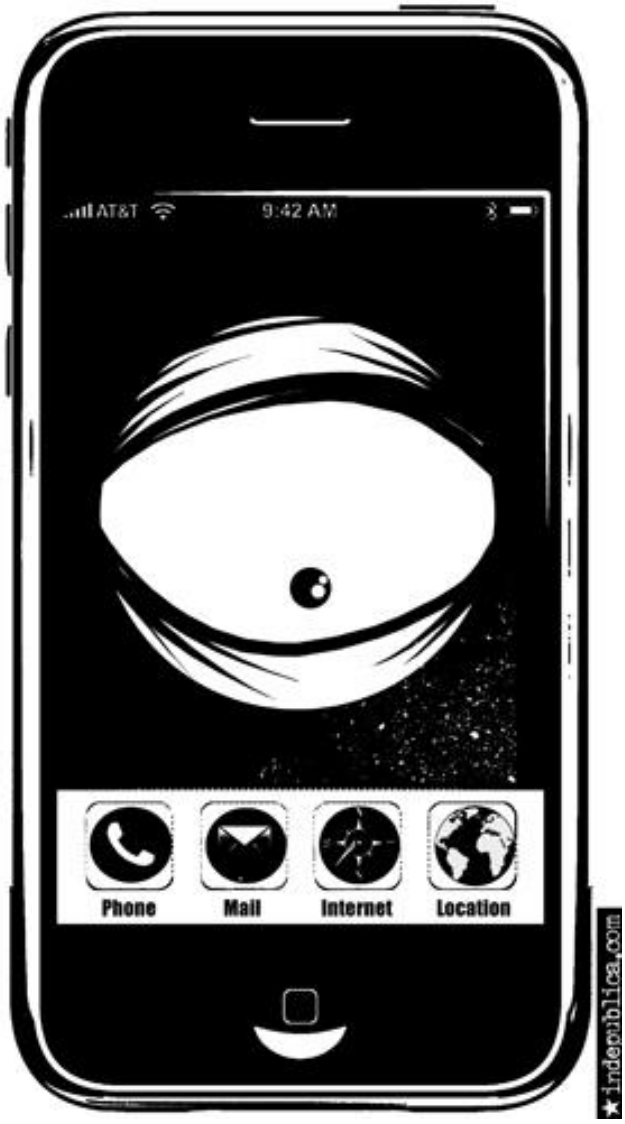
BEZPIECZEŃSTWO INFORMACYJNE W SERWISACH WEB 2.0

Grzegorz Prujszczyk

Kamil Śliwowski



Październik 2010, wersja 1.0. Treść podręcznika dostępna jest na licencji: Creative Commons – Uznanie Autorstwa – Na Tych Samych Warunkach 3.0 PL

Ilustracja na okładce aut. humblecitizen@Flickr, dostępne na Creative Commons – Uznanie Autorstwa – Na tych Samych Warunkach.

SPIS TREŚCI

„Jedyną możliwością wygranej jest nie grać wcale”

“The only winning move is not to play”

WOPR – Superkomputer do symulacji wojen nuklearnych z filmy Gry wojenne (WarGames) z 1986 r.

UDOSTĘPNIANIE DANYCH

Poniższy poradnik dotyczy Internetu, dlatego polecamy nie traktować go jak podręcznika szkolnego – ponieważ Internet, a nawet „internety”[1] są wszędzie i korzystamy z nich prawie nieustannie. Dlatego też problemy bezpieczeństwa udostępniania danych w sieci i komunikowania się przez niego dotyczą środowiska, które nigdy nie przestaje działać. Nie można z niego wyjść i wrócić za kilka dni, licząc, że gdy nas w nim nie ma, nic się nie dzieje i nic złego nie może się stać.

Niezależnie od serwisu, z którego chcemy skorzystać, poczty e-mail, strony, na której chcemy coś umieścić czy komunikatora, przez który chcemy się z kimś skomunikować, **wszelkie dane, jeśli nie są szyfrowane, są potencjalnie dostępne dla osób trzecich**. Wszystkie informacje przesyłane przez sieć bez użycia szyfrowania są dostępne dla wszystkich innych użytkowników naszej sieci lokalnej i wszystkich pośredników pomiędzy nami a serwerem docelowym. Oznacza to, że osoby postronne mogą przeczytać to, co czytamy i piszemy w sposób niezauważalny dla nas.

Jest to możliwe ponieważ komunikacja z serwerem serwisu, z którego korzystamy, prowadzona jest w formie standardowych pakietów informacji, które muszą przebyć drogę od naszego komputera do serwera, po drodze przechodząc przez naszą sieć lokalną do routera, potem do dostawcy internetu i poprzez kolejne punkty przesyłowe. Ponieważ pakiety mają określony format, mogą bez trudu zostać rozpoznane przez oprogramowanie do analizy ruchu, np. program Wireshark, i przedstawione w formie pozwalającej na wygodne odczytanie treści. Wszelka niezaszyfrowana komunikacja bez problemu może paść ofiarą takiej analizy sieci i osoba „uzbrojona” w taki program może czytać nasze czaty czy przechwycić prywatne zdjęcia.

[1]Jeśli chcesz dowiedzieć się więcej o „internetach” czy różnych sposobach korzystania z sieci przez młodzież polecamy raport „Młodzi i media” Centrum Badań nad Kulturą Popularną SWPS, http://www.mim.swps.pl/.

ŹRÓDŁA I CEL

- Każdy na trasie komunikacji może ustalić jej źródło i cel.
- Każdy komputer identyfikuje się nie tylko numerem IP, ale i innymi danymi, których suma pozwala rozróżnić konkretne komputery.
- Jeżeli łączymy się poprzez nieszyfrowane łącze (bez SSL), każdy ma dostęp do naszego hasła i reszty treści naszej komunikacji.
- W szczególnych przypadkach także połączenie szyfrowane SSL może być zagrożone – osoba atakująca może podać fałszywy (inny) certyfikat lub po fakcie złamać kodowanie z zapisanego zaszyfrowanego połączenia.
- Automatyczne działania przeglądarki i nasza nieuwaga stanowią podstawę większości z tych zagrożeń – możemy im zapobiec, odpowiednio konfigurując przeglądarkę i zwracając uwagę na to, co się w niej dzieje – nie wszystko da się zautomatyzować.

SŁOWNICZEK

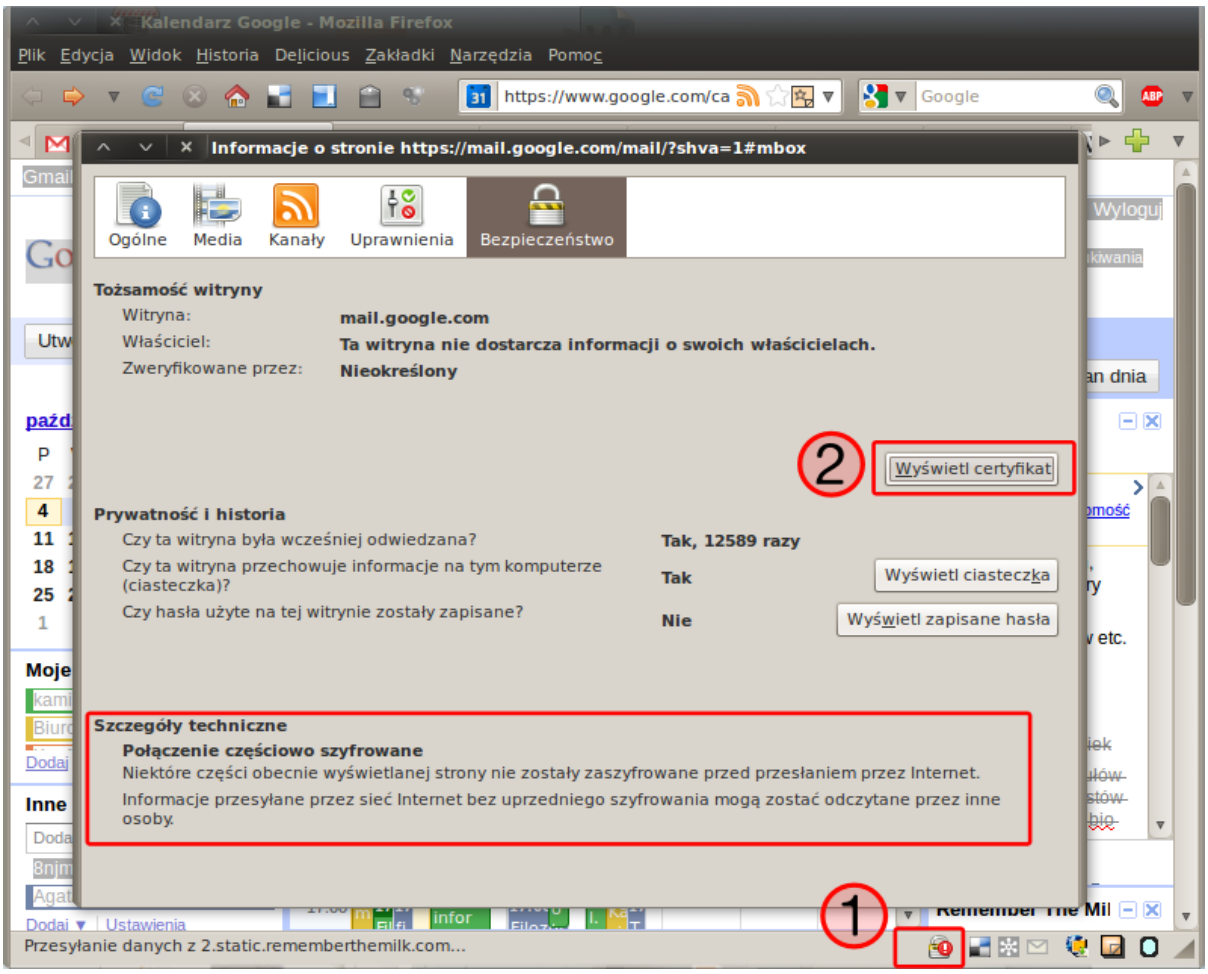
SSL (TSL) *jest to protokół (sposób przesyłania danych) pozwalający na poufność transmisji (jej zaszyfrowanie) i uwierzytelnienie źródła (co można rozumieć jako dowód tożsamości dla strony). Najpopularniejszym zastosowaniem protokołu SSL jest szyfrowanie komunikacji między stroną (serwerem usługi) a przeglądarką. Jest to głównie szyfrowanie symetryczne, którego działanie Wikipedia definiuje następująco: „do szyfrowania i deszyfrowania danych używany jest ten sam klucz; znając klucz szyfrujący możemy dokonać również deszyfracji danych (wyznaczyć klucz deszyfrujący)". W praktyce oznacza to, że serwer i nasza przeglądarka są w stanie same automatycznie zabezpieczyć połączenie i bardzo trudne byłoby odczytanie naszej komunikacji. Co więcej, w przeglądarce potwierdzić możemy tożsamość strony – sfałszowanie tej informacji (tak jak legitymacji czy dowodu) jest bardzo trudne i zdarza się bardzo rzadko.*

ZAGROŻENIA:

- każdy z większą wiedzą techniczną może bez problemu odczytać całość naszej komunikacji, prywatne zdjęcia itd., a potencjalnie także przechwycić nasze hasła i użyć ich według własnego uznania;
- instytucje rządowe przeważnie są w stanie dokładnie ustalić, z którego komputera zostały opublikowane treści, jeśli ktoś zgłosi popełnienie przestępstwa;
- osoba o dużej wiedzy technicznej może być w stanie złamać szyfrowanie SSL, dlatego należy pamiętać, że **zawsze wszystko, co publikujemy w internecie bez bardzo wysokiego poziomu zabezpieczenia, może wcześniej czy później stać się publiczne**.

