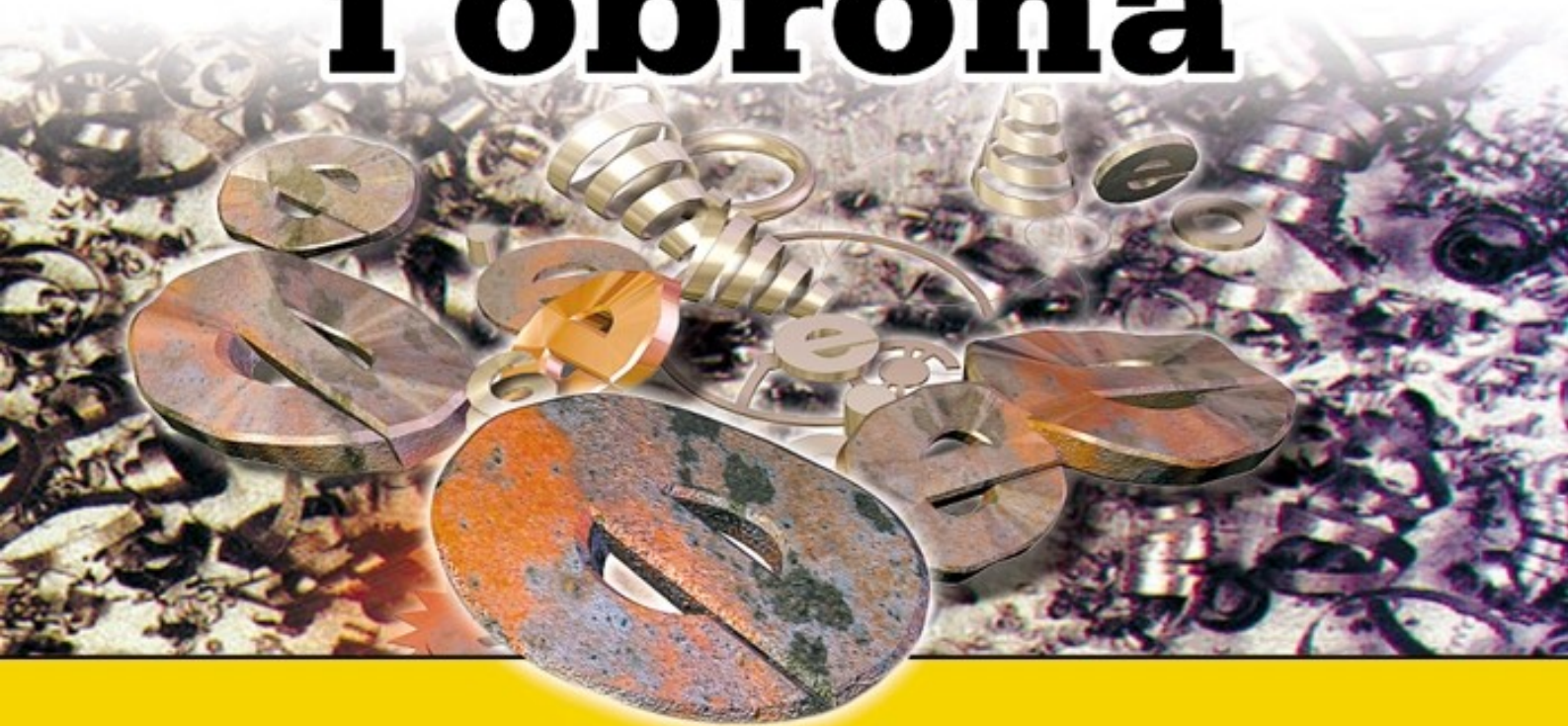


**Koniec z niechcianą pocztą!  
Oszczędzaj swój czas i nerwy.**

# **Spam**

## **Profilaktyka i obrona**



- **Poznaj rodzaje spamu**
- **Chroń swój adres mailowy**
- **Obroń się przed różnymi rodzajami spamu**

