpoczynają oglądanie ponad 108 tys. filmów na YouTube. Każdy z nas wysyła do sieci dane o swojej lokalizacji, zainteresowaniach, preferencjach zakupowych itd. Pozornie nic nieznaczący „like” zawsze jest zapisywany na serwerze.

Jak się okazało, Facebook niedostatecznie chroni dane swoich użytkowników. Wyciek danych pozwolił sprofilować miliony osób przez firmę Cambridge Analytics i w ten sposób wpływać na wyniki wyborów m. in. w Stanach Zjednoczonych. Ta sprawa pokazała, jak dużym problemem jest zachowanie prywatności w sieci. Oto kilka sposobów na zabezpieczenie swoich internetowych danych.

Prywatność na Facebooku

Jak zarządzać prywatnością na Facebooku? Przejdź do menu (na komputerach – trójkąt obok znaku zapytania, na urządzeniach mobilnych – trzy poziome kreski) wybierz „Ustawienia konta”. To centrum dowodzenia twoim facebookowym kontem. W drugiej zakładce nazwanej „Bezpieczeństwo i logowanie” możesz wskazać znajomych, których Facebook poinformuje, gdy konto zostanie zablokowane. Jeśli chcesz mieć kontrolę nad tym, kto loguje się na twoje konto, wybierz opcję powiadomienia o nierozpoznanych logowaniach – otrzymasz wówczas wiadomość, gdy ktokolwiek spróbuje na Facebooku wpisać twoje hasło.



Data publikacji: 30.03.2018, 10:30 Ostatnia aktualizacja: 30.03.2018, 12:56
Jakub Kowalik

Statystyczny użytkownik internetu każdego dnia generuje około 12 gigabajtów danych. Każde kliknięcie w witrynę, wyszukanie informacji w Google, wciśnięcie „Lubię to” czy wysłanie maila to dane, na podstawie których można dokładnie opisać każdego człowieka. Generowane przez nas informacje są łakomym kąskiem dla firm i hakerów, dlatego też warto zadbać zabezpieczenie swojej prywatności w internecie.

Otrzymujesz na swoją skrzynkę mailową informację, że ktoś próbował przejąć twoje konto na Facebooku. Na szczęście próba ataku hakerskiego została przerwana, jednak konieczne jest usunięcie poprzedniego hasła. By odzyskać dostęp do konta, wystarczyło kliknąć w link i postępować zgodnie z instrukcjami. Ale pobrany plik to nie generator nowego hasła, lecz wirus, który może np. usunąć wszystkie dane z komputera.

Inna historia, kobieta odbiera telefon od swojej siostry z pytaniem: „Po co ci te pieniądze?”. Siostra wyjaśniła zaskoczonej dziewczynie, że przecież pisała do niej na Facebooku, że potrzebuje pilnie kilku tysięcy złotych i poprosiła o przelew. Co się wydarzyło? Ktoś włamał się na jej konto społecznościowe i wysyłał do znajomych prośby przelanie pieniędzy. Haker miał ułatwione zadanie: dziewczyna używała tego samego hasła do kilkunastu innych kont w internecie.

Jeszcze inna prawdziwa, i to bardzo częsta historia: dostajesz maila, że twoje konto w banku zostało zablokowane. Konieczne jest kliknięcie w link, który przenosi na stronę wyglądającą identycznie jak tak twojego banku. Po wpisaniu dotychczasowego loginu i hasła masz otrzymać na maila nowe hasło. Wiadomość jednak nigdy nie nadejdzie, a po kilku chwilach pieniądze znikną z Twojego konta bankowego.

W internecie można znaleźć całe morze podobnych historii. Jeden błąd może spowodować utratę pieniędzy i cennych danych.