OCHRONA:

- zawsze jeśli to tylko możliwe korzystamy z szyfrowania SSL;
- jeżeli chcemy by dane były naprawdę bezpieczne, szyfrujemy je, np. przy użyciu programu truecrypt i hasło przekazujemy inną drogą komunikacji;
- używanie alternatywnych sieci, np. TOR;
- uważne korzystanie z przeglądarki internetowej; nigdy nie korzystaj z opcji zapamiętywania haseł do żadnych kont i serwisów, każdy z dostępem do Twojego komputera będzie miał do nich dostęp.



Rys.1. SSL – widok informacji o bezpieczeństwie na stronie kalendarza Gmail z szyfrowaniem.

1. Ikonka informująca o działaniu szyfrowania na stronie („kłódka”) ale bez uwierzytelnionych wszystkich źródeł treści.
2. Widok ustawień bezpieczeństwa w Mozilla Firefox – możliwość wyświetlenia certyfikatu bezpieczeństwa, anulowania itd. oraz podstawowe informacje o szyfrowaniu danej strony.

SŁOWNICZEK

Wtyczka *(ang. plug-in, add-on) dodatkowy moduł do programu komputerowego, który rozszerza jego możliwości. Stosowanie wtyczek jest coraz częstszym zabiegiem wśród twórców programów, a zwłaszcza tych tworzących otwarte oprogramowanie. Zaletą takiego rozwiązania jest to, że użytkownicy mogą wybierać pomiędzy funkcjami, które chcą mieć w programie, a których nie. Poza tym odciąża to autora od pisania całego kodu programu, a zrzuca część tego obowiązku na zewnętrznych programistów. Najpopularniejszymi programami oferującymi wtyczki są przeglądarki internetowe oraz programy pocztowe, np. Mozilla Firefox i Mozilla Thunderbird. W obu dzięki wtyczkom można znacząco zwiększyć poziom bezpieczeństwa i prywatności komunikacji, co opisujemy poniżej.*

Źródło: http://pl.wikipedia.org/wiki/Wtyczka, treść dostępna na licencji CC-BY-SA.

WAŻNY LINK

HTTPS Everywhere

https://www.eff.org/https-everywhere oraz https://www.eff.org/https-everywhere to wtyczka do przeglądarki Mozilla Firefox wymuszająca połączenie szyfrowane SSL na popularnych stronach, które często nie mają uruchomionego szyfrowania automatycznie, ale mają taką możliwość.

SŁOWNICZEK

TOR – *Tor (ang. The Onion Router) jest wirtualną siecią komputerową zapobiegającą analizie ruchu sieciowego i w konsekwencji zapewniającą użytkownikom prawie anonimowy dostęp do zasobów Internetu. Podobnie jak sieci Freenet, GNUnet czy MUTE, Tor może być wykorzystywany w celu ominięcia mechanizmów filtrowania treści, cenzury i innych ograniczeń komunikacyjnych. Gdy używasz Tora do przeglądania witryn sieci Web, Twoje połączenia są losowo kierowane przez sieć niezależnych serwerów proxy (czyli serwerów pośredniczących w komunikacji). Cały ruch między serwerami Tor (lub przekaźnikami) jest szyfrowany, a każdy z przekaźników zna adres IP tylko dwóch innych przekaźników – tego, który go bezpośrednio poprzedza i tego, który następuje bezpośrednio po nim.* ***TOR, dzięki zapewnianiu prawie całkowitej anonimowości, jak każde narzędzie może być wykorzystywane w dobrej i złej wierze, np. prowadzeniu działalności przestępczej. Podobnie jak w normalnym internecie znajduje się tam wiele miejsc, w które dla własnego dobra lepiej nie zaglądać.*** *Więcej o projekcie znajdziecie na stronie: www.torproject.org*

Najprostszym sposobem na rozpoczęcie pracy z TOR-em jest zainstalowanie pakietu wraz z wtyczką do przeglądarki Firefox o nazwie TOR Button (https://www.torproject.org/torbutton/), która umożliwia zmianę trybu pracy ze standardowego do połączenia przez TOR za pomocą jednego przycisku. Więcej o konfiguracji TOR-a oraz serwerów proxy znajdziecie w podręczniku o obchodzeniu cenzury w sieci z serii Floss Manuals. Znajdziecie tam dokładne informacje, jak konfigurować swoje połączenie w najbezpieczniejszy sposób.

WAŻNY LINK

Floss Manuals – http://en.flossmanuals.net/

zbiór darmowych podręczników o korzystaniu z narzędzi internetowych oraz wolnego i otwartego oprogramowania. Znajduje się tam m.in. podręcznik o obchodzeniu cenzury w sieci czy korzystaniu z popularnego oprogramowania do publikacji stron internetowych Wordpress.

REGULAMINY SERWISÓW, POLITYKA PRYWATNOŚCI I PRAWO AUTORSKIE

W świecie fizycznym kupując coś w sklepie lub wsiadając do autobusu, jesteśmy świadomi podejmowania czynności prawnej – a przynajmniej, że podejmowana czynność jest regulowana prawnie. Wiemy, że np. za usiłowanie zmiany trasy autobusu lub jego niszczenie możemy zostać z niego usunięci i ukarani.

W przypadku korzystania z serwisów internetowych, w większości darmowych, często zapominamy, że również wchodzimy w podobną relację. Dlatego podczas rejestrowania się w serwisach społecznościowych czy innego rodzaju serwisach internetowych wymagane jest, abyśmy potwierdzili, że zapoznaliśmy się z regulaminem serwisu i/lub polityką prywatności. Oba dokumenty dostępne są zwykle jako linki gdzieś poniżej lub obok miejsca, w którym potwierdzamy ich przeczytanie. Jest to moment, w którym zgadzamy się na warunki stawiane przez właścicieli serwisu oraz zgadzamy się na przetwarzanie naszych danych w sposób opisany w *Polityce prywatności*. W obu dokumentach, zależnie od dobrej lub złej woli ich twórców, mogą czekać na nas różnego rodzaju niebezpieczeństwa: od zbyt szerokiego zakresu przetwarzania danych po warunki regulaminowe umożliwiające właścicielom serwisu np. usunąć nasze konto z byle powodu lub wykorzystywać nasze dane lub treść umieszczaną w serwisie do celów reklamowych. Niektóre serwisy wręcz zastrzegają sobie możliwość przekazywania naszych danych innym firmom, agencjom rządowym, gdyby o te dane poprosiły lub wykorzystania naszych treści w celach komercyjnych (wymuszając w regulaminie przeniesienie praw autorskich majątkowych z autora na właścicieli serwisu). Ogromnym ryzykiem w tej sytuacji jest również wykorzystywanie serwisów zarejestrowanych w różnych państwach – w przypadku, których nie posiadamy ochrony i regulacji jak w Polsce, np. ze strony Generalnego Inspektora Danych Osobowych.

WAŻNY LINK

Generalny Inspektor Ochrony Danych Osobowych – www.giodo.gov.pl

Serwisy internetowe, a zwłaszcza Facebook, Google czy sklep internetowy Amazon.com bardzo często zmieniają treść dokumentacji opisującej warunki korzystania z serwisu. Teoretycznie o każdej takiej zmianie wszyscy użytkownicy powinni zostać powiadomieni, ale bardzo często dokonuje się tych zmian tak, że większość z korzystających tego nie zauważa. Aby zobaczyć jaka jest skala i częstotliwość zmian lub sprawdzić czy na pewno dobrze wiemy, jakie warunki stawia nam dostawca jakiejś usługi, warto wejść na **stronę monitorującą TOS** (ang. *terms of service* – warunki korzystania), gdzie śledzi się 56 najważniejszych serwisówpod kątem ich TOS.

WAŻNY LINK

Terms of Service tracker – www.tosback.org

Warto pamiętać, że sytuacja braku kontroli nad treścią może zepsuć nam wiele planów, np. z serwisu społecznościowego może zostać usunięty nasz projekt albo ogłoszenia nauczyciela, co spowoduje automatycznie wiele problemów: kara za brak pracy domowej albo nieobecność na ważnym wydarzeniu, o którym nie dowiedzieliśmy się, bo informacja „zniknęła”. W przypadku szkoły zawsze najlepiej zorganizować przestrzeń do publikacji zarówno dla uczniów, jak i nauczycieli, nad którą będzie się posiadać kontrolę. Najlepszym miejscem na ogłoszenia jest strona szkoły, a do publikowania naszych prac możemy wykorzystać oprogramowanie wiki. Dobra organizacja informacji w sieci i kontrola nad nią będzie sprzyjać komunikacji między uczniami, nauczycielami i rodzicami. Aby była stała i nie powodowała problemów, musimy zadbać najpierw o jej infrastrukturę i bezpieczeństwo, a zwłaszcza bezpieczeństwo danych osób komunikujących się ze sobą. Posiadanie praw do naszych treści, możliwość wyłączenia naszych kont w dowolnym momencie lub brak możliwości eksportowania danych do innych serwisów nie ułatwią nam komunikacji.

SŁOWNICZEK

Polityka prywatności *– dokument umieszczany na witrynie internetowej w celu poinformowania użytkowników o tym, jakie dane osobowe są o nich zbierane i jak będą wykorzystywane, w szczególności czy są przekazywane innym firmom. Mogą to być dane zbierane automatycznie przez serwer lub podawane przez użytkownika*, np. *podczas rejestracji. Taki dokument powinien zawierać następujące informacje: w jaki sposób właściciel witryny internetowej będzie się kontaktował z użytkownikiem, w jaki sposób można dokonać zmian w danych osobowych użytkownika, w jaki sposób są zabezpieczane dane pobierane od użytkowników.*

W Polsce nadzór nad przetwarzaniem danych osobowych sprawuje Generalny Inspektor Ochrony Danych Osobowych. Źródło: Wikipedia.

CZY WIESZ, KTO JEST WŁAŚCICIELEM TWOJEJ PRACY I TWOICH PRYWATNYCH DANYCH?