**Bartosz Danowski  
Łukasz Kozicki**

**Helion** 

Ten ebook zawiera darmowy fragment publikacji "[Spam. Profilaktyka i obrona](#)"

## Darmowa publikacja dostarczona przez [www.darmowe-ebooki.pl](http://www.darmowe-ebooki.pl)

Copyright by Złote Myśli & , rok 2006

Autor:

Tytuł: Spam. Profilaktyka i obrona

Data: 02.12.2011

Złote Myśli Sp. z o.o.

ul. Toszecka 102

44-117 Gliwice

[www.zlotemysli.pl](http://www.zlotemysli.pl)

email: [kontakt@zlotemysli.pl](mailto:kontakt@zlotemysli.pl)

Niniejsza publikacja może być kopiowana, oraz dowolnie rozprowadzana tylko i wyłącznie w formie dostarczonej przez Wydawcę. Zabronione są jakiegokolwiek zmiany w zawartości publikacji bez pisemnej zgody Wydawcy. Zabrania się jej odsprzedaży, zgodnie z regulaminem Wydawnictwa Złote Myśli.

Autor oraz Wydawnictwo Złote Myśli dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo Złote Myśli nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Wszelkie prawa zastrzeżone.

All rights reserved.

*Wszystkim, którzy przyczynili się  
do powstania tej książki*

# SPIS TREŚCI

<u>Wstęp</u> .....	7
<b>Rozdział 1.</b>	
<u>Wprowadzenie do tematyki spamu</u> .....	9
<u>Zarys historyczny spamu</u> .....	9
<u>Co jest spamem</u> .....	15
<u>Co nie jest spamem</u> .....	20
<u>„SPAM” i „spam” to nie to samo</u> .....	24
<u>Kto zarabia na spamie</u> .....	26
<u>Polska a spam</u> .....	29
<u>Konsekwencje istnienia spamu</u> .....	30
<b>Rozdział 2.</b>	
<u>Obszary funkcjonowania i popularne typy spamu</u> .....	33
<u>Obszary funkcjonowania spamu</u> .....	33
• <u>Poczta elektroniczna</u> .....	34
• <u>Grupy dyskusyjne</u> .....	36
• <u>Strony WWW</u> .....	37
• <u>Komunikatory internetowe</u> .....	39
• <u>Spam wysyłany za pomocą windows-messengera</u> .....	40
• <u>Telefony, faksy, SMS-y i MMS-y</u> .....	41
• <u>Ulotki reklamowe w skrzynkach pocztowych</u> .....	43
<u>Popularne typy spamu e-mailowego</u> .....	46
• <u>E-maile reklamowe</u> .....	46
• <u>„Zgodne z ustawą o świadczeniu usług...”</u> .....	47
• <u>Oszustwa i wyłudzenia</u> .....	52
• <u>Łańcuszki i żarty biurowe</u> .....	58
• <u>Spyware, zombie i e-pluskwy</u> .....	61
<b>Rozdział 3.</b>	
<u>Spam a regulacje prawne w naszym kraju</u> .....	63
<u>Ustawa zasadnicza – konstytucja</u> .....	64
<u>Ustawa o świadczeniu usług drogą elektroniczną</u> .....	65
<u>Ustawa o ochronie danych osobowych</u> .....	72
<u>Ustawa o zwalczaniu nieuczciwej konkurencji</u> .....	75
<u>Ustawa o ochronie konkurencji i konsumentów</u> .....	76
<u>Ustawa o ochronie praw konsumentów</u> .....	77
<u>Prawo działalności gospodarczej</u> .....	78
<u>Prawo antyspamowe w Unii Europejskiej</u> .....	78
<b>Rozdział 4.</b>	
<u>Analiza nagłówków pocztowych</u> .....	79
<u>Analiza nagłówka SMTP</u> .....	79
<u>Szukanie osób odpowiedzialnych za konkretne adresy IP</u> .....	84