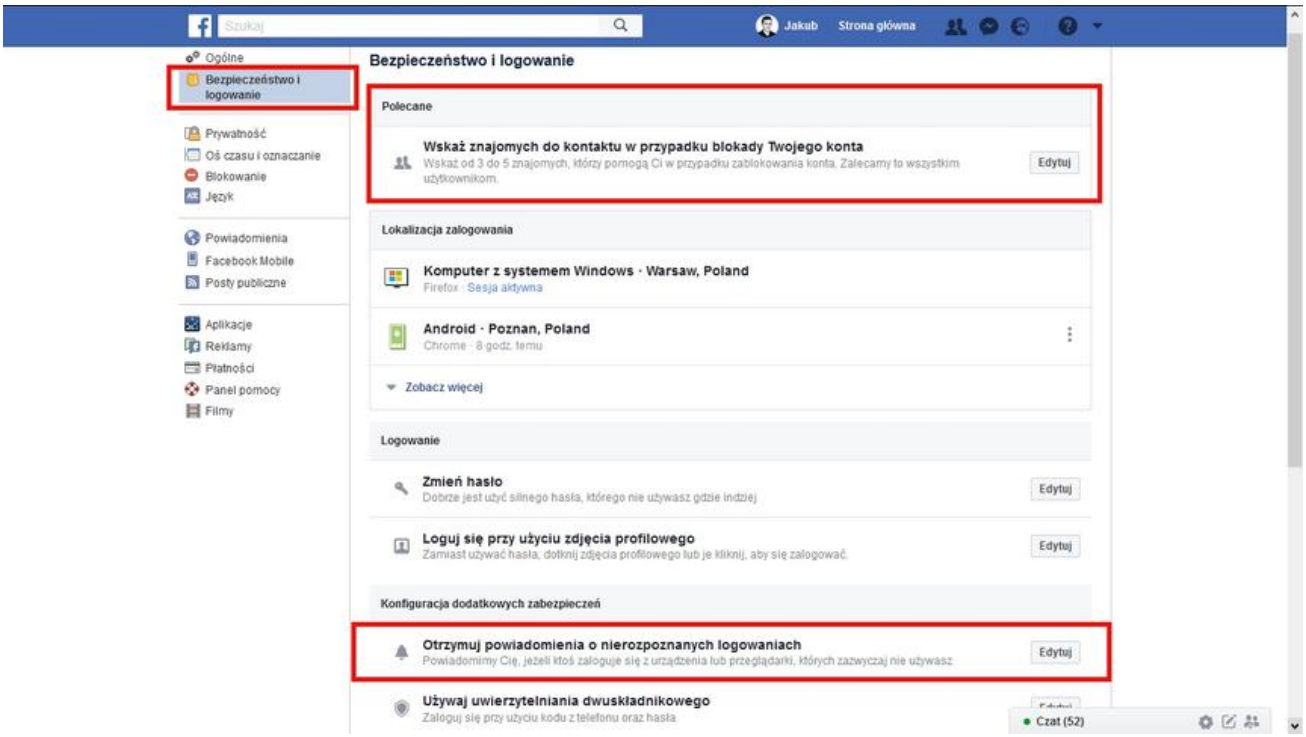
Gigabajty danych

W ciągu jednej sekundy internauci z całego świata pobierają 80 aplikacji, piszą ponad 10 tys. tweetów, przeprowadzą 1 885 rozmów na Skype, 51 tys. razy szukają czegoś w Google i rozpoczynają oglądanie ponad 108 tys. filmów na YouTube. Każdy z nas wysyła do sieci dane o swojej lokalizacji, zainteresowaniach, preferencjach zakupowych itd. Pozornie nic nieznaczący „like” zawsze jest zapisywany na serwerze.

