

# BEZPIECZNE SURFOWANIE

Michał „Cihy” Cichocki

Nazywam się Michał Cichocki, z sieci Internet korzystam niemal pięć lat. W miarę upływu czasu moja czujność, jeśli chodzi o bezpieczeństwo w Internecie stawała się coraz większa. Od pewnego czasu interesuje się zachowaniami ludzi, związanymi z bezpiecznym poruszaniem się po stronach WWW. Przeprowadziłem dwa eksperymenty, które skłoniły mnie do napisania tego ebooka, a także stworzenia strony <http://www.bezpieczne-surfowanie.pl>, która ma być pewnego rodzaju kampanią reklamową, na rzecz bezpiecznego surfowania w sieci. Byłem głęboko poruszony beztróskim podejściem do spraw bezpieczeństwa młodych użytkowników Internetu, dla których właściwie słowo „bezpieczeństwo” nie występuje.

Zapraszam do lektury.

*Data 12 lipca 2007r.*

*Ebook Bezpieczne Surfowanie jak i jego reklama stanowią przedmiot praw autorskich i podlegają ochronie zgodnie z ustawą z dn. 04.02.1994r. o prawie autorskim i prawach pokrewnych (Dz. U. nr 24 poz.93) oraz ochronie z ustawy z dn. 08.06.1993r. o zwalczaniu nieuczciwej konkurencji (Dz. U. nr. 47 poz. 211). Rozpowszechnianie ebooka bez zgody jego autora jest zabronione.*

*Zabronione są jakiegokolwiek zmiany w zawartości publikacji bez pisemnej zgody autora.*

*Wszelkie prawa zastrzeżone.*

*All rights reserved.*

Miło mi, że zainteresowałeś się moją książką, a także cieszy mnie to, że zaciekały Cię aspekty bezpiecznego surfowania w Internecie.

Z książki dowiesz się jak ważną rzeczą jest Twoje hasło. Postaram się uświadomić Ci, że hasło jest wirtualnym kluczem do Twojego mieszkania, dlatego trzeba strzec go jak oka w głowie. Zobaczysz ile danych osobowych nieświadomie zostawiasz po sobie, wędrując po stronach WWW, wypowiadając się na forach internetowych, wpisując się do ksiąg gości, czy rejestrując się w serwisach społecznościowych lub randkowych.

Zajmę się również pojęciem anonimowości w Internecie, której w rzeczywistości nie ma. Na każdym kroku informacje o nas są zapisywane na serwerach, które później mogą zostać wykorzystane przez władze państwowe, lecz nie tylko – sprawny informatyk dotrze do tych danych.

Poznasz również sposób na tworzenie bezpiecznego i w miarę prostego do zapamiętania hasła. Hasło jest bardzo ważnym narzędziem w Internecie. Im bardziej jest skomplikowane, tym mniejsze prawdopodobieństwo, że zostanie przez kogoś złamane. Chociaż poważne serwisy internetowe wprowadzają masę zabezpieczeń przed niepowołanymi dostęпами do czyichś kont, nie zaszkodzi na własną rękę zwiększyć swoje bezpieczeństwo.

Wyrażam głęboką nadzieję, że po przeczytaniu tej książki staniesz się znacznie ostrożniejszy. Poniżej podane eksperymenty były przeprowadzane przeze mnie w rzeczywistości i dane statystyczne, jakie podałem również są realne.

Wielu użytkowników, w większości tych młodych przekonana jest, że siadając przed monitorem jest anonimowa. Pisząc posty na forum, logując się na pocztę, czy do niemal każdego innego serwisu internetowego zostawiasz po sobie ślad, jakim jest adres IP. O tym zapewne już słyszałeś. Po adresie IP można dotrzeć do Twojego miejsca zamieszkania; informacje takie mogą uzyskać osoby do tego uprawnione, choćby policja. Teraz już wiesz, że pisząc coś na forum, co jest niezgodne z prawem, mogą zapukać do Ciebie panowie w niebieskich mundurach... Jednak nie o tym chciałem.

Logując się do sieci WWW nie jesteś anonimowy, mimo to, Twoich danych osobowych nie pozna zwykły użytkownik Internetu – taki jak Ty. Jak pisałem wyżej do poznania danych potrzebne są uprawnienia. Przeciętny użytkownik z Twojego adresu IP może, w sprzyjających warunkach dowiedzieć się, z jakiego miasta pochodzisz. To oczywiście ciekawa i przydatna informacja, jednak bez dalszych wiadomości o Tobie nie dotrze do Twojego adresu zamieszkania.

