Marcelina Czyż
Fizyka

Zagrożenia prywatności

W dobie komputerów jesteśmy narażeni na utratę prywatności z wielu stron, w szczególności ze strony Internetu. W niniejszej pracy wspomnę tylko o kilku możliwych zagrożeniach prywatności związanych z Internetem.

Dane osobowe

W ostatnich latach powstało w Internecie wiele stron typu „społeczność internetowa" (takich jak www.myspace.com, www.grono.net czy www.nasza-klasa.pl), zamkniętych forów dyskusyjnych, społeczności związanych z konkretną tematyką. Z tych serwisów korzystają miliony ludzi na całym świecie i niestety bardzo niewielu z nich zdaje sobie sprawę z tego, że może to stanowić dla nich zagrożenie prywatności.

Otóż rejestrując się na tego typu portalach (i wielu innych) jesteśmy proszeni o podanie danych osobowych. Często podajemy je dobrowolnie bo wymagany jest jedynie e-mail i login. Twórcy portali namawiają jednak aby podać więcej danych takich jak nazwisko, data urodzin, telefon, nr Skype, nr GG – tłumaczy się to tym, że np. inni użytkownicy będą mogli nas łatwiej odnaleźć. Wielu internatów podaje chętnie kompletne dane. Natomiast niewielu zastanawia się nad ewentualnymi konsekwencjami.

Sam fakt udostępniania danych budzi wątpliwości, w końcu każdy może je przeglądać. Na podstawie tych danych można wnioskować hasło do poczty/konta bankowego (wiele osób ma zbyt oczywiste hasła typu data urodzin, numer telefonu). Również zdjęcia często zawierają cenne informacje, których czasem powinniśmy chronić, a nie zdajemy sobie z tego sprawy[1]. Tego typu możliwe następstwa można mnożyć bez końca.

Inna konsekwencja, która występuje po podaniu e-maila to sprawa spamu. Można być niemal pewnym, że naszą skrzynkę pocztową zasypie niechciana korespondencja. A najczęściej trzeba się zgodzić na przetwarzanie danych w celach marketingowych bo inaczej konto nie zostanie utworzone…

Również bezpieczeństwo naszych danych podlega wątpliwościom. Dane często są narażone na ataki hackerów – portale często powstają w krótkim czasie i w pośpiechu, jednocześnie zaniedbując sprawy bezpieczeństwa. Ale nawet jeżeli GIODO[2] stwierdzi, że w tym czy innym portalu dane są bezpieczne to nie wiemy czy jakiś administrator nie sprzeda co jakiś czas kilku tysięcy danych osobowych (koncepcja sprzedania danych jest mocno kusząca, szczególnie biorąc pod uwagę, że na czarnym rynku za jeden rekord można otrzymać 1-5 zł).

Takie zagrożenia prywatności jak powyżej są ewidentnie związane z nieuwagą i beztroską internautów, ale dalsze przykłady o jakich chciałabym wspomnieć nie już takie proste do przewidzenia.