Poniżej fragment warunków użytkowania serwisu zawierającego zapis o licencji jakiej użytkownik udziela firmie Google, właścicielowi serwisu YouTube:

„8. Prawa, na które użytkownik udziela licencji

8.1 Przesyłając do YouTube lub zamieszczając w jego witrynach Treści, użytkownik udziela:

YouTube nieograniczonej terytorialnie, niewyłącznej, bezpłatnej, zbywalnej licencji (z prawem sublicencji) na korzystanie z Treści, powielanie takich Treści, ich rozpowszechnianie, opracowywanie na ich podstawie utworów zależnych, ich wystawianie bądź wykonywanie w związku ze świadczeniem Usług i prowadzeniem działalności YouTube, w tym m.in. do promowania i rozpowszechniania Usług w części lub całości (wraz z utworami zależnymi) niezależnie od formatu nośnika i sposobu przekazywania materiału;

każdemu użytkownikowi Usług - nieograniczonej terytorialnie, niewyłącznej, bezpłatnej licencji na dostęp do jego Treści za pośrednictwem Usług oraz na korzystanie z takich Treści, ich powielanie i rozpowszechnianie, opracowywanie na ich podstawie utworów zależnych, oraz ich wystawianie bądź wykonywanie w ramach zespołu funkcji oferowanych przez Usługi oraz w granicach dozwolonych na podstawie niniejszych Warunków.8.2 Powyższe licencje udzielane przez użytkownika w odniesieniu do Treści wygasają z chwilą, gdy użytkownik usunie lub wykasuje je z Witryny Internetowej. Powyższe licencje udzielone przez użytkownika w odniesieniu do komentarzy tekstowych zgłoszonych jako Treść są nieograniczone w czasie i nieodwołalne, jednakże pod innymi względami pozostają bez znaczenia dla praw własności użytkownika określonych w artykule 7.2 powyżej."

Możesz z powyższego fragmentu lub całej umowy (dostępnej na stronie http://www.youtube.com/t/terms) wypisać w punktach, na co się zgadzasz, zamieszczając film w tym serwisie. Pomyśl też, jakie użycia może taka zgoda za sobą pociągnąć. Podobnie ma się sprawa z Facebookiem i wieloma innymi serwisami. Licencje na treści, które umieszczamy, zezwalają tym firmom promować się dzięki nam oraz wykorzystywać nasze dane i materiały komercyjnie. Facebookowi użył zdjęć z profili swoich użytkowników na billboardach reklamujących serwis w Australii. Ogromny sprzeciw i ostatecznie zmianę warunków wykorzystywania przez serwis treści umieszczanych w nim przez użytkowników wzbudził zapis zezwalający dostawcom aplikacji oraz firmom współpracującym z serwisem na wykorzystywanie m.in. zdjęć w celach komercyjnych.
Ochrona Twoich praw autorskich w sieci jest szczególnie ważna, rzeczy, które sam zrobiłeś i umieszczasz w sieci, są Twoją twórczością, którą chcesz się podzielić z innymi, ale niekoniecznie chciałbyś, by były wykorzystywane komercyjne lub wbrew Twojej woli. W internecie nigdy nie będziesz mieć nad raz opublikowaną rzeczą kontroli, ale zawsze powinieneś/powinnaś być świadom/a możliwości ochrony prawnej.

Nie kradnij i nie daj się okraść! 3. punkt Kodeksu Szkoły 2.0 wyraźnie zwraca uwagę na niebezpieczeństwa związane z prawem autorskim w sieci. Rzadko zwraca się uwagę na to, że to nasze prawa są częściej zagrożone przez korporacje i firmy, a nie odwrotnie. W szkole większym problemem od piractwa jest plagiat, którego powinniście się szczególnie wystrzegać. Internet daje ogromne możliwości sprawnego wykrywania plagiatów, równocześnie ułatwiając samo kopiowanie. Ważne jest, by umiejętnie cytować i wykorzystywać twórczość innych, a nie jedynie ją kopiować – również w sieci. Ogrom informacji i łatwość, z jaką można nimi i mediami obracać w sieci ułatwia również bezkrytyczne korzystanie z nich. Jeśli nauczysz się dbać o bezpieczeństwo swoich danych, kontrolować swoje prawa oraz rozumieć prawa innych osób publikujących w sieci, będziesz również potrafił/a ***korzystać z sieci samodzielnie i krytycznie***, o czym mówi pkt. 2. Kodeksu 2.0.

FORMY OCHRONY:

- Korzystanie z serwisów hostujących (to znaczy trzymających i udostępniających) media na warunkach definiowanych przez użytkownika, np. zezwalających na jedynie prywatne wyświetlanie filmów (po podaniu np. adresów mailowych) lub dających możliwość nadania materiałom licencji Creative Commons lub innych, np. www.flickr.com dla zdjęć, www.blip.tv lub www.vimeo.com dla materiałów wideo, http://identi.ca/ dla publikowania mikroblogu.
- Niepublikowanie mediów w najwyższej jakości, jeśli nie chcemy ich potencjalnego wykorzystania (np. zdjęcia albo klipy video publikujemy w jakości w jakiej będą prezentowane).

METADANE I INFORMACJE UDZIELANE AUTOMATYCZNIE

SŁOWNICZEK

Metadane *– czyli „dane o danych”, ich przykładem są klasyczne katalogi biblioteczne. Przy pomocy metadanych opisywane są dokumenty elektroniczne, w szczególności dokumenty dostępne poprzez sieci komputerowe, np. strony World Wide Web, a także dokumenty tworzące nowoczesne biblioteki cyfrowe. Jednym ze standardów metadanych jest Dublin Core Metadata Element Set (DCMES) czy EXIF standard metadanych dla plików z obrazkami.*
Metadanymi są również informacje na temat danych (plików, katalogów) zapisanych w systemie plików na dysku. (źródło: Wikipedia, http://pl.wikipedia.org/wiki/Metadane*)*

Wiele informacji udostępniamy nieświadomie właśnie za pośrednictwem metadanych, np.:

- Dane identyfikujące – programy biurowe i wiele innych domyślnie wstawiają dane licencyjne w opis pliku; zestaw informacji podawanych przez przeglądarkę (user agent + adres ip + konfiguracja wtyczek + odwiedzane strony) pozwala na wyróżnienie pojedynczego użytkownika;
- Zdjęcia wykonane telefonami często zawierają zapisane położenie telefonu, można w ten sposób nie tylko pokazać, co ma się w domu, ale też podać swój adres. Telefony wyposażone w GPS, np. iphone, często same i bez informowania o tym użytkownika podają swoją dokładną lokalizację na potrzebę różnych serwisów; niektóre uruchamiają tę funkcje domyślnie.

GEOLOKALIZACJA. PUBLIKOWANIE INFORMACJI O TYM GDZIE JEST-EŚMY I CO ROBIMY

Okazja czyni złodzieja, mawia mądrość ludowa, w myśl której działają nie tylko złodzieje, ale również sceptycy ujawniania informacji o tym, co robimy i gdzie jesteśmy w danym momencie. **http://pleaserobme.com/** to inicjatywa nie tyle mająca nam uświadomić, że gdy wpiszemy na Twitterze, Facebooku czy innym serwisie informację o tym, że właśnie wyjechaliśmy na wakacje zaraz obok informacji o naszym miejscu zamieszkania, aż prosi się, by ktoś o złych zamiarach połączył te wiadomości i po prostu okradł nasz dom. Jeśli brzmi to mało prawdopodobnie, poszukajcie w sieci artykułów z brytyjskiego pisma „The Independent" o szajce złodziei, która okradała domy znanych gwiazd, dokładnie śledząc ich informacje w serwisach społecznościowych[2].

ZAGROŻENIA:

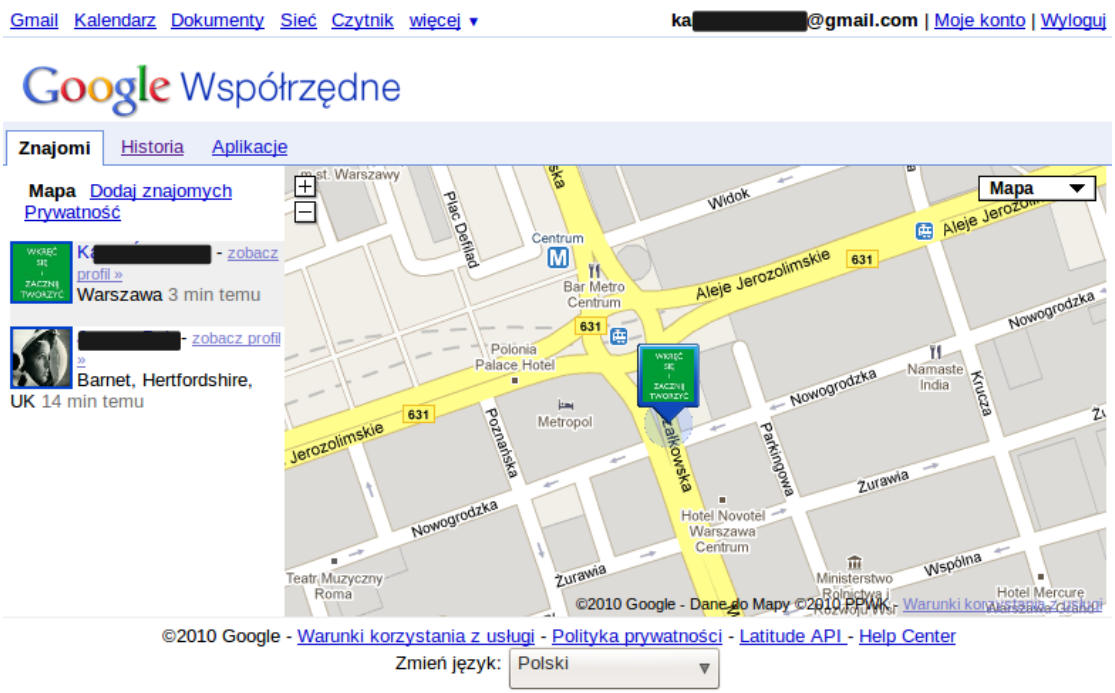
Możemy zdradzić więcej niż chcemy. Jeśli publikujemy opowiadanie pod pseudonimem, ale chcemy umożliwić kontakt zainteresowanym, to warto zadbać, aby podany adres email nie zawierał naszego prawdziwego nazwiska.

Zdjęcie z komórki może zawierać dokładne położenie aparatu w chwili jego wykonania – domu, szkoły, czy innego miejsca, które ma pozostać prywatne.

FORMY OCHRONY:

- Myślenie o tym, co robimy – nasze rozsądne zachowanie jest ważniejsze niż moda czy coś, co robią nasi znajomi.
- Świadomość działania programów i sprzętu, który posiadamy (ich opisy powinny znajdować się w instrukcjach lub warunkach korzystania). Szczególnie uważaj na aplikacje instalowane w telefonach komórkowych oraz programy korzystające ze stałego połączenia z siecią.
- Najlepiej nigdy nie publikować dokładnego adresu naszego zamieszkania czy pobytu, z wyjątkiem sklepów lub innych usług wysyłających nam dokumenty nikt nie powinien go znać.
- Zawsze należy się liczyć z tym, że gdy tweetujemy, gdzie idziemy, dowiadują się o tym wszyscy, a nie tylko nasi przyjaciele i bliscy (ułatwiamy tym samym możliwość śledzenia nas, nachodzenia lub wykorzystywania przez innych tej wiedzy do ich celów).
- Należy się liczyć z tym, że nasze raportowanie na bieżąco z rodzinnych wakacji informuje wszystkich zainteresowanych, że nasz dom stoi pusty itp.