Nie tylko Twój adres IP zapisywany jest w sieci. Wyszukiwarka google zapisuje historię wyszukiwanych przez Ciebie stron, a następnie przechowuje ją u siebie na serwerach przez kilka miesięcy. Zdarzały się przypadki, że władze państwowe prosiły właścicieli google'a o udostępnienie danych dotyczących danego adresu IP (a tym samym danego człowieka). Z informacji tych można wiele się dowiedzieć – czego człowiek szukał, czym się interesował itd. Oczywiście informacje te mogą być bardzo przydatne dla policji, czy prokuratury, jednak zastanowić się trzeba, czy niektórzy nie posuwają się za daleko.

Trwają również prace nad nowelizacją prawa telekomunikacyjnego, która pozwoli policji i ABW na wgląd w naszą wirtualną korespondencję.

Jak widać anonimowości w sieci nie ma. Można jednak ograniczyć dostęp do naszych danych osobowych innym użytkownikom Internetu. W jaki sposób?

Jak pisałem wyżej przeprowadziłem niedawno dwa eksperymenty, z których jeden dotyczył zdobywania danych osobowych człowieka, znając jedynie jego numer gadu-gadu. Wybrałem jeden, losowy numer i zacząłem bawić się w detektywa. Na samym początku wpisałem numer GG do wyszukiwarki google i otrzymałem masę wyników, która w większości nie miała nic wspólnego z owym numerem GG (były to dane statystyczne strony lub kawałki adresu). Dotarłem jednak do danych, które są ściśle powiązane z numerem GG.

Na początku trafiłem na forum internetowe, na którym człowiek ten szukał swoich przodków – miałem, więc jego nazwisko. Z kolejnej strony – tym razem był to serwis społecznościowy, dowiedziałem się, w jakim mieście mieszka, jak ma na imię i ile ma lat. Zdobyłem mnóstwo informacji, z których mogłem już szukać jego numeru telefonu. Był to młody chłopak, więc w książce telefonicznej nie było jego imienia, tylko jego rodziców.

W powyższym mieście było tylko sześć osób, o podanym nazwisku. Zadzwoiłem do każdego po kolei. Jak się jednak okazało, żaden z numerów nie był jego – mówi się trudno. Szukałem dalej, wygooglowałem jego adres e-mail, przejrzałem jego profil GG, nic więcej zrobić się nie dało. W tym wypadku zastosowałem trochę inną technikę, która nie jest do końca fair, jednak chciałem sam sobie udowodnić, że zdobycie kogoś danych osobowych, znając jedynie jego numer GG wcale nie jest trudne.

Jest to 18-letni chłopak, więc podałem się za 17-letnią dziewczynę. Rozmowa pięciominutowa i znałem nazwę restauracji, w której ma praktyki. I to w zasadzie koniec naszego poszukiwania. Googlujemy nazwę restauracji, wraz z nazwą miejscowości i mamy jej numer telefonu. Dzwonimy do właściciela lub osoby odpowiedzialnej za przyjmowanie praktykantów, podajemy się za dyrektora szkoły, do której praktykant uczęszcza i zgłaszamy pewne nieprawidłowości, które wymagają weryfikacji danych, ze strony restauracji.

Oczywiście tak daleko się nie posuwałem, jednak w powyższym przykładzie jasno i klarownie widać, że zdobycie czyichś danych osobowych nie jest niczym trudnym.

Zdobyłem tak cenne dane użytkownika tylko dlatego, że był on nieostrożny. Na forum, gdzie szukał swoich przodków, wraz z informacją o swoim nazwisku podał również numer gadu-gadu, na który prosił o kontakt poinformowane osoby. Nie znalazłbym jego nazwiska, gdyby zamiast kontaktu GG, preferował kontakt przez prywatne wiadomości na forum. Dopiero po skontaktowaniu się z kimś przez PM, mógł podać swój numer GG.

Kolejny był serwis społecznościowy. Zdecydowana większość młodych ludzi zostawia tam swoje prywatne dane. Nie widzę w tym nic złego, sam jestem zarejestrowany w kilku takich serwisach, jednak nie zostawiam tam swojego adresu e-mail, czy numeru GG, do publicznego wglądu. Gdyby Radek – bo tak miał osobnik na imię, nie zostawił tam numeru GG, nie dotarłbym do jego danych, nie wiedziałbym gdzie mieszka, jak ma na imię. Czasami – jak dowiesz się z kolejnego eksperymentu wystarczy znać zainteresowania człowieka, aby podał nam, nieświadomie klucz do swojego „mieszkania”.

Jak chronić się przed takimi sytuacjami? Wszystko jest dla ludzi, serwisy internetowe również. Nie zabraniam Ci rejestracji w takim, czy innym serwisie, bo jest to szalenie niebezpieczne. Pragnę tylko pokazać, że zostawianie w swoim profilu adresu e-mail, numeru gadu-gadu, czy telefonu jest bezmyślnością. Rozumiem, że takie informacje są dla osób, które chcą Cię poznać. Nie zaszkodzi jednak, gdy najpierw takie osoby skontaktują się z Tobą przez prywatną wiadomość w serwisie – większość stron udostępnia taką możliwość.