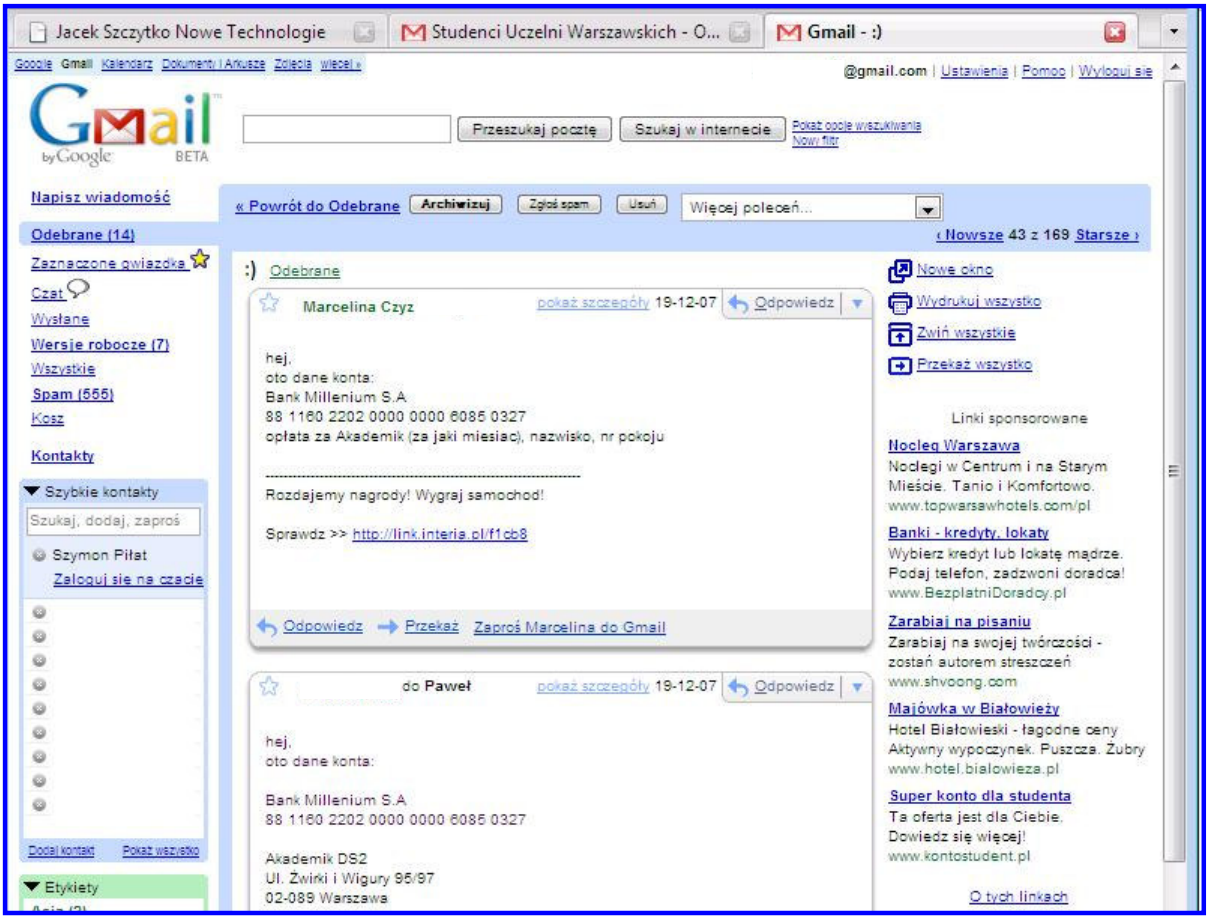
[1] Przykład: zdemaskowani tajniacy wskutek zamieszczenia zdjecia klasowego ze szkoły policyjnej na portalu www.nasza-klasa.pl
[2] Głowny Inspektor Ochrony Danych Osobowych

Gmail

Poczta, którą udostępnia Google jest nieporównywalnie lepsza od wszystkich darmowych i większości płatnych kont pocztowych (konto ma pojemność kilkukrotnie większą niż inne, (podobno) najlepsze filtry antyspamowe, brak graficznych reklam, najszybsze serwery na świecie). Czy ktoś się czasem zastanawia nad tym dlaczego Google daje nam za darmo coś co powinno kosztować krocie?

Jedna odpowiedź jest oczywista: Google wyświetla reklamy, na których zarabia. Ale jakie to są reklamy! Na rysunku nr 1 widoczny jest zrzut ekranowy z poczty Gmail. Wiadomość wysłana przeze mnie zawiera informacje o sposobie przelewania należności za akademik. A reklamy? Są idealnie dopasowane do treści e-maila i do profilu mojego odbiorcy. W reklamach występują np. słowa „student", „bankowość". To nie przypadek.

System poczty Gmail analizuje e-maile i wyświetla reklamy dopasowane do użytkownika. Jest to w pewnym sensie utrata prywatności bo ktoś lub coś analizuje naszą korespondencję. A treść reklam nie zależy tylko od tego co zawiera e-mail – zależy również od wszystkich pozostałych e-maili użytkownika.



Inaczej mówią Google na podstawie zawartości e-maili tworzy profil każdego użytkownika i przesyła mu reklamy o odpowiednich treściach. Taki profil może być bardzo trafny w przypadku kiedy użytkownik korzysta również innych usług Googla w ramach jednego konta, np.. Google Docs, Google Analytics, Google Sitemaps i wiele, wiele innych. System Google'a analizuje wszystkie dane pochodzące ze wszystkich

usług i przesyła do nas reklamy dobrze dopasowane do tego co robimy i co nas interesuje. Np. jeżeli Google nie potrafi dopasować reklam do konkretnej wiadomości e-mail (bo np. jest zbyt krótka) to wyświetla reklamy pasujące do całej pozostałej korespondencji.