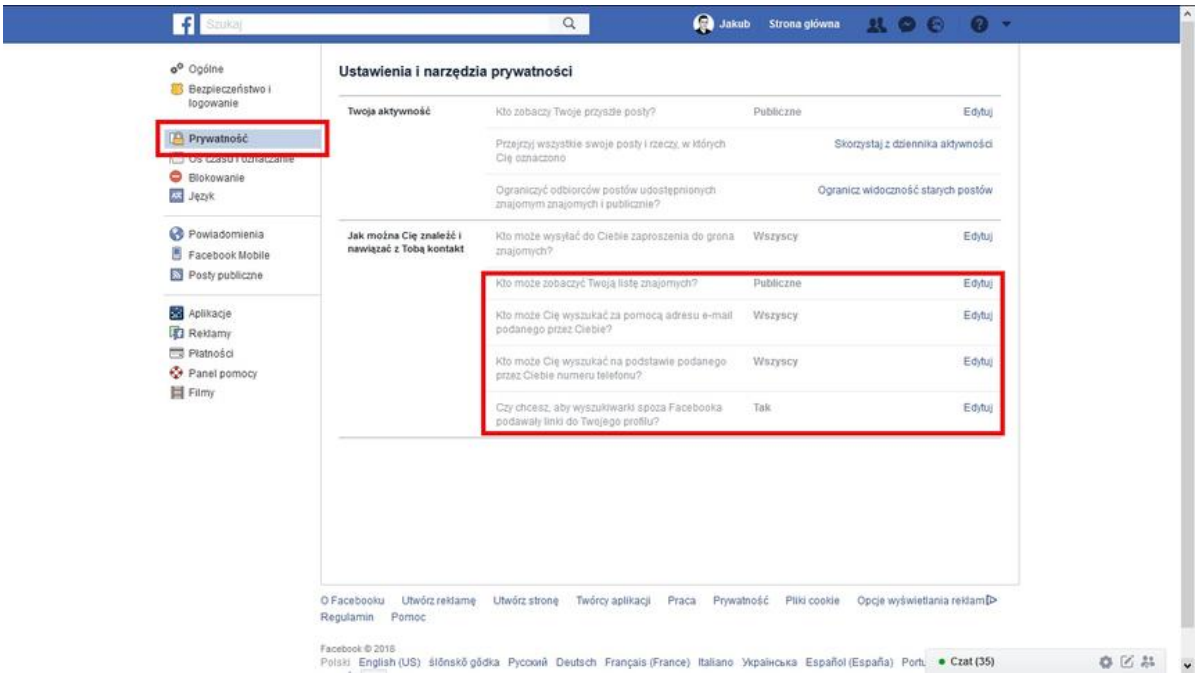
Jak się okazało, Facebook niedostatecznie chroni dane swoich użytkowników. Wyciek danych pozwolił sprofilować miliony osób przez firmę Cambridge Analytics i w ten sposób wpływać na wyniki wyborów m. in. w Stanach Zjednoczonych. Ta sprawa pokazała, jak dużym problemem jest zachowanie prywatności w sieci. Oto kilka sposobów na zabezpieczenie swoich internetowych danych.

Prywatność na Facebooku

Jak zarządzać prywatnością na Facebooku? Przejdź do menu (na komputerach – trójkąt obok znaku zapytania, na urządzeniach mobilnych – trzy poziome kreski) wybierz „Ustawienia konta”. To centrum dowodzenia twoim facebookowym kontem. W drugiej zakładce nazwanej „Bezpieczeństwo i logowanie” możesz wskazać znajomych, których Facebook poinformuje, gdy konto zostanie zablokowane. Jeśli chcesz mieć kontrolę nad tym, kto loguje się na twoje konto, wybierz opcję powiadomienia o nierozpoznanych logowaniach – otrzymasz wówczas wiadomość, gdy ktokolwiek spróbuje na Facebooku wpisać twoje hasło.



Z kolei po przejściu do zakładki „Prywatność” znajdziesz ustawienia związane z aktywnością i nawiązywaniem kontaktów. Warto zmienić tam dostępność do listy znajomych (inni użytkownicy i aplikacje nie dowiedzą się, ko jest twoim znajomym), możliwość wyszukiwania poprzez adres e-mail czy numer telefonu (twoje konto będzie niewidoczne), a także zablokować podawanie linków do konta przez wyszukiwarki zewnętrzne (innymi słowy – twoje konto nie zostanie wyszukane w Google).



Pozyskiwanie danych przez aplikacje

Dla wielu użytkowników zaskakujące jest wejście w zakładkę „Aplikacje”. Może tam znajdować się od kilkudziesięciu do nawet kilkuset aplikacji, które pozyskują informacje. Wystarczy kliknąć którąkolwiek z nich, by przekonać się, że pozwoliliśmy im na pobieranie danych o profilu, listy znajomych czy zdjęć. Nawet na potrzeby jednorazowego rozwiązania prostego quizu konieczne jest nadanie szerokich uprawnień.