Odstępstwem od tego są strony prywatne, na których swoje dane kontaktowe możesz podać w formie graficznej. Żadna dotychczas działająca wyszukiwarka nie zaindeksuje tych danych, więc nie ma obaw, że ktoś niepowołany do nich dotrze.

Swojego adresu e-mail nie należy nigdzie również zostawiać w normalnej formie (nazwa@domena.pl) z powodów spambotów, które wędrują po stronach i zbierają te dane, aby później wysyłać niechciane wiadomości.

Kolejną sprawą jest korzystanie z tego samego hasła, na różnych serwisach internetowych. Przeprowadziłem kolejny eksperyment, aby sprawdzić jak wiele osób zostawia klucze do swojego mieszkania osobom nieznanym.

Stwierdzić muszę, iż ludzie są bezmyślni... Przepraszam, złego słowa użyłem. Są niedoświadczeni. To jest tak jak z kradzieżą. Pomyśl, jakbyśmy funkcjonowali, gdyby nie było czegoś takiego jak kradzież, przywłaszczenia sobie czyjegoś mienia. W drzwiach nie mielibyśmy zamków, samochody z otwartymi drzwiami na parkingach, rowery pozostawione bez klódek. Właśnie. I chyba podobnie myślą szczególnie młodzi (lecz nie tylko) ludzie zostawiając swoje hasła na różnych serwerach.

Rejestrując się tygodniowo na kilkunastu serwisach internetowych trudno tworzyć nowe hasła - przyznaję Wam rację. Ciężko spamiętać je wszystkie. Jednak korzystanie z jednego hasła na wszystkich stronach WWW jest przesadą. Porównam to do posiadania 10 mieszkań, w różnych częściach kraju, do których pasuje jeden, ten sam klucz. Jeśli owy klucz zgubimy lub zostanie nam on zabrany nie stracimy majątki z jednego, lecz z dziesięciu mieszkań.

Musisz przyjąć pewną taktykę, filtrować serwisy, na których się rejestrujesz, podzielić je na te ważniejsze, bezpieczniejsze i błahe, których administrator nie musi być uczciwy.

Do konta e-mail miej oddzielne hasło, niezależne od całej reszty - to dzięki niemu mogę poznać hasła do pozostałych serwisów. Na tych bezpieczniejszych i ważniejszych (czyt. większych, mających długi staż w sieci) serwisach możesz stosować jedno hasło, do którego dodasz ciąg znaków - szczegółowo opisałem to poniżej

Pozostają serwisy błahe. Hasła do nich koniecznie muszą różnić się od wyżej wymienionych.

Tak opowiadam o bezpieczeństwie haseł, jednak nie piszę nic o konsekwencjach. Jak już wspominałem, niedawno przeprowadziłem eksperyment, aby na własnej skórze przekonać się jak wiele ludzi nie szanuje swoich wirtualnych kluczy. Utworzyłem stronę internetową, na popularnym systemie Jportal, dzięki której użytkownicy mogli ściągnąć dodatki do pewnej gry internetowej, po uprzedniej rejestracji. Puściłem link, wśród grupy zainteresowanych osób i po kilku chwilach grupka 20-osobowa zarejestrowała się na stronie.

Sprawdziłem maile wszystkich osób. Okazało się, że cztery osoby, z dwudziestu wymienionych podało takie samo hasło do konta e-miał, jak u mnie na stronie. Zatrważający wynik? Były to z reguły osoby młode, średnia wieku nie przekraczała dwudziestu lat. Jednak sam fakt, że osoby młode nie są ostrzegane przez starszych, przed niebezpieczeństwem, jakie niesie za sobą posługiwanie się jednym hasłem na wszystkich serwerach jest niepokojący.

To jest tak jak z prawdziwymi kluczami do domu. Pamiętasz ten dzień, w którym pierwszy raz rodzice dali Ci klucze do ręki? Następnie pouczali, aby strzec tego klucza, nie dawać go nikomu i NIE ZGUBIĆ? Tak samo powinno być z naszymi hasłami. Przed dopuszczeniem młodszych osób do komputera trzeba uświadamiać ich, że hasło w rzeczywistości jest wirtualnym kluczem, którego również trzeba chronić, nie dawać nikomu i oczywiście nie zgubić.