[2]http://www.independent.co.uk/news/world/americas/hollywood-stars-robbed-by-teenage-bling-ring-1968241.html



Rys. 2. Dokładna lokacja miejsca pracy autora w trakcie pisania tego podręcznika podawana również znajomym w usłudze Google Latitude. Lattitude lokalizuje użytkowników za pomocą danych sieci, z których korzystają, np. WiFi, połączeń 3g.

Zadanie:

Wykonaj kilka zdjęć w różnych miejscach dowolnymi telefonami komórkowymi i zamieść je w usłudze Google Picassa. Sprawdź, które z nich zawierają dane o lokalizacji wykonania zdjęcia. Picassa wyświetli precyzyjną mapę obok galerii. Za pomocą programu Exiftool (http://www.sno.phy.queensu.ca/~phil/exiftool/) odczytaj i zmodyfikuj informacje o zdjęciu, np. lokalizację wykonania, i ponownie umieść je w serwisie Picassa. Jaki efekt osiągnąłeś/aś?

ZAGROŻENIA BEZPOŚREDNIE

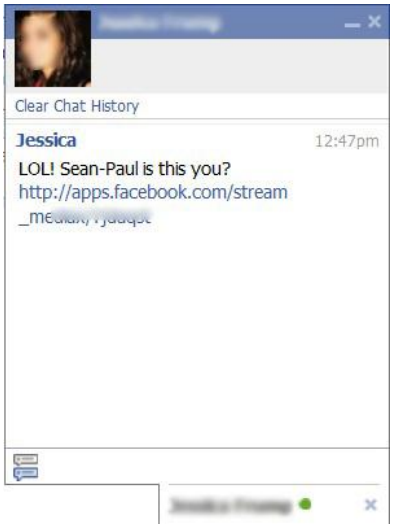
O bezpieczeństwie danych należy myśleć w kontekście całej naszej komunikacji i korzystania ze sprzętu komputerowego czy innych urządzeń połączonych z siecią. Na końcu Kodeksu 2.0 znajdujemy najbardziej podstawowe problemy – bezpieczeństwa oraz korzystania z komputerów. Wiemy, że dobrze mieć je zawsze pod ręką (lub w telefonie) i połączone z siecią, lecz musimy pamiętać, że to tylko narzędzia, które są narażone na wiele problemów i nigdy nie mogą zastąpić nas w myśleniu o bezpieczeństwie.

Zagrożenia bezpośrednie zdarzają się w każdym serwisie: od Facebooka przez Twittera i naszą klasę. Wykorzystują zarówno możliwości bezpośredniej komunikacji między użytkownikami, jak również luki bezpieczeństwa w serwisach czy w oprogramowaniu działającym na naszym sprzęcie.

SŁOWNICZEK

Spam *to niechciana komunikacja. Powszechnie kojarzony przede wszystkim z pocztą elektroniczną, jest jednak popularnym 'zjawiskiem' także na serwisach społecznościowych, a w zasadzie w dowolnej przestrzeni pozwalającej na komunikację. Spam może powodować szereg problemów i nie chodzi tu tylko o zapychanie nam skrzynki przez znajomych spędzających za dużo czasu w sieci.*
Spam to blisko 90% całej korespondencji w sieci, a więc i kolosalne obciążenie dla jej infrastruktury. W interesie wszystkich internautów jest nie tylko obrona przed spamem własnej skrzynki, ale także minimalizowanie jego ilości. W sieciach społecznościowych również występują typy spamu, które znać możemy z poczty – reklamy, scam (nigerian scam).

Scam*, często nazywany też nigerian scam ze względu na stereotyp popularności tego rodzaju zarobku w Nigerii. Scam to ogólnie naciąganie czy wyłudzenie – klasycznie polega na próbie wmówienia nam, że oczekuje na nas wielki spadek/nagroda pod warunkiem, że przelejemy trochę pieniędzy. Z drugiej strony mogą być to próby przekrętów przy płatności za przedmioty na aukcjach.*
Źródło: Wikipedia, pl.wikipedia.org/wiki/Scam)



Rys.3. Przykładowa próba Scamu w serwisie Facebook. 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 obiecuje korzyści finansowe (wygrane w konkursach), obejrzenie kontrowersyjnych materiałów lub sugeruje, że np. nasze zdjęcia zostały umieszczone gdzieś w sieci (jak na obrazku).

Większość treści SPAM-u to reklamy, które mają nas nakłonić do zakupu najróżniejszych produktów. Często SPAM to również masowy marketing szeptany, tzn. wiadomości, które mają wyglądać jak wiadomości od naszych przyjaciół. Większość sklepów reklamujących się w ten sposób nie ma w zwyczaju wysyłać opłaconego towaru, ale nawet gdyby mieli to zrobić, czy jest sens nagradzać tak szkodliwe dla sieci zachowanie?

SŁOWNICZEK

Phishing (spoofing) *– wyłudzanie poufnych informacji osobistych (np. haseł lub szczegółów karty kredytowej) przez podszywanie się pod godną zaufania osobę lub instytucję, której te informacje są pilnie potrzebne (np. Twój bank). Jest to rodzaj ataku opartego na inżynierii społecznej, tzn. wykorzystujący naszą nieuwagę, zaufanie do danej instytucji i często odruchowe działania.*

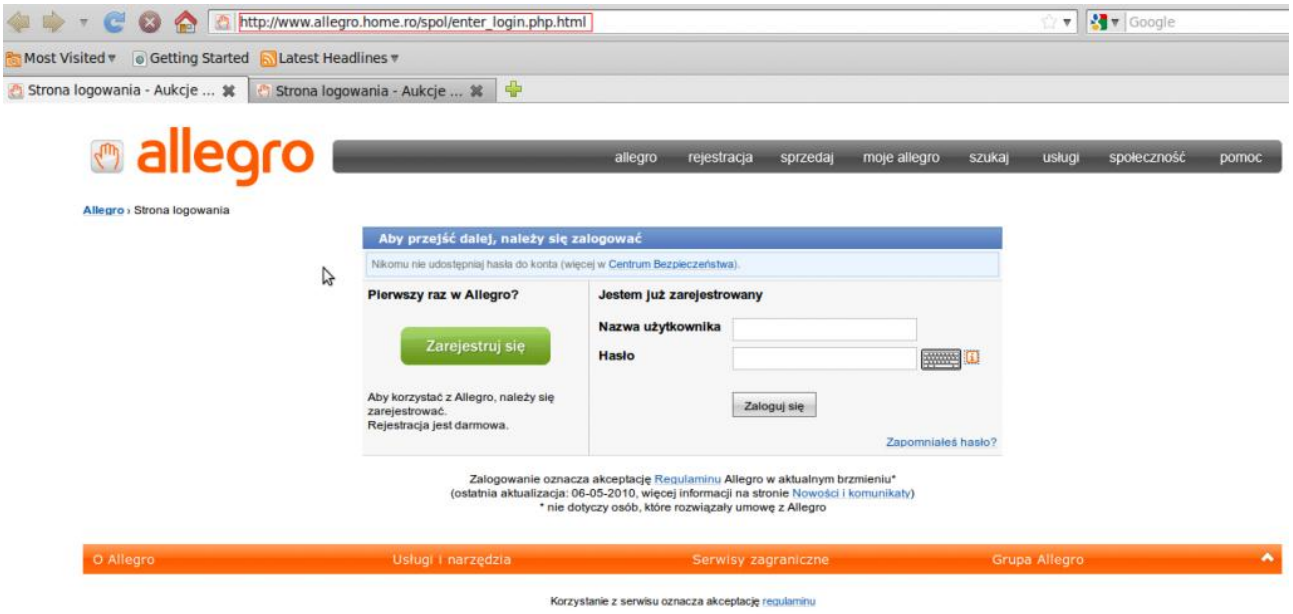
Więcej na http://pl.wikipedia.org/wiki/Phishing

ZAGROŻENIA:

- Możemy dać się oszukać i stracić pieniądze lub informacje;
- Kradzież tożsamości – wykorzystanie naszych danych do operacji finansowych, sprokurowania fałszywych zeznań etc.;
- Przejęcie kontroli nad kontami w danych serwisach – wykorzystanie ich w celach spamowania, niszczenia naszej reputacji, usunięcia etc.

OCHRONA:

- Serwisy i ich pracownicy nigdy nie potrzebują naszego hasła i nie będą o nie prosić, dlatego nigdy nie podawaj go poza miejscami, w których się logujesz i jesteś pewien, że są bezpieczne (zwracaj uwagę, czy serwis zawsze stosuje bezpieczne szyfrowanie). Uważaj na wygląd stron, na których podajesz swoje dane; czy na pewno wyglądają tak samo i czy nie zawierają elementów nietypowych.
- Zawsze należy uważnie przyjrzeć się linkom z maila oraz adresom stron logowania, na które jesteśmy przekierowywani (jeśli nie zauważyliśmy nic podejrzanego już w samym mailu). Zwróć uwagę, czy link nie zawiera dziwnych elementów, których nie mają sprawdzone adresy danego serwisu.
- Jeśli otrzymujemy informację personalną z jakiejś instytucji lub serwisu, upewnijmy się czy na pewno napisała do nas osoba, z której konta otrzymujemy maila? Jeśli prosi o jakieś ważne informacje lub opłaty, warto to potwierdzić inną drogą.
- Jeśli korzystasz z systemu operacyjnego Windows, pamiętaj o posiadaniu sprawnego i aktualnego oprogramowania antywirusowego, choć żaden taki program nie zastąpi ostrożności, a jedynie pomoże w wykryciu najprostszych zagrożeń.



Rys.4. Przykład próby phishingu (wyłudzenia danych konta) z serwisu allegro.

Strona jest prawie identyczna wizualnie z prawdziwą, ale jej adres nie – zwróć uwagę na niestandardowe fragmenty.

WAŻNY LINK

Security in a box – http://security.ngoinabox.org/

Zestaw darmowego oprogramowania służącego bezpieczeństwu informacji oraz Twojego komputera. Znajdują się tu również informacje o jego instalacji oraz o podstawowych zasadach „higieny informacyjnej", np. jak i dlaczego należy robić kopie zapasowe (tzw. backupy).

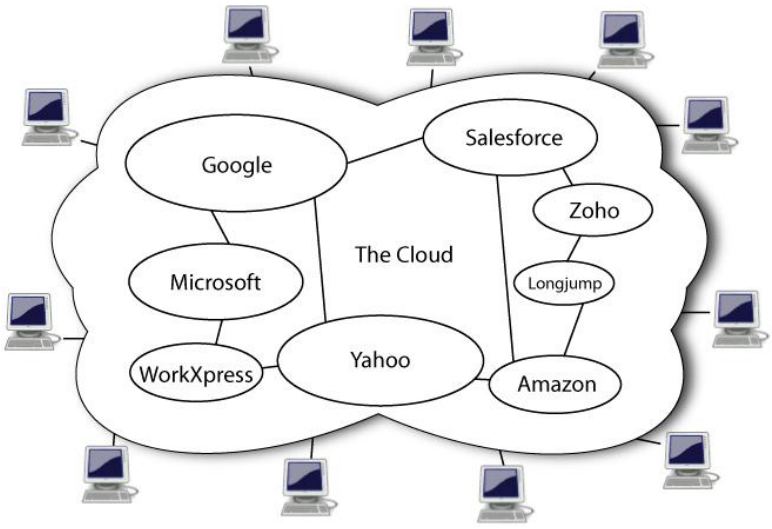
SŁOWNICZEK

Likejacking *to złośliwa technika nakłaniania użytkowników do odwiedzenia niechcianych linków poprzez opcję „lubię to" na Facebook'u (tzw. like button) i delegowanie informacji jako ich statusu. Po kliknięciu na link ofiara zwykle nie widzi obiecanej treści, ale raczej puste strony z informacją "kliknij tutaj, aby kontynuować". Ta strona zawiera robaka (Troj / Iframe-ET lub podobnego). Kliknięcie „dalej", a czasem nawet w dowolne miejsce na stronie, powoduje umieszczenie informacji na naszym profilu i dalsze rozprzestrzenianie się robaka. Zwykle metodą na zachęcenie do kliknięcia jest kontrowersyjny lub intrygujący temat wiadomości, np. „Controversial truth about 9/11, know what really happened to collapsed buildings" (źródło: Wikipedia,* http://en.wikipedia.org/wiki/Likejacking).