<b>Rozdział 5.</b>	<b>88</b>
<b><u>Profilaktyka – ochrona adresu e-mailowego</u></b>	<b>88</b>
<u>Bardzo osobisty adres e-mailowy</u>	90
<u>Ochrona adresów e-mail w usenecie</u>	92
• <u>Odspamiacze</u>	94
<u>Ochrona adresów na stronie WWW</u>	98
• <u>Kodowanie</u>	99
• <u>Użycie grafiki</u>	102
• <u>Użycie JavaScriptu</u>	103
• <u>Flash, formularze, CGI</u>	109
• <u>Alias pocztowe</u>	110
<b>Rozdział 6.</b>	
<b><u>Obrona, czyli jak skutecznie bronić się przed spamem</u></b>	<b>112</b>
<u>Bierna ochrona konta e-mailowego</u>	112
• <u>Proste filtrowanie</u>	112
• <u>Analiza statystyczna</u>	113
• <u>Czarne i białe listy nadawców</u>	116
• <u>RBL</u>	118
• <u>Szare listy</u>	122
• <u>Systemy typu pytanie-odpowieź</u>	124
• <u>Systemy rozproszone</u>	126
<u>Obrona po stronie serwera</u>	129
• <u>Obrona za pomocą mechanizmów zaimplementowanych w systemie obsługi konta e-mail poprzez WWW</u>	129
• <u>Procmil</u>	134
<u>Obrona po stronie klienta</u>	139
• <u>Obrona za pomocą klienta pocztowego – Outlook Express (proste filtrowanie)</u>	139
• <u>Obrona za pomocą klienta pocztowego – Mozilla (metoda Bayesa)</u>	143
• <u>Obrona za pomocą zewnętrznych programów</u>	149
<u>Obrona poprzez oddziaływanie na spamera</u>	187
<u>Pisz skargi</u>	187
<u>Tłumacz spamerowi, że spam jest zły</u>	189
<u>Nie wypisuj się z list mailingowych, z których dostajesz spam</u>	190
<u>Nie korzystaj z „list Robinsona”</u>	192
<b>Rozdział 7.</b>	
<b><u>Atak - wyprzedź uderzenie spamera</u></b>	<b>193</b>
<u>Pułapki antyspamowe</u>	193
<u>Podsuwanie fałszywych adresów</u>	200
<u>Filtry samoatakujące</u>	203

## Rozdział 8.

<u>Przykłady obrony przed różnymi typami spamu</u> .....	205
<u>Dlaczego może jednak nie blokować reklam</u> .....	205
<u>Blokowanie popupów oraz natrętnych reklam</u> .....	210
<u>Usuwanie oprogramowania szpiegującego</u> .....	218
<u>Blokowanie usługi Messenger</u> .....	222
<u>Przykład pisma z prośbą o zaprzestanie nadawania reklam</u> .....	236

## Rozdział 9.

<u>Rady dla stawiających pierwsze kroki w e-biznesie</u> .....	240
<u>Listy opt-in i opt-out</u> .....	241
<u>Po pierwsze – witryna internetowa</u> .....	243
<u>Uruchamiasz listę opt-in</u> .....	244
<u>Przykład gotowego systemu mailingowego</u> .....	250

## Dodatek A.....

<u>Netykieta i standardy obowiązujące w sieci</u> .....	255
<u>Akty prawne związane ze spamem obowiązujące w Polsce</u> .....	255
<u>Akty prawne związane ze spamem obowiązujące w Unii Europejskiej</u> <u>(po polsku)</u> .....	256
<u>Prawo w internecie</u> .....	256
<u>Metody walki ze spamem</u> .....	257
<u>Oprogramowanie do walki ze spamem</u> .....	257
<u>Unix, Linux</u> .....	257
<u>MS Windows</u> .....	257
<u>Najpopularniejsze czarne listy (RBL)</u> .....	258
<u>Sprawdzanie wielu list RBL jednocześnie i inne narzędzia</u> .....	258
<u>Strony poświęcone tematyce spamu</u> .....	259