Najczęściej wpisując hasło na stronie mamy nadzieję, że tylko my je znamy i nikt inny nie ma do niego dostępu. W większości przypadkach tak właśnie jest – hasła są szyfrowane i nawet sami administratorzy nie mają do nich dostępu. Nigdy jednak nie możemy mieć pewności, czy hasło w rzeczywistości jest szyfrowane i – co najważniejsze, czy administrator strony jest do nas pozytywnie nastawiony. Pamiętaj o tym.

Do czego miałby służyć komuś dostęp do Twojego konta e-mail? Pojęcia nie mam. Wiem jednak, co można zdobyć mając do niego dojsie.

Na samym początku Twoja prywatna korespondencja. Chyba nie chciałbyś, aby ktokolwiek ją czytał. Pomijając to, z Twojego uzupełnionego profilu, na koncie e-mail można dowiedzieć się gdzie mieszkasz, jaki masz numer telefonu i tak dalej. Mając dostęp do tych informacji następnie można przejąć kontrolę nad Twoim kontem w allegro, kontem bankowym, czy numerem GG. Człowiek mający dostęp do numeru GG może manipulować Twoimi znajomymi, choćby Was skłócić. Jeśli komuś zależy na Twoim numerze telefonu uda się do Twoich znajomych. Prosta rozmowa:

- Maciek? Ty masz mój nowy numer, czy stary?

- A masz jakiś nowy?

- Podaj, który masz.

- \*Podaje numer\*.

- A, to masz nowy.

Numer zdobyty. Co z danymi osobowymi?

Rozumiesz, jakie konsekwencje niesie za sobą korzystanie z tego samego hasła na różnych stronach internetowych? Nie masz pewności, kto jest administratorem strony WWW, na której właśnie się rejestrujesz. Może jest to oszust, który chce tylko wyłudzić Twoje hasło, może specjalnie stworzył tą stronę, podesał Ci adres, abyś się na niej zarejestrował? Pamiętaj, co pisałem wyżej, Twoje zainteresowania może znać z serwisów społecznościowych, na których zostawiłeś swój numer GG.

Jak się chronić przed takimi sytuacjami? Po pierwsze i najważniejsze – korzystać z różnych haseł. Nie musi wcale to być trudne hasło, możesz korzystać z tego samego, dodając tylko człon na początku lub na jego końcu. Jak stworzyć bezpieczne hasło? Poniżej podałem prosty sposób.

Wybierz jedno, proste słowo, które na pewno zapamiętasz. Niech to będzie na przykład **obrazek**. Zajmijmy się przekształcaniem hasła. Zamiast litery o piszemy cyfrę 0, zamiast litery a – 4, zamiast litery e – 3. I otrzymujemy taki ciąg znaków: **0br4z3k**. Cały czas hasło dla nas jest proste, wiemy, co tam piszę. Możemy pójść krok dalej i zastosować duże i małe litery: **0bR4z3K**. To również nie jest trudne. Pierwsza litera mała, potem duża, mała, duża (ignorujemy cyfry). Stworzyliśmy hasło siedmiocyfrowe, składające się cyfr, liter małych i dużych – hasło to jest bardzo bezpieczne i praktycznie nie do złamania. Można? Można.

Masz już hasło podstawowe. Teraz do każdego z serwisu utwórz osobny człon.

Serwis:

Allegro.pl: **0bR4z3K**allegro

Gadu-gadu: **0bR4z3K**GG (**0bR4z3K**gadugadu)

Poczta: **0bR4z3K**poczta

Proponuje jednak znacznie podnieść poziom bezpieczeństwa hasła i dodać na początku lub końcu pewną, losową liczbę.

Serwis:

Allegro.pl: **0bR4z3K**allegro6

Gadu-gadu: 3**0bR4z3K**GG (3**0bR4z3K**gadugadu)

Poczta: **0bR4z3K**poczta9

Nawet, jeśli komuś powiedzie się i dotrze do Twojego hasła np. do profilu GG dalej nic z tym nie zrobi. Twojego hasło jest podobne do reszty, jednak nikomu nie uda się złamać kolejnych członów.

Miło mi, że dotrwałeś do końca książki. Mam nadzieję, że wiele z niej wywnioskowałeś i słowa „Bezpieczne surfowanie” będą miały dla Ciebie duże znaczenie. Wiesz już jak tworzyć bezpieczne hasło, wiesz czym grozi zostawianie w serwisach swoich numerów GG, a także wiesz jakie przykre konsekwencje niesie za sobą korzystanie z jednego hasła, na wielu stronach internetowych. Wykorzystaj tą wiedzę!).

Podziękowania:

**Filip „TheRamzes” Adamus** – Za drobne poprawki stylistyczne w ebooku.

**Kontakt z autorem:**

e-mail: [cihy@list.pl](mailto:cihy@list.pl)

WWW: <http://blog.cihy.pl>

Pozdrawiam,  
Michał Cichocki