

Prezentacja opracowana na podstawie materiałów „Bezpieczeństwo w serwisach informacyjnych Web 2.0” autorstwa Grzegorza Pruszczyka i Kamila Śliwowskiego

Krótkie wprowadzenie na podstawie Facebooka

SERWISY SPOŁECZNOŚCIOWE



Kodeks 2.0 - Komunikujmy się!

- **Serwisy społecznościowe** (Social Networks): definicja, typy, przykłady.
- Facebook jako narzędzie komunikacji: kto i w jakim celu najczęściej korzysta z Facebooka?
- Dorośli na Facebooku.
- Kontakt nauczyciel-uczeń na Facebooku.
- Profil szkoły na Facebooku. Korzyści i zagrożenia.

Kodeks 2.0 - Bezpieczeństwo

- I. Jak korzystać z wszelkich serwisów społecznościowych?
- I. Najważniejsze fakty o (nie)bezpieczeństwie Facebooka.



I. Jak korzystać z serwisów społecznościowych?

5 najbardziej przydatnych wskazówek.





1. Ustawienia

- Korzystanie z serwisu zacznij od wybrania ustawień prywatności i bezpieczeństwa.
 - Wybierz złożone, unikalne hasła dla konta. Zasady tworzenia haseł.
- 



2. Aplikacje

- Bądź ostrożny podczas instalacji aplikacji innych firm (np. aplikacji firmy Zynga na Facebooku).
 - Nie instaluj aplikacji ze źródeł, którym nie ufasz.
- 



3. Ludzie

- Przyjmuj zaproszenia wyłącznie od ludzi, których znasz.
- 



4. Polityka prywatności

- Zapoznaj się z *polityką prywatności* i warunkami korzystania z serwisu.
 - Ogranicz ilość informacji osobistych, do których usługa/ serwis ma dostęp.
- 



5. Odpowiedzialność

- Pisz i publikuj odpowiedzialnie.
 - Pamiętaj, że wszystkie informacje, zdjęcia, filmy staną się publiczne.
- 



II. (Nie)bezpieczeństwo Facebooka

5 najważniejszych faktów



1. Redystrybucja informacji

- Informacje o Tobie i Twoich działaniach są przesyłane do zewnętrznych firm: reklamodawców, operatorów gier online, etc.
- 



2. Automatyczne zmiany

- Ustawienia prywatności automatycznie zmieniają się na mniej restrykcyjne podczas dużych zmian w serwisie (np. dodania nowych funkcjonalności).
- 



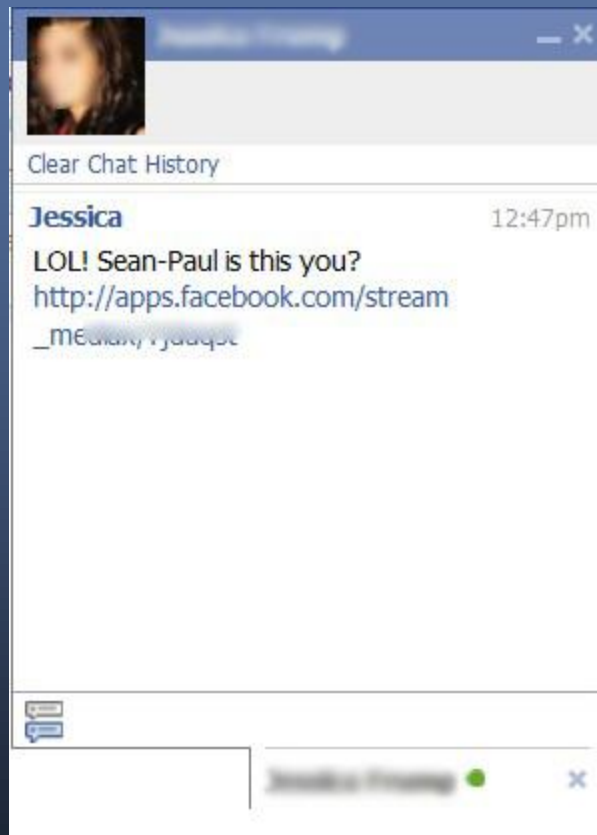
3. Malware

- Reklamy na Facebooku mogą zawierać malware, czyli złośliwe oprogramowanie.
- 

4. Ochrona znajomych

- Twoi znajomi nieświadomie mogą narażać Cię na niebezpieczeństwo – *Twoja ochrona jest tak dobra, jak ochrona twoich znajomych.*
- Jeśli Twój znajomy ma słabe hasło, które zostanie złamane, ktoś może rozesłać poprzez jego konto spam lub złośliwe oprogramowanie.

Próba Scamu na Facebooku



- Zainfekowane konto rozsyła automatycznie spam do znajomych z linkiem do strony, która będzie próbować wyłudzić nasz login i hasło; formularz logowania może być bardzo podobny do prawdziwej strony Facebooka. Wiele tego typu oszustw (Scam) obiecuje korzyści finansowe, wygrane w konkursach, obejrzenie kontrowersyjnych materiałów lub sugeruje, że np. nasze zdjęcia zostały umieszczone gdzieś w sieci (jak na obrazku).



5. A w realu...

- Za wieloma fałszywymi profilami czają się prawdziwi oszuści.
- 