## Podsumowanie.....

260

## Wstęp

Zapewne każdy użytkownik internetu znalazł w swojej skrzynce e-mail, którego nie zamawiał i który go nie interesuje. Zazwyczaj taka poczta trafia do Twojej skrzynki z bliżej nieokreślonego źródła i może być napisana w różnych językach. Najczęściej niechciana poczta zawiera reklamy produktów lub usług, choć zdarzają się również inne typy reklamowych listów. Taka niechciana poczta została przez internautów ochrzczona mianem *spamu*.

Zjawisko spamu w ostatnich latach drastycznie się nasila i doprowadziło do sytuacji, w której coraz więcej państw zaczęło wprowadzać regulacje prawne mające na celu ograniczenie plagi niechcianych listów elektronicznych. Również użytkownicy internetu nie pozostają bierni i starają się walczyć na własną rękę z uciążliwościami spowodowanymi tą plagą.

Postanowiliśmy przygotować niniejszą książeczkę z nadzieją, że część naszej wiedzy na temat form spamu oraz obrony przed nim umożliwi każdemu początkującemu użytkownikowi internetu zabezpieczenie się przed uciążliwościami wynikającymi z otrzymywania niechcianych wiadomości różnego rodzaju – takich jak e-maile, SMS-y i bannery na stronach WWW, a także faksy, telefony i inne przesyłki. Pomimo, że książka jest przeznaczona dla początkujących użytkowników internetu i poczty elektronicznej, to również osoby bardziej zaawansowane zapewne znajdą tutaj ciekawe informacje, których często można próżno szukać w fachowej prasie komputerowej.

W kolejnych rozdziałach wyjaśniliśmy, czym jest spam, opisaliśmy sytuację prawną spamu w naszym kraju oraz zaprezentowaliśmy najpopularniejsze techniki używane przez nadawców spamu. Uznaliśmy, że aby skutecznie zwalczać spam, należy poznać zasadę działania wroga. Dopiero ta wiedza pozwala na skuteczne zabezpieczenie się przez niechcianą pocztą elektroniczną. Oczywiście, nie uczymy wysyłać spamu, ale w myśl zasady mówiącej o tym, że aby skutecznie walczyć z wrogiem, należy go dobrze

poznać, staramy się kompleksowo przygotować naszych czytelników do tej wojny. Kolejne rozdziały uczą, jak skutecznie zabezpieczyć się przed otrzymywaniem spamu w przyszłości oraz jak zwalczać spam otrzymywany na posiadane konto e-mail. Nie zapomnieliśmy również o prezentacji pewnych rozwiązań pozwalających na zabezpieczenie serwerów pocztowych.

Jeżeli po przeczytaniu naszej książki będziesz miał pytania lub uwagi, to chętnie służyliśmy pomocą, gdyż zdajemy sobie sprawę, że nasza publikacja nie zawiera wszystkiego, co dotyczy zakresu omawianych zagadnień. Przyczyną takiego stanu jest fakt, że dysponowaliśmy ograniczoną ilością stron w książce oraz to, że od chwili zakończenia pracy nad pisaniem i wydaniem książki mogły i z pewnością pojawiły się nowe techniki wysyłania niechcianych e-maili. Poza tym wraz z wymyślaniem nowych sposobów obrony zmuszamy nadawców spamu do szukania nowych możliwości kontynuowania tego niecnego procederu. Dlatego za kilka lub kilkanaście miesięcy w sieci pojawią się nowe techniki umożliwiające wysyłanie niechcianej poczty, o których siłą rzeczy nie mogliśmy wspomnieć w niniejszej publikacji.