Datamining *– in. eksploracja danych. Idea eksploracji danych polega na wykorzystaniu szybkości komputera do znajdowania ukrytych dla człowieka (właśnie z uwagi na ograniczone możliwości czasowe) prawidłowości w danych zgromadzonych w dużych bazach danych, np. serwisów społecznościowych. Tworząc profil na stronie zakładamy, że dane, które publikujemy, będą dostępne jedynie na zasadach, które proponuje firma i które my akceptujemy, jednak niestety nie musi tak być. Częściej niż się do tego przyznają, firmy tracą nasze dane czy to w wyniku własnych pomyłek, czy celowych ataków ze strony tzw. „hackerów". Nawet służbom wywiadowczym zdarza się zgubić ściśle tajne dane – nie powinniśmy więc zakładać, że nasze dane powierzone prywatnej firmie, której podstawowym celem jest jak największy zysk przy jak najmniejszych kosztach, będą bezpieczniejsze... Skalę problemu ujawniania poufnych danych możemy zobaczyć na stronie:* http://datalossdb.org/

GOOGLE I ZAGROŻENIA Z "CHMURY"

Cloud Computing (ang. "przetwarzanie w chmurze, chmury obliczeniowe") – model przetwarzania danych przez usługi dostarczane użytkownikowi przez zewnętrzne organizacje. W skrócie, zamiast dostarczać użytkownikowi oprogramowanie, które musi zainstalować (oraz licencji na jego użytkowanie), dostarcza się usługę (np. obsługę poczty mailowej) dostępną w sieci. Umożliwia to m.in. dostępność usług niezależnie od sprzętu oraz zwiększenie możliwości obliczeniowych rozbitych na wiele miejsc obsługujących oprogramowanie. Mówi się, że „internet jest chmurą", ponieważ wszystkie operacje odbywają się nie tylko na sprzęcie i oprogramowaniu należącym do użytkownika, lecz również na serwerach. Współcześnie jednak o *cloud computing* mówi się w kontekście masowego przenoszenia i obsługi danych przez prywatnych dostawców, np. Google, Amazon czy Microsoft.



Rys.5. Schemat Cloud Computing. Usługi są dostarczane użytkownikom za pośrednictwem „chmury", tzn. dostępne są z serwerów dostawcy. Użytkownik nie posiada tym samym kontroli nad nimi, gdyż nie znajdują się na jego komputerze jak klasyczne oprogramowanie.
(Źródło Rys.: Wikimedia Commons, Cloud Computing)

Konto Google to konto, które po założeniu umożliwia dostęp do wielu usług Google wymagających logowania – od skrzynki pocztowej Gmail po serwisy zarządzania reklamą online Adwords. **Google Account** ma być rodzajem uwierzytelnienia i zarządzania tożsamością online. Z rosnącą popularnością różnych serwisów firmy Google, które często świetnie i mobilnie zastępują tradycyjne aplikacje desktopowe (instalowane na komputerze użytkownika) takie jak poczta e-mail, edytory dokumentów czy albumy ze zdjęciami, rosną zagrożenia danych w nich przechowywanych.

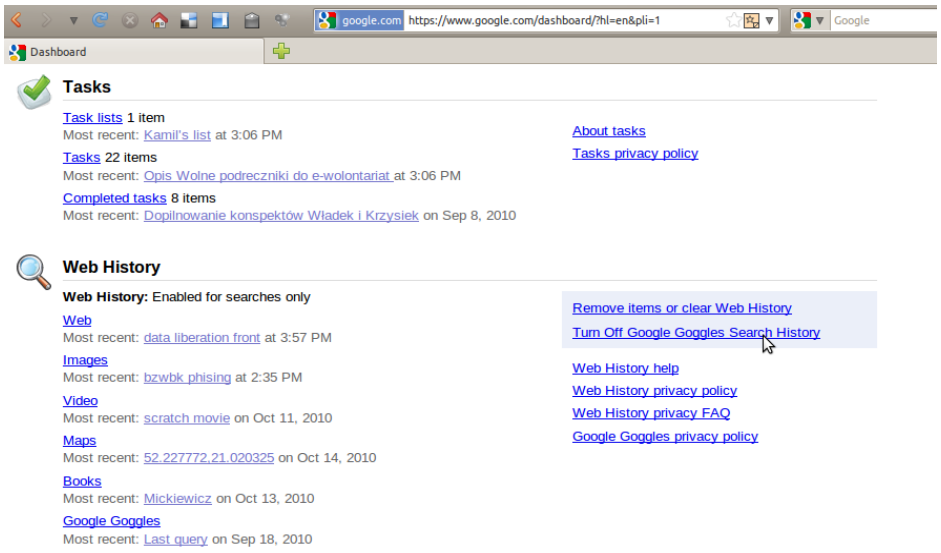
Podstawowym zagrożeniem jest brak kontroli nad naszymi danymi, które przechowywane są na serwerach dostawcy usługi, a nie na naszym komputerze, co daje nam możliwość korzystania z nich z różnych urządzeń, ale uniemożliwia w sytuacji braku dostępu do internetu albo...

zamknięcia serwisu. Jest to sytuacja, w której nie posiadamy żadnej kontroli (a często również żadnej instytucji pomocy). Ryzyko niosą ze sobą nie tylko problemy techniczne, np. awaria po stronie dostawcy, ale również warunki umów, na które się zgadzamy, np. braku odpowiedzialności dostawcy za ewentualne wycieki danych czy błędy, które mogą przykładowo usunąć lub zmienić nasze dane.

Podobnie jak w przypadku fragmentów umowy z serwisem YouTube musimy zwracać uwagę na zapisy w umowach każdego serwisu, w którym chcemy przechować lub udostępnić jakieś dane – szczególnie unikajmy publikowania informacji wrażliwych. Google, choć udostępnia użytkownikom wiele opcji dodatkowych zabezpieczeń, np. logowanie z potwierdzeniem innym kanałem (np. za pomocą smsa), jest równocześnie ogromnym dostawcą i jego najmniejszy błąd może dotknąć ogromnej rzeszy użytkowników, jak to zdarzyło się z Dokumentami Google. Jak wiele usług Google posiadają ustawienia prywatności, dzięki którym możemy udostępnić je np. znajomym na adres mailowy lub pod linkiem, lub nie udostępniać wcale.

USTAWIENIA GOOGLE

Jeśli jesteś użytkownikiem aplikacji Google, warto byś był świadom ich ustawień i potrafił je zmieniać. Google pozwala m.in. zarządzać historią Twoich wyszukiwań oraz działań w ich serwisach – dane te automatycznie są archiwizowane, ale możesz usunąć je za pomocą tzw. **Dashboard** (https://www.google.com/dashboard/).



Rys. 6. Google Dashboard. Widok historii autora wyszukiwania w serwisach Google – wyszukiwania miejsc na mapach, książek, obrazów czy video.

Jest to miejsce, w którym zebrane są wszystkie serwisy, z których korzystasz, ich ustawienia oraz opcje do zarządzania nimi, np. usuwanie historii wyszukiwania czy zmiany haseł. Po wejściu na Dashboard możesz zobaczyć, jak wiele danych o Tobie zebranych jest w jednym miejscu. Pomyśl, że ktoś, mając do nich dostęp, mógłby odtworzyć prawie całą Twoją działalność i Zycie w sieci. Musisz również pamiętać, że jeśli zalogujesz się do dowolnej usługi Google, Twoje pozostałe działania, np. wyszukiwanie za pomocą wyszukiwarki, są również zapamiętywane. Możesz to wyłączyć lub zawsze pamiętać o korzystaniu z osobnej przeglądarki dla czynności wymagających logowania, a osobnej do wyszukiwania i przeglądania zasobów sieci.

Jeśli jesteś użytkownikiem aplikacji „w chmurze", takich jak te oferowane przez Google, pamiętaj, że Twoje dane są tam narażone na wyciek lub naruszenie. Żeby ustrzec się przed takimi wypadkami, nigdy nie publikuj w takich serwisach danych wrażliwych, np. zdjęć, które powinny być dostępne jedynie dla Twoich bliskich lub ważnych danych w dokumentach. Takie informacje czy zdjęcia zawsze zamiast serwisu online możesz bezpieczniej przesłać mailem – ryzyko będzie mniejsze. Zawsze również rób kopię swoich dokumentów, prac czy zdjęć na dysku.

Google oferuje ważną z perspektywy bezpieczeństwa opcję – **Data Liberation Front** zostało uruchomione jako odpowiedź użytkownikom domagającym się możliwości „odzyskania" swoich danych i historii z serwerów Google. Jak pisaliśmy wcześniej, wiele umów i warunków korzystania z serwisów, na które się zgadzamy obejmuje przechowywanie naszych danych również po likwidacji naszych kont. Często oznacza to, że jeśli firma zdecyduje się na zamknięcie danej usługi przepadają wraz z nią nasze dane i informacje, które w niej umieściliśmy. Inną sytuacją jest brak możliwości przeniesienia naszych danych do innych serwisów lub programów. Data Liberation Front aktualnie wspiera 27 z najpopularniejszych usług Google. Na stronie znajdują się instrukcje, w jaki sposób wyeksportować swoje dane z tych serwisów lub jak je przywrócić.

WAŻNY LINK

Google Data Liberation Front **–** http://www.dataliberation.org/

Zadanie:

Znajdź w sieci informacje **o Facebook Social Graph** i **Google Social Circle** – dowiedz się czym są i w jaki sposób analizują dane o Tobie i innych użytkownikach. Oba projekty pozornie pozwalają nam lepiej zorientować się w informacjach naszych znajomych lub informacjach o nich, jednak równocześnie ujawniają dane i połączenia między nimi, których by sobie nie życzyli upubliczniać.

FACEBOOK (I NIE TYLKO)

Facebook i wiele innych serwisów społecznościowych powstałych w ciągu ostatnich kilku lat to domena ludzi młodych. Internet jest dla Was środowiskiem naturalnym, dlatego mówi się o Was żartobliwie „cyfrowi tubylcy". Ucząc się, jak być bezpiecznym w sieci i w jej najmodniejszych aktualnie miejscach, warto pomyśleć o przekazywaniu tej wiedzy dalej. Pamiętajcie, że ucząc się, możecie również uczyć swoich kolegów oraz dorosłych. To kolejny ważny punkt na mapie Kodeksu 2.0.