Co więcej, ciasteczka, Googla (kontrowersyjne z wielu względów) pozwalają przeglądarce na dopasowywanie nie tylko reklam, ale również wyników wyszukiwania! Niejednokrotnie wyniki przeszukiwania sieci dla jakichś słów kluczowych będą inne niż te, które dostanie nasz kolega/koleżanka dla tych samych słów kluczowych! Google personalizuje wyniki wyszukiwania biorąc pod uwagę adres IP – nawet usuwanie ciasteczek niewiele daje. Poza tym, że wyszukiwarka narusza naszą prywatność (poprzez analizę naszych maili i zachowań w sieci) to pod znakiem zapytania staje obiektywność wyników wyszukiwania (co rodzi dalsze pytania, np. czym jest „prawda" w Internecie – czyżby dla każdego „prawda" była inna?).

Sklepy internetowe

Trochę bardziej futurystyczne są systemy, które mają korzystać z ciasteczek (cookies), informacji przesyłanych pocztą, informacji o numerze komórkowym właściciela, informacji o jego lokalizacji (miasto, dzielnica) i może jeszcze innych informacji. System taki wiedziałby, że użytkownik poszukiwał w Internecie informacji o np. brązowym krawacie. Później będąc w centrum handlowym obsługa sklepu, w którym robimy zakupy jest informowana, że pojawił się użytkownik, który w ich sklepie on-line poszukiwał brązowego krawata. Mogą oni od razu zareagować, podejść do klienta i zaproponować pomoc w odnalezieniu krawata, którego szuka. Jest to w oczywisty sposób bardzo daleko idące naruszenie prywatności. Inny przykład spokrewniony z powyższym to śledzenie toru osób robiących zakupy w sklepie. Technicznie jest to wykonalne za pomocą śledzenia sygnału GSM z telefonów komórkowych. Analiza szczegółowej mapy tego jak poruszają się po sklepie klienci/klientki pozwala poznać upodobania klientów i można np. dużo efektywniej rozmieszczać towary na terenie sklepu. Można na to patrzeć jak na przedmiotowe traktowanie ludzi: towary ustawia się w określonej kolejności, z odpowiednimi cenami i w tak obliczony sposób, żebyśmy coś w końcu kupili. Takie systemy wprowadza *podobno* brytyjska sieć sklepów Marks & Spencer.

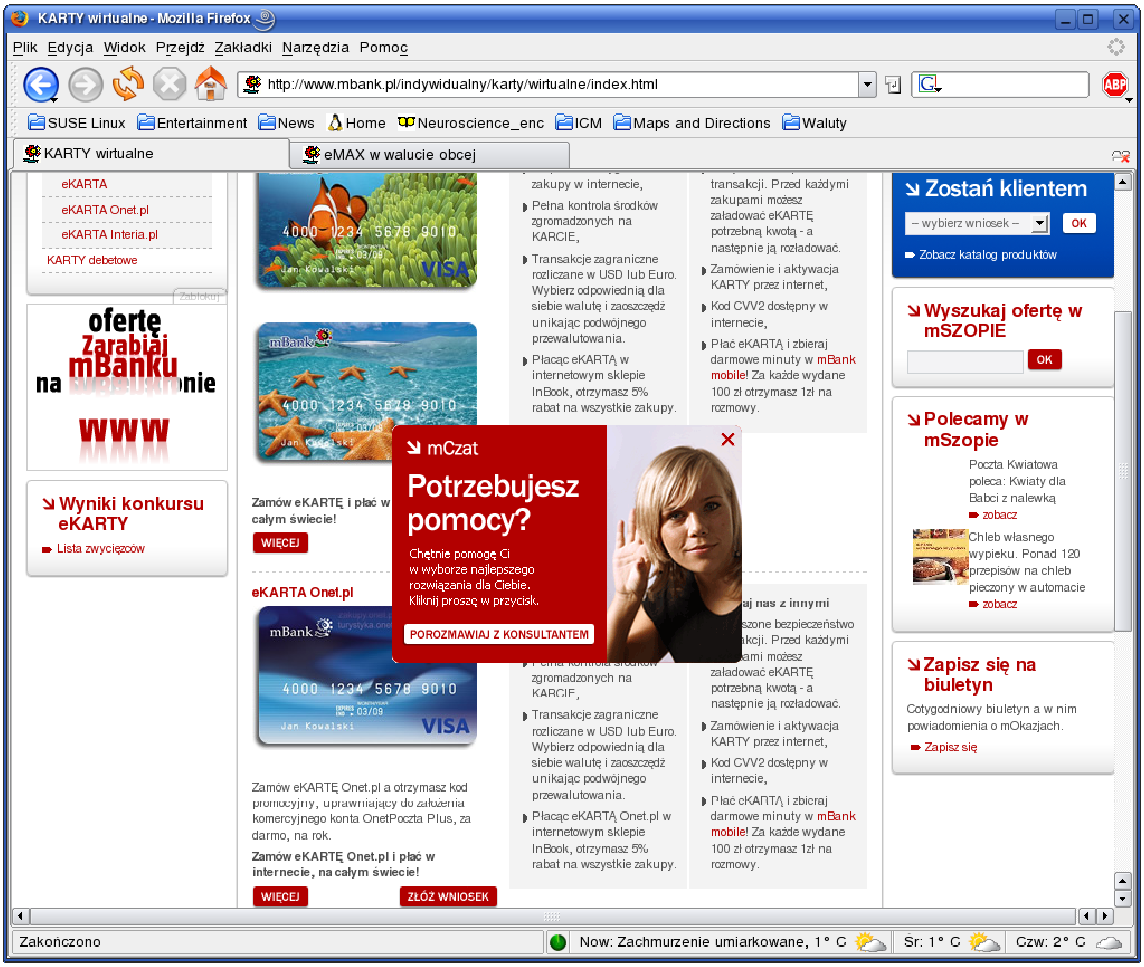
Inna forma ingerencji w prywatność przejawia się podczas zakupów w Internecie. W zależności od tego jak użytkownik porusza się po stronie WWW, czy długo rozważa zakup biletu, jak wiele razy odwiedza stronę przed zakupem wpływa na cenę produktu, którą pokaże mu system. Polega to oczywiście na przechowywaniu informacji o użytkowniku na serwerach sklepu. Użytkownika identyfikuję się za pomocą ciasteczek, adresu IP, lokalizacji. Banalny przykład jest taki że czasem samo ustawienie innego języka interfejsu WWW skutkuje wyświetlaniem się innych cen.