Serdecznie dziękujemy za pomoc w zgromadzeniu zebranych tu materiałów licznym osobom – administratorom serwerów pocztowych, prawnikom, twórcom stron WWW i innym osobom, które tworzyły rozwiązania antyspamowe, dzieliły się z nami swoją wiedzą i pomagały zgłębić omawianą problematykę oraz przyczyniły się do korekty znalezionych błędów. Osób, którym należą się podziękowania, jest tak wiele, że po prostu nie sposób wymienić ich wszystkich...

Życzymy przyjemniej lektury, skutecznej i przemyślanej profilaktyki pozwalającej na zabezpieczenie się przez niechcianą pocztą, a wreszcie doskonałej obrony przed spamem. Nie zapomnij odwiedzić naszych stron domowych – zapraszamy. Zachęcamy też do kontaktu w przypadku dostrzeżenia błędów lub ważnych braków w omawianej tematyce, uwagi takie na pewno zostaną wykorzystane – jeśli nie w kolejnym wydaniu książeczki, to przynajmniej na stronie internetowej.

*Bartosz Danowski [bartosz@danowski.pl](mailto:bartosz@danowski.pl); <http://danowski.pl>  
Łukasz Kozicki [nospam@nospam-pl.net](mailto:nospam@nospam-pl.net); <http://nospam-pl.net>*

## ROZDZIAŁ 5.

### Profilaktyka – ochrona adresu e-mailowego

Obronę przed spamem należy zaplanować znacznie wcześniej – zanim stanie się on utrapieniem. Jeżeli założysz nowe konto albo na istniejące konto jeszcze nie dostajesz spamu i pozornie problem Cię nie dotyczy, i tak musisz podjąć działania profilaktyczne, aby uchronić się przed spamem w przyszłości.

Niniejszy rozdział ma za zadanie pokazać Ci sposoby zabezpieczenia się przez otrzymywaniem spamu. Dlatego przeczytaj go dokładnie i sumiennie zastosuj się do wszystkich zaleceń.

Jeżeli problem spamu już Cię dotknął, nie bagatelizuj profilaktyki, gdyż dzięki niej możesz jeszcze ograniczyć ilość spamu, jaka będzie do Ciebie trafiać w przyszłości.

Stosując się do niżej zebranych porad należy pamiętać, że przedstawione przykłady są aktualnie dość skuteczne, ale będą takie jedynie do chwili, gdy nie staną się zbyt popularne. Wtedy spamerzy zapewne opracują nowe wersje robotów, które sobie z nimi poradzą. Dlatego kluczem do sukcesu jest duża pomysłowość podczas wymyślania własnych wersji odspamiaczy czy osobistych zabezpieczeń.

Ochrona adresu e-mailowego przed wpisaniem do spammerskich baz adresów jest najlepszym środkiem obrony przed spamem. Jest to tym bardziej ważne dlatego, że aktualnie niemal wszędzie ktoś może Cię spytać o adres e-mailowy – nawet w tak zdawałoby się odległych od internetu okazjach jak na przykład

rezerwacja stolika w restauracji czy wysyłka dokumentów do jakiegoś urzędu. W każdym z takich przypadków właściwie nie masz kontroli nad tym, co dalej będzie się działo z ujawnionym obcej osobie adresem. Adres może zostać wpisany do bazy klientów firmy, skąd może go nawet wynieść i sprzedać spamerom (wraz z całą bazą) nieuczciwy pracownik; firma może podzielić się na dwie mniejsze, a wtedy każde nowo utworzone przedsiębiorstwo będzie chciało zachować bazę klientów – i może stać się mnóstwo innych, zupełnie nieprzewidywalnych rzeczy.

Oto krótkie podsumowanie najważniejszych zasad ochrony adresu – zostaną one omówione dalej.

Przyjmij generalną zasadę, że nikomu nie podajesz swojego adresu e-mailowego. Szczególnie chroń adresy, które są dla Ciebie najcenniejsze. Wyjątek od tej zasady, czyli udostępnienie adresu e-mailowego, zawsze wymaga przekonującego uzasadnienia.

