



Jak chronić swoje konto i prywatność na Facebooku?

2026-10-13

W drugim artykule z cyklu „Cyfrowa Tarcza Seniora” podpowiadamy, jak bezpiecznie korzystać z Facebooka. Dzięki niemu łatwiej być w kontakcie z bliskimi, odnaleźć dawnych znajomych czy dowiedzieć się o wydarzeniach w okolicy. Korzystając z Facebooka, zostawiamy jednak wiele informacji o sobie: zdjęcia, wiadomości, datę urodzenia, miejsce zamieszkania, a czasem także numer telefonu. Warto wiedzieć, jak chronić je przed oszustami.

Fot. Canva Photos

Jeżeli konto trafi w ręce oszusta, może on nie tylko poznać prywatne informacje, ale również podszywać się pod właściciela profilu i wyłudzać pieniądze od jego bliskich. Warto więc poświęcić kilka minut na sprawdzenie ustawień Facebooka.

I. Sprawdź, kto widzi Twoje posty

Podczas publikowania posta, zdjęcia lub filmu możemy wybrać jego odbiorców. Najczęściej dostępne są między innymi opcje:

- **Publiczne** – treść może zobaczyć każdy, także osoba, która nie należy do naszych znajomych;
- **Znajomi** – post zobaczą osoby znajdujące się na naszej liście znajomych;
- **Tylko ja** – treść będzie widoczna wyłącznie dla właściciela konta;
- **Wybrani znajomi** – post można pokazać tylko wskazanym osobom.

Przed opublikowaniem treści warto spojrzeć na oznaczenie widoczne pod naszym imieniem i nazwiskiem. Symbol kuli ziemskiej oznacza zwykle post publiczny, natomiast ikona przedstawiająca osoby – post przeznaczony dla znajomych.

Widoczność można zmienić także po opublikowaniu wpisu. Trzeba otworzyć menu posta, wybrać opcję edycji odbiorców i wskazać właściwą grupę. Facebook umożliwia również ograniczenie widoczności starszych publikacji.

II. Nie wszystko powinno trafić do internetu

Przed dodaniem zdjęcia lub informacji warto zadać sobie pytanie: czy powiedziałbym to również zupełnie obcej osobie?

Lepiej nie publikować zdjęć dokumentów, kart płatniczych, recept ani korespondencji zawierającej adres. Ostrożnie należy podchodzić również do informowania o dłuższym wyjeździe. Publiczny post o pustym mieszkaniu może zainteresować nie tylko znajomych.

Zdjęcie także może ujawniać więcej, niż się wydaje. W tle mogą być widoczne numery dokumentów,



adres na kopercie, tablica rejestracyjna samochodu albo charakterystyczne elementy wskazujące miejsce zamieszkania.

III. Skorzystaj z kontroli prywatności

Facebook udostępnia funkcję pozwalającą przejrzeć najważniejsze ustawienia prywatności. Można tam sprawdzić między innymi:

- kto widzi publikowane przez nas treści;
- kto może wysyłać zaproszenia do grona znajomych;
- kto może znaleźć nasz profil na podstawie numeru telefonu lub adresu e-mail;
- jakie informacje są widoczne na profilu;
- które osoby zostały zablokowane.

Na komputerze ustawienia te można znaleźć po kliknięciu zdjęcia profilowego, a następnie wejściu w **Ustawienia i prywatność** oraz **Ustawienia**. W części dotyczącej odbiorców i widoczności można zmienić zasady udostępniania postów, relacji, danych profilowych i oznaczeń. Nazwy oraz położenie poszczególnych opcji mogą się nieznacznie różnić w zależności od urządzenia i wersji aplikacji.

IV. Uważaj na zaproszenia od nieznajomych

Zdjęcie profilowe i znajome nazwisko nie są dowodem, że po drugiej stronie znajduje się właściwa osoba. Oszuści potrafią utworzyć kopię prawdziwego profilu, wykorzystując znalezione w internecie zdjęcia i informacje.

Zanim przyjmimy zaproszenie, sprawdźmy:

- czy dana osoba nie znajduje się już na naszej liście znajomych;
- kiedy konto zostało założone;
- czy ma wcześniejsze posty i wspólnych znajomych;
- czy sposób pisania pasuje do osoby, którą znamy.