Co więcej, pobieranie na smartfona dowolnych aplikacji wiąże się najczęściej z przyznawaniem od kilku do nawet kilkudziesięciu uprawnień. Jeśli przed zainstalowaniem poprosi ona o dostęp do właściwie całej zawartości telefonu i powiązanych kont, warto zastanowić się, jak nasze dane zostaną wykorzystane. A także przemyśleć, czy taka aplikacja faktycznie jest nam potrzebna.

Uwierzytelnianie dwuskładnikowe

Warto poświęcić kilka chwil i pogrzebać w ustawieniach posiadanych przez nas kont i zainstalowanych aplikacji, by ograniczyć pozyskiwanie udostępnianych przez nas danych. Jednak nawet najlepsze ukrycie informacji nie zapobiegnie atakowi hakerskiego. Według statystyk każdego dnia w Polsce dochodzi do około 15 tys. ataków, więc prawdopodobieństwo próby przejęcia konta jest bardzo wysokie. Hakerzy przejmują kontrolę nad kontem, zmieniają hasła i żądają „okupu” za odzyskanie dostępu.

Pierwszą linią obrony przed potencjalnym atakiem jest utworzenie silnego hasła złożonego z kombinacji wielkich i małych liter oraz znaków interpunkcyjnych i tzw. znaków specjalnych (np. @, $, # itd.). Eksperci zalecają, by jedno unikalne hasło było przypisane wyłącznie do jednego konta.

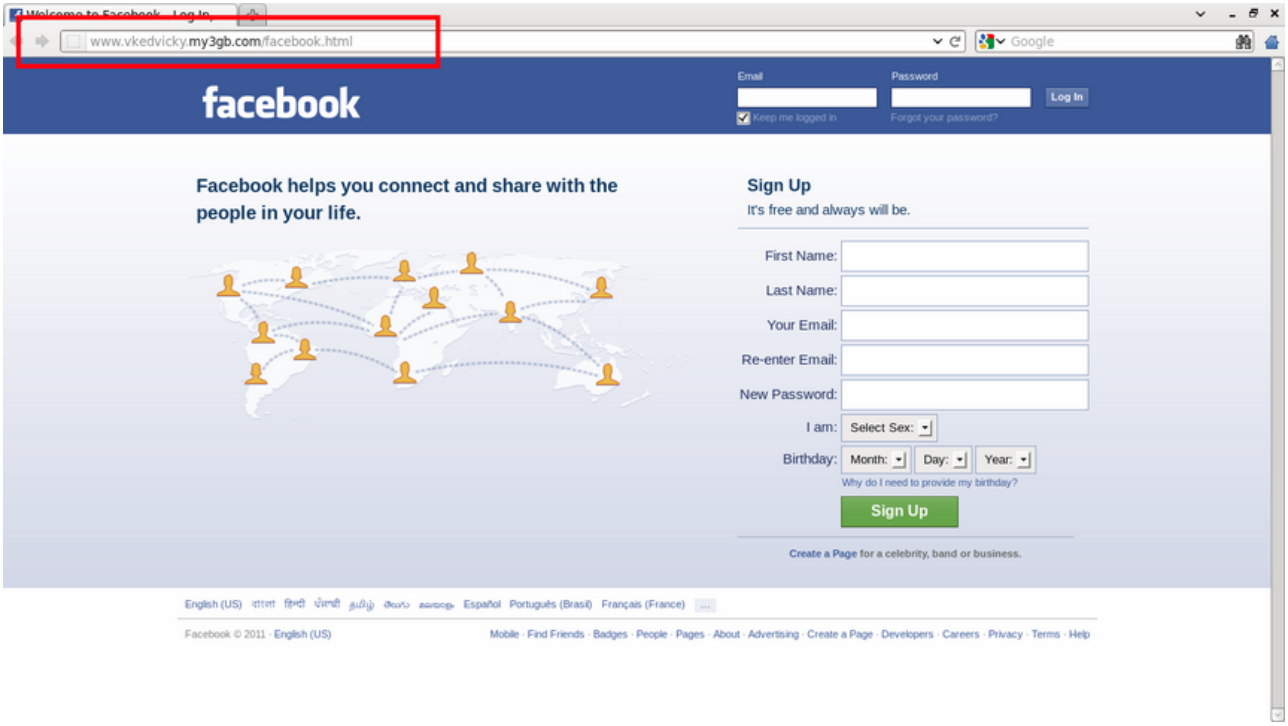
Nie ma jednak hasła, którego nie da złamać. Warto więc dodatkowo zabezpieczyć się, wprowadzając uwierzytelnianie dwuskładnikowe. Po wstukaniu standardowego hasła, system wysyła smsem lub mailem unikalny kod, którego wpisanie jest konieczne, by zalogować się na konto. Uwierzytelnianie dwuskładnikowe maksymalnie zabezpiecza konto przy minimalnym wysiłku. Można je włączyć w większości mediów społecznościowych czy na koncie Google.