Jeśli w jakiejś witrynie internetowej podajesz swój adres, zawsze sprawdzaj obowiązujące w niej zasady ochrony prywatności – dowiedz się, jak ten adres będzie użyty, zanim zdecydujesz się go ujawnić i zastanów się dwa razy, czy podawanie adresu jest naprawdę konieczne.

Wypełniając jakikolwiek formularz on-line sprawdź, jakie opcje domyślnie w nim zaznaczono. Zastanów się, czy sam byś te opcje zaznaczył.

Używaj filtrów pocztowych, blokujących wiadomości lub odpowiednio je odznaczających.

Nigdy nie klikaj odnośników zawartych w spamach, nie odwiedzaj reklamowanych witryn, nie „wypisuj” się z list mailingowych, nie wypisuj swojego adresu ze spammerskich baz mailingowych.

Wyłącz ładowanie obrazków w listach formatu HTML.

Użyj dodatkowego (np. darmowego) konta e-mailowego, gdy jesteś zmuszony podać swój adres, np. robiąc zakupy on-line.

Sam nie wysyłaj czegoś, co może być uznane za spam, nie przesyłaj do znajomych wiadomości, które mogą uznać za niepożądane.

### **Bardzo osobisty adres e-mailowy**

Profilaktyka antyspamowa zaczyna się już w momencie zakładania konta pocztowego – konto powinno mieć taką postać, by było jak najmniej podatne na ataki. Spamerzy często „wymyślają” adresy swoich ofiar, dodając do znanych domen przypadkowe ciągi znaków – np. wysyłając małe próbki spamu na wszystkie adresy od *aaaaa@domena.pl* do *zzzzz@domena.pl*. Jeśli któryś e-mail się nie „odbija”, to znaczy, że dane konto istnieje i zostaje ono dopisane do spammerskiej bazy danych. Inna metoda zgadywania adresów, to podstawianie kolejnych imion „z kalendarza”. Z tego powodu adresy kilkuliterowe czy oparte na imieniu lub imieniu i jednej literze nazwiska są znacznie bardziej narażone na spam niż adresy dłuższe, szczególnie, jeśli zawierają dodatkowo kilka losowych liczb – np. *jankowalski005@domena.pl*.

Właścicielowi tego nowo założonego adresu zależy na zachowaniu go z dala od spammerskich baz, to konto będzie najbardziej chronione i określane jako *adres podstawowy*. Czasem jednak okazuje się, że trzeba podać swój adres w miejscu, w którym jego ujawnienie może wiązać się z dużym ryzykiem – np. by uzyskać hasło dostępu do jakiejś usługi, zakupić towar w sklepie internetowym lub wysłać wiadomość do usenetowej grupy dyskusyjnej. Najwygodniejszą i najczęściej stosowaną formą zabezpieczenia się przed ryzykiem wpisania podstawowego adresu e-mailowego do bazy gromadzonej przez spamerów jest założenie innego konta, na przykład na jakimś darmowym serwerze (*http://poczta.onet.pl*, *http://poczta.interia.pl*) i używanie go we wszystkich ryzykownych okolicznościach. Ten adres zostanie nazwany *publicznym*. Darmowe konto można bez żalu porzucić i zamienić w razie potrzeby na inne, zaś spamu, który trafi na ten adres, można użyć do

„uczenia” filtrów antyspamowych bazujących na statystycznym klasyfikatorze treści Bayesa w programach SpamPal czy Mozilla.