Jeśli mamy wątpliwości, najlepiej zadzwonić do tej osoby i zapytać, czy rzeczywiście utworzyła nowe konto.

V. Jak rozpoznać, że konto znajomego zostało przejęte?

Pierwszym sygnałem może być nietypowa wiadomość. Oszust często zaczyna od niewinnego pytania: „Masz chwilę?”, „Możesz mi pomóc?” albo „Czy możesz zagłosować na moje zdjęcie?”. Później przesyła link, prosi o podanie kodu, wykonanie przelewu lub opłacenie zamówienia.

Niepokój powinny wzbudzić szczególnie:



- nagła prośba o pieniądze lub kod BLIK;
- wywieranie presji i podkreślanie, że sprawa jest pilna;
- wiadomość napisana w sposób nietypowy dla znajomego;
- unikanie rozmowy telefonicznej;
- prośba o kliknięcie w link i ponowne zalogowanie się do Facebooka;
- informacja o konkursie lub głosowaniu wymagającym podania danych.

Przestępcy często wykorzystują przejęte konta, ponieważ wiadomość od znanej osoby budzi większe zaufanie. CERT Polska ostrzega, że oszuści kontaktują się ze znajomymi właściciela profilu i proszą o szybką pomoc finansową, licząc na działanie pod wpływem emocji.

VI. Znajomy prosi o kod BLIK. Co zrobić?

Przede wszystkim nie należy od razu przekazywać kodu. Trzeba skontaktować się ze znajomym w inny sposób - najlepiej zadzwonić na znany wcześniej numer telefonu. Nie wystarczy zadać pytania przez komunikator, ponieważ na wiadomości może odpowiadać oszust.

Jeżeli znajomy potwierdzi prośbę, przed zatwierdzeniem płatności należy dokładnie przeczytać komunikat w aplikacji bankowej. Warto sprawdzić kwotę oraz rodzaj operacji. Kod BLIK może posłużyć nie tylko do zapłaty, ale również do wypłaty gotówki z bankomatu.

Jeśli przekazaliśmy kod i zatwierdziliśmy podejrzaną operację, trzeba jak najszybciej skontaktować się z bankiem, a następnie zgłosić sprawę Policji. Należy zachować wiadomości, potwierdzenia i zrzuty ekranu.

VII. Uważaj na quizy i zabawy

„Jak będziesz wyglądać za 20 lat?“, „Jakie zwierzę pasuje do Twojego charakteru?“ albo „Odpowiedz na kilka pytań i poznaj swoją przyszłość“ – takie zabawy mogą wyglądać niewinnie.

Nie każdy quiz jest oszustwem, ale przed rozpoczęciem warto sprawdzić, czy przenosi nas na inną stronę i jakich danych żąda. Jeżeli aplikacja chce uzyskać dostęp do profilu, listy znajomych, zdjęć lub innych informacji, lepiej z niej zrezygnować.

VIII. Co zrobić, jeśli nasze konto zostało przejęte?

Jeżeli nadal możemy zalogować się na Facebooku, należy od razu:

1. zmienić hasło;
2. wylogować konto na wszystkich pozostałych urządzeniach;
3. włączyć uwierzytelnianie dwuskładnikowe;
4. sprawdzić, czy do konta nie dodano obcego adresu e-mail, numeru telefonu lub aplikacji;
5. przejrzeć wysłane wiadomości i opublikowane wpisy;



**Magiczny
Kraków**

6. ostrzec znajomych, aby nie odpowiadali na prośby o pieniądze.

Trzeba również zabezpieczyć pocztę elektroniczną, ponieważ osoba mająca dostęp do skrzynki może ponownie zmienić hasło do Facebooka. Jeśli nie możemy się zalogować, odzyskiwanie konta najlepiej rozpocząć na stronie **facebook.com/hacked**, korzystając z urządzenia, na którym wcześniej logowaliśmy się do Facebooka.

Seniorzy pamiętajcie, najlepszą ochroną jest chwila namysłu. Oszuści próbują wywołać pośpiech, strach albo chęć natychmiastowej pomocy. Zatrzymanie się na moment i sprawdzenie wiadomości może ochronić nie tylko nasze konto, ale również pieniądze naszych bliskich.

Marcin Majerek