Pięć wskazówek używania wszelkich Serwisów Społecznościowych (Social Network's):

1. Zacznij od wybrania ustawień prywatności i bezpieczeństwa, wybierz złożone / unikalne hasła dla konta.
2. Bądź ostrożny podczas instalacji aplikacji innych firm. Nie instaluj aplikacji ze źródeł, którym nie ufasz.
3. Przyjmuj zaproszenia wyłącznie od ludzi, których znasz.
4. Zapoznaj się z polityką prywatności i warunkami korzystania z usługi uważnie. Ogranicz ilość informacji osobistych, do których usługa może mieć dostęp.
5. Pisz i publikuj odpowiedzialnie. Zawsze pamiętaj, że wszystkie informacje, zdjęcia, filmy staną się publiczne.

Najważniejsze fakty o (nie)bezpieczeństwie Facebooka:

- Informacje o Tobie i Twoich działaniach są dystrybuowane do zewnętrznych firm (np. reklamodawców lub operatorów gier online).
- Ustawienia prywatności automatycznie zmieniają się na mniej restrykcyjne podczas dużych zmian w serwisie (np. dodania nowych funkcjonalności).
- Reklamy na Facebooku mogą zwierać złośliwe oprogramowanie (malware).
- Twoi znajomi nieświadomie mogą również narażać Cię na niebezpieczeństwa (*Twoja ochrona jest tak dobra, jak ochrona twoich znajomych.* Jeśli ktoś z Twoich znajomych ma słabe hasło, które zostanie złamane, ktoś może rozesłać przez jego konto spam lub złośliwe oprogramowanie).
- Za wieloma fałszywymi profilami czają się prawdziwi oszuści...

PODSTAWOWE USTAWIENIA PRYWATNOŚCI NA FACEBOOKU

Facebook w ciągu 6 lat działalności zgromadził już grupę ponad 500 milionów użytkowników (szacuje się, że globalnie Internet ma ok 2 mld. użytkowników). Nie osiągnął tego żaden inny serwis internetowy. Według firmy Alexa zajmującej się statystykami największych stron i firm internetowych Facebook jest drugim po Google serwisem internetowym. Żaden inny serwis nie wzbudzał też tak wielu kontrowersji i obaw użytkowników o ochronę ich prywatności, danych osobowych i bezpieczeństwa. Facebook, co bardzo ważne, podkreśla sens dzielenia się informacjami przez użytkowników z ich znajomymi, z serwisem i reklamodawcami, równocześnie zaznaczając, że udostępnia swoim użytkownikom pełną kontrolę nad ich prywatnością.

Zanim przejdziemy do ustawień prywatności, zwróć uwagę na to, że są to jedynie ustawienie techniczne, które nigdy nie będą doskonałe. Umieszczenie informacji lub zdjęcia nawet z najbardziej restrykcyjnymi ustawieniami prywatności nie zabezpiecza nas przed tym, że ktoś z naszych znajomych może te dane skopiować i opublikować bez naszej zgody i wiedzy. Zabezpieczenia prywatności nie zabezpieczają nas przed sytuacją włamania na nasze konto – o którego ochronę (siłę hasła, jego zmiany) powinniśmy dbać szczególnie (w każdym serwisie). Żadne zabezpieczania serwisów, z których korzystamy, nie pozwolą też uniknąć problemu braku kontroli nad siecią, z której korzystamy – treści, których nie szyfrujemy zawsze mogą wpaść w niepowołane ręce. Zabezpieczenie takie jak w serwisie Facebook to jedynie ograniczenia w bezpośredniej dostępności tych danych dla innych użytkowników serwisu.

Poniżej znajdziesz dokładny poradnik tego, gdzie i jak spersonalizować swoje ustawiania prywatności. Pamiętaj, aby sprawdzać co jakiś czas (zwłaszcza gdy cały serwis ulega aktualizacji) czy nie zostały zmienione bez Twojej wiedzy.

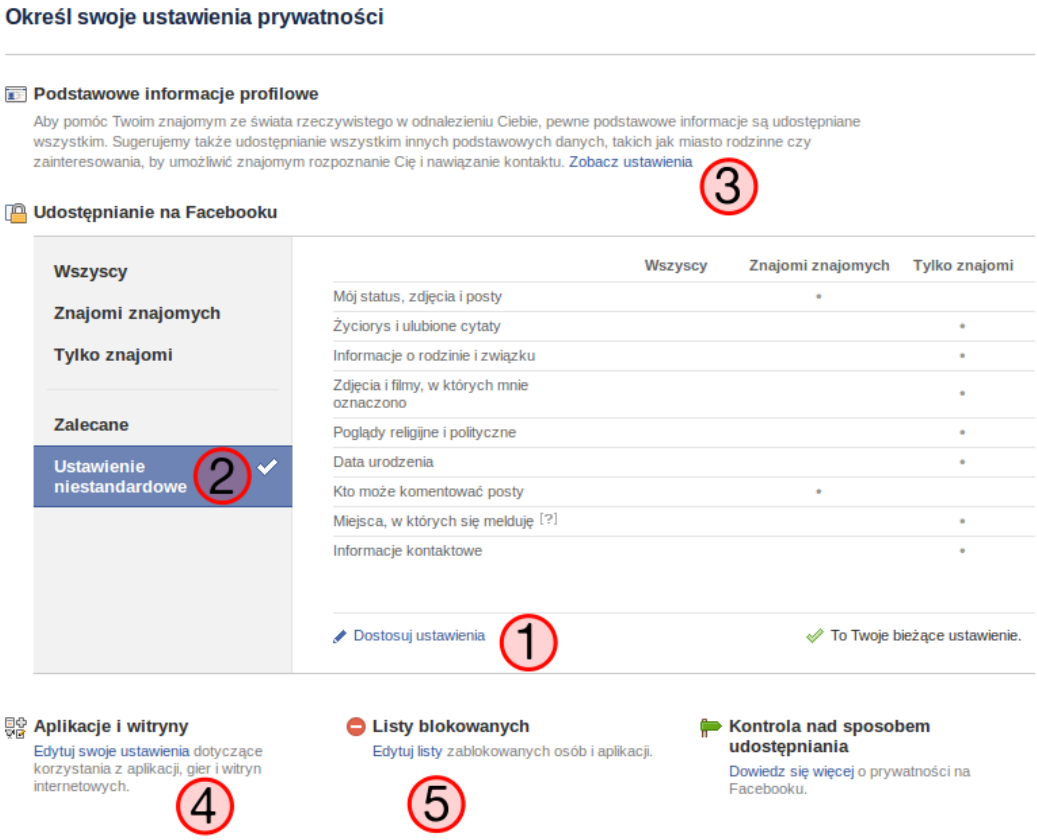
O ustawieniach prywatności możesz pomyśleć jak o relacjach między znajomymi w szkole. Nie wszystkim mówisz o swoich perypetiach miłosnych, a tylko bardzo bliskim osobom o Twoich osobistych lub domowych problemach. To naturalne, ponieważ od osób, którym ufamy oczekujemy nie tylko zrozumienia i pomocy, ale również zachowania dyskrecji. Bycie z kimś w klasie przez kilka lat nie gwarantuje, że ta osoba nawet, gdy obieca nam, że „nic nikomu nie powie", nie opowie o tym komuś innemu, wierząc w jego dyskrecję. Podobnie ustawienia prywatności w serwisach społecznościowych – obiecują, że nie pokażą Twoich informacji nikomu poza Twoimi znajomymi, ale dla Ciebie najważniejsze powinno być, czy Twoi znajomi na pewno również pozostaną dyskretni lub czy do ich konta (lub pamiętnika) nie ma dostępu ktoś trzeci. W ten sposób „wyciekają" ważne informacje zarówno w szkole, jak i życiu dorosłych osób.

Serwisy społecznościowe dzięki swojej prostocie i szybkości działania są niezwykle niebezpieczne dla wszelkich wrażliwych informacji. Jeśli w szkole wiele osób będzie wiedzieć o jakimś przykrym i być może dla innych brzmiącym zabawnie wydarzeniu, bardzo łatwo może to zmienić się w nieprzyjemną plotkę lub przezwisko. Każdy, kto chodził lub nadal chodzi do szkoły, wie jak takie rzeczy potrafią się „ciągnąć" i, co gorsza, jak trudno je zmienić. W internecie jest jeszcze gorzej. Raz upubliczniona informacja nie tylko bardzo łatwo i szybko może się rozprzestrzenić, np. Twoje zdjęcie, na którym próbujesz zapalić papierosa, ale również nie będziesz miał możliwości takiej informacji czy zdjęcia kontrolować lub usunąć. Dlatego niezależnie od dalszego negatywnego stosunku do palenia to zdjęcie pozostanie w sieci i w każdej chwili ktoś będzie mógł o tym przypomnieć.

Zadanie:

Zbadaj zmiany ustawień prywatności, jakie wprowadzał Facebook na przestrzeni ostatnich lat. Zastanów się, jakie elementy umieszczone na nim na początku istnienia serwisu, np. zdjęcia – które były początkowo prywatne, wg zmian ustawień zostałyby upublicznione automatycznie przez serwis.

Krok po kroku:



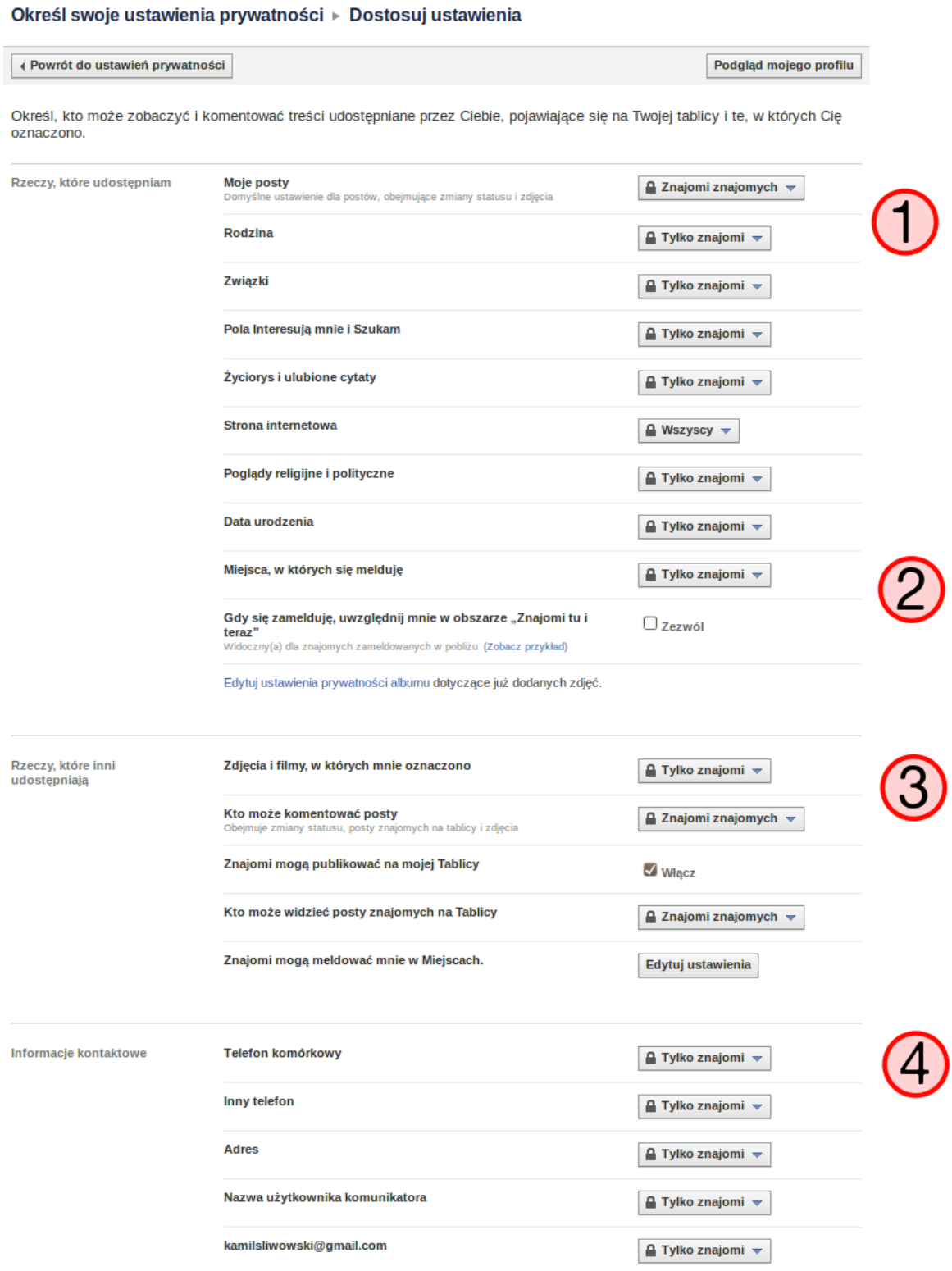
Rys.7. Ustawienia prywatności

1-2. Po wejściu w *Ustawienia prywatności* zobaczysz domyślnie wybrane *Zalecane* – możesz zmienić je dzięki opcji *Dostosuj ustawienia* (Rys. 8). Po ich zmianie będą widnieć jako *Ustawienia niestandardowe*.

3. Podstawowe informacje profilowe – czyli to kto może Cie wyszukiwać, kontaktować się z Tobą oraz widzieć podstawowe informacje o Tobie, np. miejsce pracy czy listę Twoich znajomych (szczegółowo opisane w Rys. 8).

4. *Aplikacje i witryny* – tu możesz zarządzać aplikacjami, których używasz oraz sprawdzić i zmienić ich ustawienia (rys. 10.).

5. *Listy blokowanych* pozwalają zarządzać Ci dostępem do danych o Tobie wybranym użytkownikom serwisu (Rys. 8).



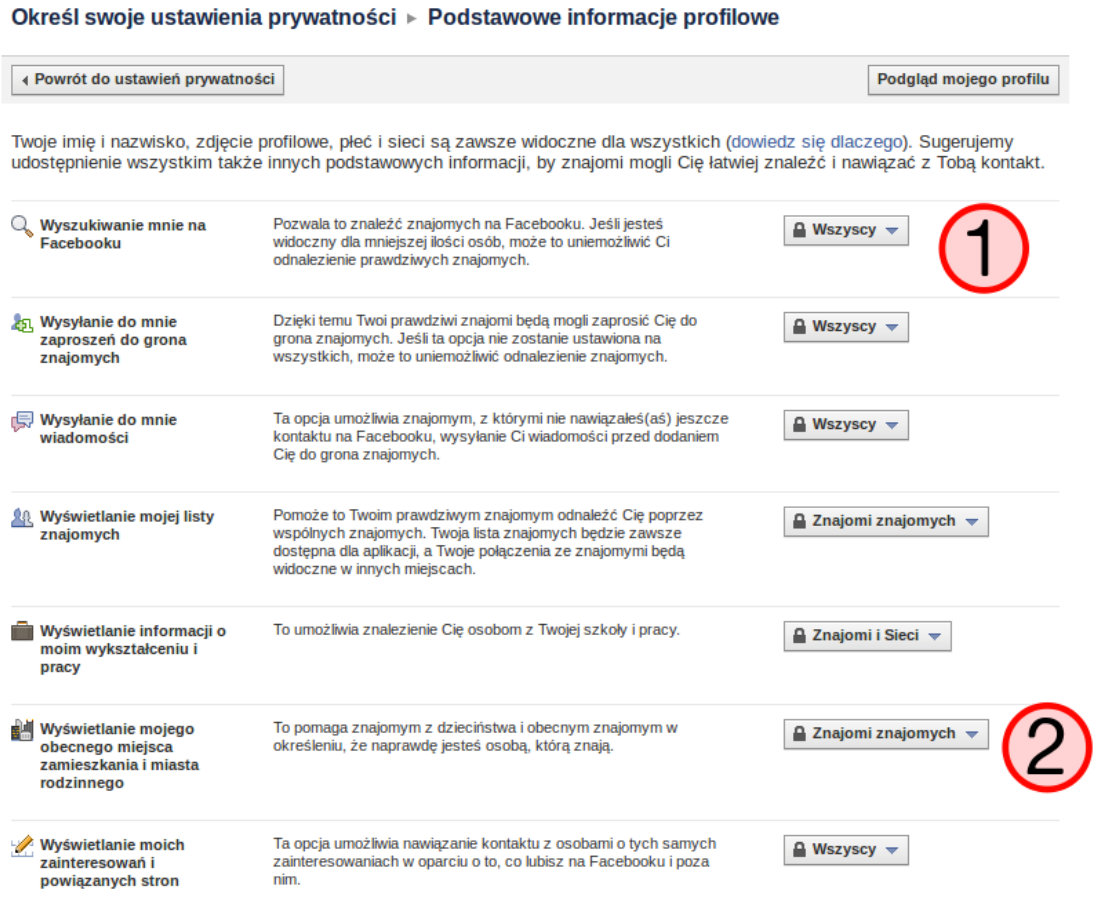
Rys. 8. Dostosuj ustawienia prywatności

1. *Moje posty.* Zwróć uwagę na to, komu chcesz pokazywać treść postów. Być może te informacje powinny być dostępne tylko Twoim znajomym.

2. Miejsca to nowa usługa, która pozwala publikować automatyczne informacje o tym, gdzie się znajdujesz. Niesie ze sobą szczególne ryzyko, np. upublicznienie informacji o tym, że w tym momencie jesteś daleko od domu, może zachęcić potencjalnych złodziei.

3. *Rzeczy, które inni udostępniają* – ogranicz możliwość tagowania zdjęć, na których się znajdujesz, oraz możliwości komentowania i publikowania na Twojej tablicy innym użytkownikom.

4. Odpowiednio do potrzeb ogranicz swoje *informacje kontaktowe*, pamiętaj, że publikując ich zbyt wiele, narażasz nie tylko swoją prywatność, ale i bezpieczeństwo.



Rys. 9. Podstawowe informacje profilowe

1. *Wyszukiwanie* na Facebooku – tu możesz określić, dla kogo (znajomych, znajomych znajomych, sieci etc.) twój profil będzie wyszukiwalny.

2. Zwróć uwagę na to, jakie elementy Twojego profilu mają być widoczne dla osób innych niż Twoi znajomi.

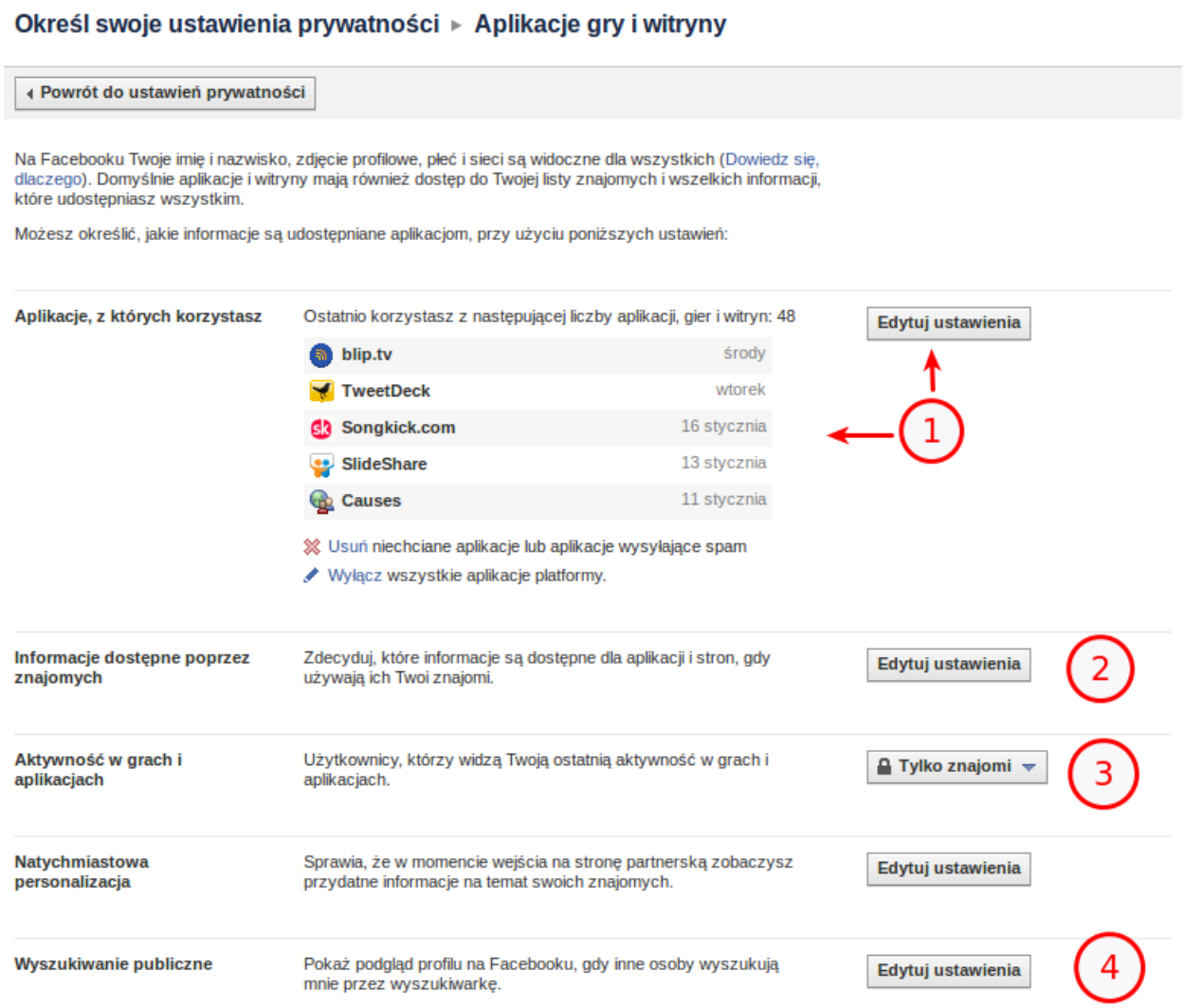
APLIKACJE I WITRYNY

Po przejściu z głównego panelu *Ustawień Prywatności* (rys. 7, pozycja nr 4) znajdziemy się w panelu umożliwiającym przegląd aplikacji, ich usuwanie oraz konfigurację sposobu ich działania na naszym profilu.