W przypadku adresu podstawowego należy przyjąć ogólną zasadę nie podawania go nigdy i nigdzie, chyba że okoliczności dostatecznie uzasadniają konieczność jego udostępnienia. Adresy e-mailowe stały się tak popularne, że często prosi się o ich podanie, nawet gdy nie ma to dostatecznego uzasadnienia – np. w formularzach rejestracyjnych zbierających zgłoszenia na konferencję (po co organizatorom adres każdego uczestnika, jeśli i tak mają już kontakty z firmą, która tych pracowników wysłała?). O adres pytają różne firmy i jeżeli go otrzymają, właściciel tego adresu nie ma praktycznie żadnej kontroli nad sposobem jego wykorzystania – może być używany do marketingu, sprzedany jako część „bazy danych” lub stać się ofiarą wirusa.

O adres publiczny też warto dbać. Jeżeli w razie konieczności podajesz gdzieś adres publiczny, zawsze upewnij się, jak ten adres będzie wykorzystywany. Podczas zakładania nowego konta lub robienia zakupów w sieci dokładnie czytaj regulaminy oraz uwagi zamieszczone na stronach, sprawdź „politykę ochrony prywatności”, wpisując adres do formularza na stronie WWW sprawdź, jakie opcje są domyślnie w tym formularzu włączone – czy nie ma tam przypadkiem „zgody na otrzymywanie materiałów promocyjnych od naszej firmy i od naszych partnerów” itp.

Pamiętaj, że niektóre strony są prowadzone wyłącznie po to, aby zbierać e-maile od naiwnych internautów, a następnie ich właściciele wysyłają na zabrane adresy spam lub sprzedają je jako towar większym spamerom. Z tego powodu *nigdy nie odpisuj na spam* i nie staraj się wypisywać z list adresowych, ponieważ wielu spamerów stosuje oszustwa w celu sprawdzenia, czy dany adres działa – zachęcają do wypisywania się po to, by potwierdzić, że adresat spamu odczytał go, przeczytał i zrozumiał. Jeżeli w stopce spamu widzisz instrukcję wypisania się z listy, w praktyce oznacza to, że po wykonaniu poleceń tam zawartych Twój adres trafi do bazy zweryfikowanych adresów i zaczniesz dostawać jeszcze więcej spamu.

Podawaj więc adres podstawowy tylko tym osobom, co do których masz przekonanie, że nie przekażą nawet mimochodem tego adresu osobom trzecim, że nie zarażą Cię wirusem, który roześle ten adres po świecie razem ze swoimi kopiami, nie wysyłają bezrefleksyjnie poczty do dziesięciu osób jednocześnie itd. – więcej na ten temat dalej.

## Ochrona adresów e-mail w usenetcie

Usenet jeszcze kilka lat temu był szalenie popularną usługą wśród użytkowników internetu. Obecnie można zaobserwować wśród młodych internautów tendencję do korzystania raczej z różnych forów dyskusyjnych na stronach WWW niż ze starego, dobrego usenetu. Na szczęście nie oznacza to, że usenet się kończy. Wręcz przeciwnie, nadal ma się dobrze, a ponadto w większości grup można zaobserwować znacznie wyższy poziom kultury dyskusji – w przeciwieństwie do wulgarności i arogancji, które są niemal typowe dla forów dyskusyjnych on-line. Grupy dyskusyjne (usenet) to bardzo przydatna usługa sieciowa, pozwalająca na dyskusje z osobami o zbliżonych zainteresowaniach, wymianę poglądów, szybką propagację informacji pomiędzy użytkownikami, uzyskanie wiedzy i pomocy od osób bardziej doświadczonych w jakimś temacie itp., itd.

Niestety, poza pomocą, jaką możesz tam otrzymać, usługa ta może być również początkiem Twojej przygody ze spamem. Każdy użytkownik usenetu wysyła tam wiadomości (artykuły, określane też jako *postingi*), które można porównać do typowych e-maili. Artykuły te są publicznie dostępne i każdy może na nie odpisywać. Oczywiście, również odpowiedzi są publicznie dostępne. W związku z tym, że użytkownicy usenetu podają swoje adresy e-mail podczas konfiguracji czytników lub wpisują je do stopek artykułów, cała korespondencja stanowi doskonałe źródło adresów. Już kilka lat temu uświadomiono sobie, że grupy dyskusyjne są doskonałym źródłem pozyskiwania adresów e-mailowych i stosunkowo szybko pokłady te zaczęły być eksploatowane. Okazuje się, że za pomocą oprogramowania popularnie