Oczywiście wiedząc o tym można to wykorzystać na swoją korzyść, jednak najczęściej tego typu systemy obracają się przeciwko nam.

Pewien przejaw zagrożenia prywatności w Internecie, o jakim wspomnę ma miejsce również w sklepach internetowych. Zjawisko to polega na tym, że przeglądając sklep internetowy czasem włącza się okno czatu, w którym pracownik sklepu doradza jak odnaleźć w sklepie produkt, którego szukamy. Pracownicy zostają poinformowani przez system o tym, że użytkownik kilkukrotnie korzystał z wyszukiwarki i najprawdopodobniej nie odnalazł poszukiwanego przez siebie produktu. Wiedząc co użytkownik wpisywał w wyszukiwarkę pracownik szybko może

pomóc odnaleźć produkt. Pracownicy sklepów mogą również śledzić w jaki sposób klienci poruszają się po sklepie i również wyciągać z tego odpowiednie wnioski.

Podobne zjawisko jak powyżej zdarza się np. na stronach mBanku. Na zamieszczonym zrzucie ekranowym widać okienko typu pop-up, które otwiera się po kilku minutach przeglądania oferty dotyczącej kart płatniczych. Okienko pojawia się w różnych sytuacjach – nie można jednoznacznie stwierdzić czy działa tutaj mechanizm taki jak opisany powyżej, ale z pewnością zakłóca spokój podczas przeglądania, co w moim przekonaniu jest naruszeniem prywatności.



Wspomniane przykłady dotyczą jedynie kilku sfer gdzie nasza prywatność jest zagrożona. Widać jednak tendencję do coraz powszechniejszego udostępniania swoich danych. Generuje to oczywiście coraz więcej możliwości przechwycenia tych danych i wykorzystania przeciwko ich właścicielowi (podszywanie się, kradzieże tożsamości). Ponadto strony internetowe przechowują informacje o nas i „uczą się" jak lepiej sprzedać nam produkt.

Zapewne zmierza to w kierunku budzącym obawy. Dlatego coraz ważniejsza jest świadomość w tym zakresie i tym samym możliwość przeciwdziałania utraty naszej prywatności.

Inspiracja do napisania pracy została zaczerpnięta z wykładu profesora Włodzimierza Gogołka na temat promocji w Internecie i związanej z tym potencjalnej ochrony prywatności z punktu widzenia użytkownika (lipiec 2006, PAN).