Warto także dodać, że logowanie dwuskładnikowe jest jednorazowe dla każdego nowego urządzenia, z którego próbujemy dostać się na nasze konto. Kiedy na naszym laptopie czy smartfonie pomyślnie przejdziemy proces weryfikacji, następnym razem zalogujemy się już normalnie. Natomiast jeśli ktoś spróbuje wejść na któreś z naszych kont z innego urządzenia, to mimo wpisania naszego hasła, będzie musiał podać także dodatkowy kod.

Uwaga przede wszystkim

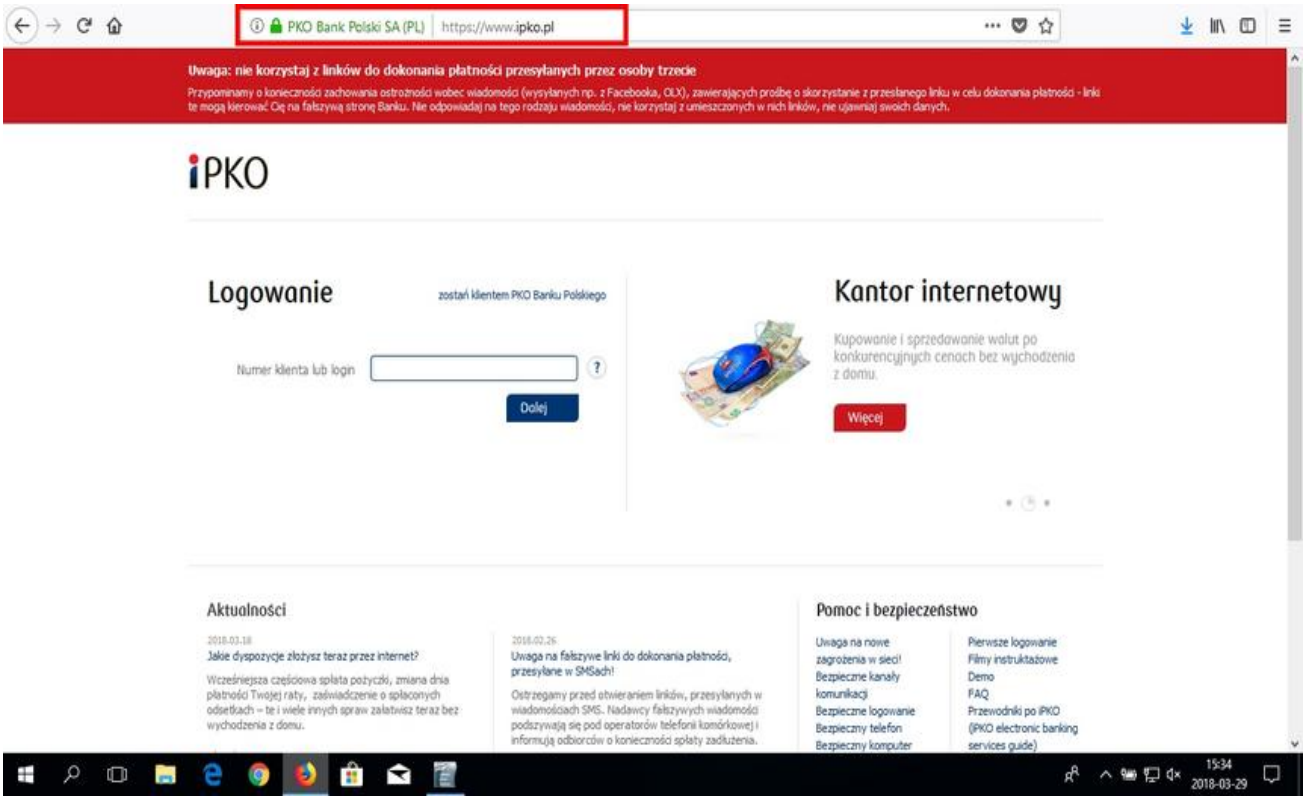
Na nic zdadzą się jednak wszelkie zabezpieczenia, jeśli będziemy klikać we wszystko, co popadnie. Choć internet przyzwyczaił nas do leniwego przeglądania stron internetowych, trzeba zwracać uwagę na drobne, pozornie nieważne detale. To może uchronić nas przed wyciekiem czy utratą danych.