Różne aplikacje wymagają różnego zakresu dostępu do Twoich danych, aby działać. Wiele aplikacji, takich jak gry Farmville czy Mafia Wars (firmy Zynga), posiadają osobne regulaminy. Są one często znacznie większym zagrożeniem dla naszej prywatności od regulaminu samego serwisu. Gry takie jak Farmville wymagają m.in. dostępu do naszych danych osobowych i treści umieszczanych na profilu, natomiast regulamin korzystania z nich daje firmie obsługującej grę m.in. możliwość dostępu do tych danych i ewentualnego przekazywania ich/sprzedawania kolejnym firmom. W przeciwieństwie do Facebooka te firmy nie zastrzegają anonimizacji danych i udostępniania jedynie profili statystycznych, co oznacza, że mogą również sprzedawać reklamodawcom nasze indywidualne dane. Ustawienia gry firmy Zynga nie oferują żadnych opcji ograniczających działanie tej aplikacji na naszym profilu lub ilości informacji, do których będzie mieć dostęp.

Rys.10. Informacje dostępne poprzez znajomych. Domyślnie wiele z nich jest udostępniane, dlatego zalecane jest wyłącznie wszystkich opcji.

Rys. 11. Aplikacje gry i strony internetowe



1. Widok *Z czego korzystasz* pozwala na szybkie usunięcie poszczególnych aplikacji lub wyłączenie całkowicie platformy aplikacji – jest to opcja, która uniemożliwi również widok naszych danych dla aplikacji używanych przez naszych znajomych. To nie jest pełna lista! Kliknij na Edytuj ustawiania aby zobaczyć całość.

2. *Informacje dostępne poprzez znajomych* (zob. rys. 10.) – aplikacje, których używają Twoi znajomi, również mają dostęp do Twoich danych; tutaj możesz ograniczyć do jakich, a aby uniknąć takiej niezależnej wymiany naszych danych możemy całkowicie wyłączyć aplikacje platformy (pkt. 1).

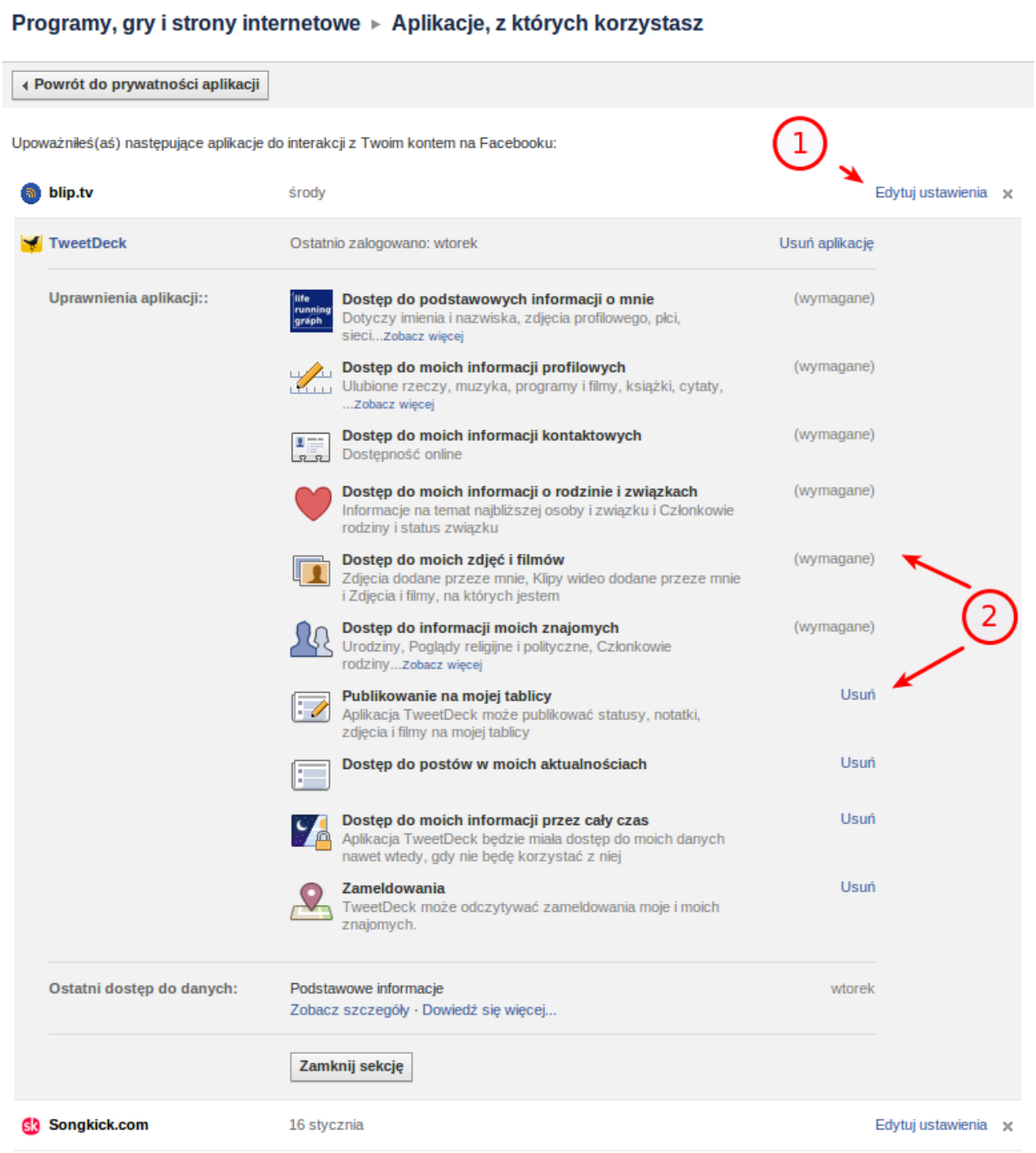
3. Naszą *aktywność w grach i aplikacjach* możemy określić jako widoczną dla różnych grup użytkowników.

4. *Wyszukiwanie publiczne* – ważne ustawienie, w którym możemy określić, jak i czy w ogóle nasz profil może być wyszukiwany przez zewnętrzne wobec Facebooka wyszukiwarki, np. Google.com .

EDYCJA USTAWIEŃ POSZCZEGÓLNYCH APLIKACJI

Rys.12. Zapytanie o uprawnienia dla aplikacji. Zwróć uwagę, że powyższa aplikacja będzie mieć dostęp do takich danych, jak Twój adres, data urodzenia. Dodatkowo polityka prywatności firmy obsługującej grę mówi o zastrzeżeniu sobie przez nią opcji redystrybucji tych danych innym firmom.

Ta sekcja (zob. rys. 13) pokazuje zainstalowane aplikacje, których używasz lub na których instalację się zgodziłeś. Można usunąć te aplikacje. W przypadku wyłączenia platformy, będziesz odłączony od wszystkich aplikacji i stron internetowych, którym wcześniej dasz na to zezwolenie (np. jeśli używasz aplikacji Blip.pl publikującej na Facebooku statusy z Blip.pl, po wyłączeniu aplikacji to połączenie i informacje przestaną działać). Będzie to również skutkować usunięciem wszystkich danych z aplikacji i ustawień związanych z tymi aplikacjami.



Rys.13. Ustawienia aplikacji – edycja. (Konto →Ustawienia prywatności→Aplikacje i witryny→Aplikacje, z których korzystasz (Edytuj ustawienia)

1. Każda aplikacja posiada ustawienia, które możemy edytować; ich opcje zależą od tego, jak zdefiniował je autor.

2. *Edycja ustawień aplikacji*. Przyjazne aplikacje zwykle pozwalają na wyłączenie widoczności dla nich naszych danych oraz powiadamiania nas lub naszych znajomych o każdym użyciu aplikacji. Takie aplikacje jak gry firmy Zynga nie posiadają żadnych ustawień – wykorzystując je, zgadzamy się na zupełny brak kontroli naszych danych oraz ich działania na naszym profilu i profilach naszych znajomych.

USUWANIE KONTA

W przypadku facebooka mamy dwie możliwości uwolnienia się od serwisu: **dezaktywacji i usunięcia konta** (co ciekawe, ta druga opcja dostępna jest od niedawna dzięki silnym naciskom użytkowników). Dezaktywacja konta powoduje, że profil użytkownika i wszystkie związane z nim informacje natychmiast staną się niedostępne dla innych użytkowników Facebooka, natomiast informacje o profilu (wraz z listami znajomych, zdjęciami, informacjami o zainteresowaniach itp.) zostaną zachowane, co umożliwia przywrócenie konta w przyszłości, ale równocześnie stałe wykorzystywanie tych danych przez serwis. W przypadku trwałego usunięcia konta wszystkie powiązane z nim dane osobowe zostają usunięte z baz danych seriwsu. O czym warto wiedzieć – w warunkach usuwania konta Facebook ostrzega „Kopie niektórych materiałów (zdjęć, notatek itp.) mogą pozostać na naszych serwerach z powodów technicznych, ale będą one całkowicie niedostępne dla innych użytkowników".

1. Aby dokonać **dezaktywacji konta** wejdź w opcję *Ustawienia konta*, na samym dole znajdziesz opcję dezaktywacji. Dezaktywacja konta spowoduje usunięcie profilu oraz całej powiązanej zawartości Twojego konta. Inni użytkownicy nie będą mogli Cię wyszukiwać w serwisie, ani przeglądać Twoich danych. Dane te jednak pozostaną na serwerach Facebooka.

2. Jeśli chcemy **usunąć konto**, Facebook nie ułatwia nam zadania. Opcja ta ukryta jest w liście przydatnych pytań i odpowiedzi *Centrum Pomocy* w dziale *Prywatność*. Tam znajdziemy pytanie „Jak trwale usunąć konto na Facebooku?" W odpowiedzi na nie znajduje się link służący do zgłoszenia chęci usunięcia konta. Prawda, że skomplikowane? A to nie koniec! Po zgłoszeniu chęci usunięcia konta za pomocą linka, musimy jeszcze otrzymać potwierdzenie od automatu, który może całą sprawę opóźnić. Ważne jest, żeby nie wylogowywać się z Facebooka, póki nie dostaniemy potwierdzenia usunięcia konta. W przeciwnym razie usuwanie konta zostanie anulowane i będziemy musieli powtórzyć całą operację.

Zadania:

1. Zapoznaj się z regulaminem serwisów społecznościowych, z których korzystasz (lub jeśli nie korzystasz, z regulaminem Naszej Klasy i Facebook.com), wypisz z nich elementy i stwierdzenia, które, jeśli tak uważasz, zagrażają Twojemu bezpieczeństwu lub prywatności. Zaproponuj lepsze rozwiązania.

2. Jeśli korzystacie z serwisów społecznościowych dla próby oceńcie wzajemnie swoje ustawienia prywatności – zmieniając je, sprawdźcie również, co można na nich znaleźć przez wyszukiwarki? Ile jesteście w stanie znaleźć informacji o sobie nawzajem?