Tak wygląda strona fałszywa (zwróć uwagę na pasek adresu):

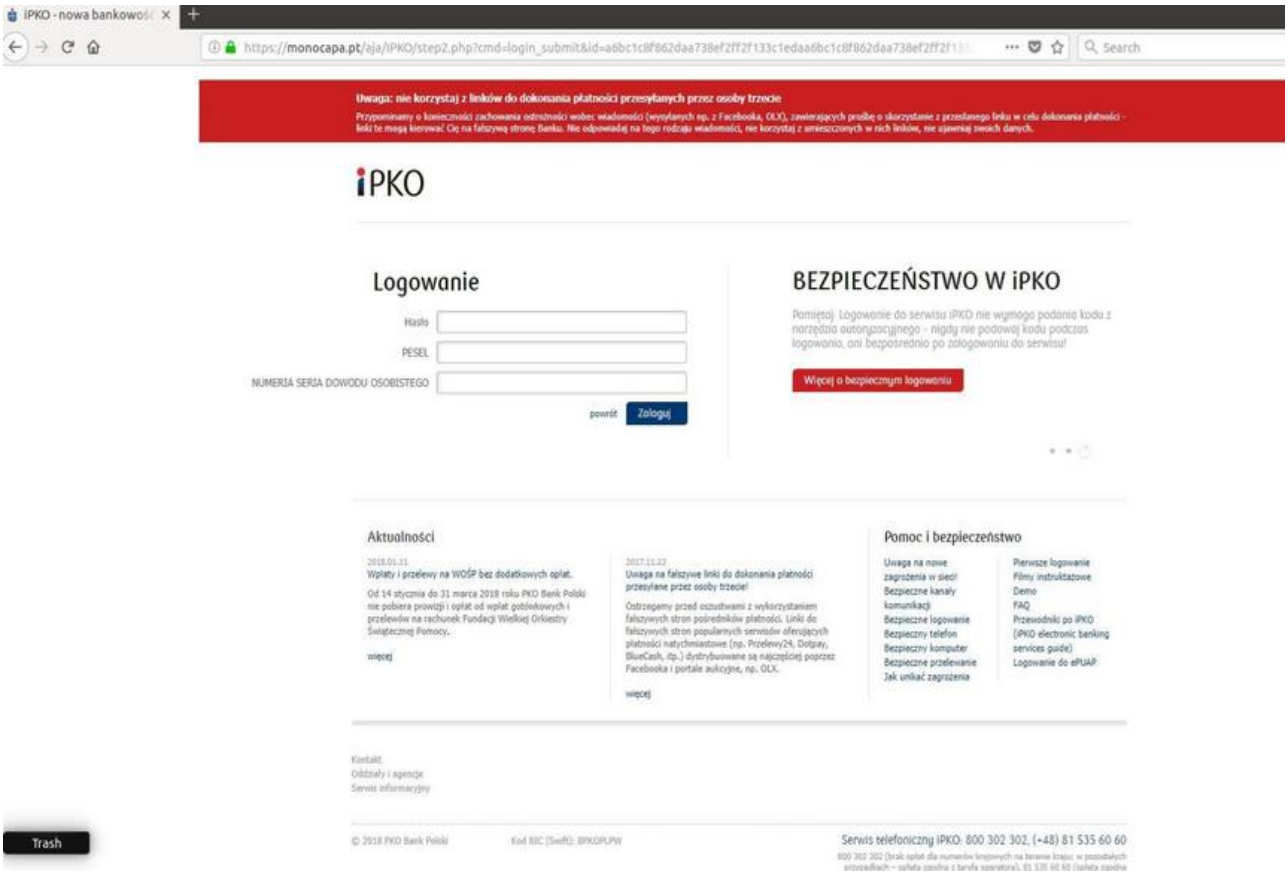


Podstawową sprawą jest zwrócenie uwagi na rodzaj połączenia. Bezpiecznie możemy się czuć, gdy na początku adresu strony znajduje się fraza: „https” (symbolizowana także zieloną kłódką). Taki przedrostek świadczy o bezpiecznym połączeniu szyfrowanym. Jeśli więc np. wejdziemy na stronę naszego banku, a adres strony nie zaczyna się od „https”, w naszej głowie powinna zapalić się lampka bezpieczeństwa.

To prawdziwa strona logowania do banku:



To fałszywa strona, wyłudzająca dane:



Ochrona konta bankowego

Szczególną ostrożność należy zachować podczas logowania się do banku. W internecie istnieje całe mnóstwo stron internetowych, które wyglądają niemal identycznie jak strona logowania na internetowe konto bankowe. Zanim jednak wpiszesz login i hasło, upewnij się, że na pasku adresu widnieje właściwa nazwa banku, a nie długi, niezrozumiały i obcy tekst.

Każdy bank wyraźnie zaznacza, że nigdy nie wymaga podawania numeru klienta, hasła ani innych danych prywatnych. Często jednak hakerzy, bazując na niewiedzy i nieuwadze, wysyłają fałszywe informacje o zablokowaniu dostępu do konta i konieczności wygenerowania nowego hasła. Pieniądze można utracić także w inny sposób. Oszuści podszywają się pod znane organizacje i wysyłają fałszywe faktury lub wymagają wpłacenia określonej sumy za korzystanie z serwisu. Częstokroć do takiej informacji dołączana jest groźba, że jeśli płatność nie zostanie uregulowana, sprawa trafi do sądu. W takim wypadku warto najpierw wyszukać w sieci informacji, czy ktoś nie ma podobnego problemu.

Pozostałe zasady bezpiecznego korzystania, o których warto pamiętać:

- Przed kliknięciem w link warto sprawdzić, z jakiego źródła pochodzi. Wystarczy najechać (nie klikać!) kursorem na link, a na dole okna przeglądarki pokaże się adres strony internetowej, do której zostaniemy przekierowani.
- Jeśli nie ma takiej potrzeby, nie powinno się podawać danych z dowodu osobistego czy karty kredytowej. Dane te mogą zostać w bezprawny sposób wykorzystane, np. do wzięcia kredytu.
- Nie należy otwierać maili z nieznanych źródeł. Jeśli jednak mail zostanie otwarty, nie wolno klikać linków czy pobierać załączników na komputer, gdyż można w ten sposób zawirusować sprzęt.
- Trzeba unikać klikania w reklamy krzyczące, że jesteśmy miliardowym użytkownikiem i czeka na nas nagroda. Podawane tam dane w najlepszym razie zostaną użyte przez reklamodawców, którzy codziennie będą dzwonić z najnowszymi ofertami. W najgorszym stracimy wszystkie dane i pieniądze z konta.
- Przed rozpoczęciem pobierania jakiegokolwiek pliku trzeba upewnić się, z jakiego źródła pochodzi. Fałszywe są najczęściej duże, kolorowe i rzucające się w oczy napisy "POBIERZ".

Jednak przede wszystkim nie należy się spieszyć, szczególnie, jeśli mamy do wykonania coś ważnego. Na pośpiechu i nieuwadze w sieci można znacznie więcej stracić, niż zyskać.

Autor tekstu: Jakub Kowalik

źródło: http://www.newsweek.pl