zwanego *harvesterem*<sup>1</sup> każdy użytkownik sieci w kilka godzin może zgromadzić ogromną bazę danych zawierającą adresy e-mail „skradzione”<sup>2</sup> z tysięcy grup dyskusyjnych. Co ciekawe, harvestery można bez problemu kupić w naszym kraju za stosunkowo niewielkie kwoty, zresztą często są one reklamowane jako „nieodzowne narzędzie marketingowe”. Pozwala to sądzić, że zjawisko kradzieży i handlu nielegalnie zdobytymi adresami będzie się nasilać, a to przełoży się na wzrost ilości spamu krążącego po sieci. Dlatego właśnie w grupach dyskusyjnych warto używać adresu publicznego. Jeżeli jednak mimo świadomości zagrożenia, jakie płynie z korzystania z grup dyskusyjnych, nadal chcesz tam używać swego podstawowego adresu e-mail, choćby po to, by swoim rozmówcom ułatwić nawiązanie prywatnego kontaktu, możesz sięgnąć po inne metody zabezpieczenia się.

Pamiętaj o tym, że większość grup dyskusyjnych posiada publicznie dostępne archiwa, co powoduje, że raz użyty adres może być dostępny dla spamerów już zawsze.

O tym, jak duże zagrożenie spamem niosą za sobą grupy dyskusyjne, świadczy fakt, że po wysłaniu testowej wiadomości na jakąś grupę dyskusyjną z nowego adresu często przed upływem czterdziestu ośmiu godzin otrzymasz pierwszy spam. Dlatego zanim zaczniesz korzystać z grup dyskusyjnych, musisz podjąć działania mające na celu ochronę adresu e-mailowego.

Harvestery czytają adresy zarówno z nagłówek wiadomości usenetowych, jak i z ich treści. Należy pamiętać o tym, że nasz adres został wpisany w konfiguracji czytnika i tam także należy go zabezpieczyć. Adres w zakodowanej postaci wystarczy umieścić w konfiguracji programu do czytania

---

<sup>1</sup>*Harvester* (ang. żniwiarka) – nazwa, która przyłgnęła już do spam-botów, programów przeszukujących strony WWW, fora dyskusyjne, grupy usenetowe itp. W poszukiwaniu adresów, na które można wysłać spam. Nazwa ta jest jednak wyjątkowo niezręczna – żniwiarz bowiem zbiera to, co sam posiał i pielęgnował – zaś spamer używa spam-bota do tego, by żąć, czego nie posiał.

<sup>2</sup>Adresy takie zostały „skradzione” w takim sensie, że są zdobyte bez wiedzy i zgody ich użytkowników, a raczej wbrew ich woli – a więc w sposób niezgodny zarówno z dobrymi obyczajami, jak i z obowiązującym w Polsce prawem.

grup dyskusyjnych zamiast swojego właściwego adresu. Można również go umieścić w stopce swoich wiadomości i używać w grupach dyskusyjnych. Oczywiście warto w stopce lub w inny sposób poinformować innych internautów, że zakodowałeś adres lub w inny sposób go zabezpieczyłeś. Dzięki temu każdy z nich będzie wiedział, jak odczytać i skorzystać z podanego e-maila.

Najwygodniejszą i najczęściej stosowaną formą zabezpieczenia się przed możliwością trafienia ze swoim adresem e-mail na listy spamerów jest korzystanie w grupach dyskusyjnych wyłącznie z adresu publicznego. Dzięki temu spam trafi na darmowe konto, które łatwo można zmienić. Rozwiązanie to jest najpewniejsze i daje stuprocentowe zabezpieczenie.

Jeżeli mimo świadomości zagrożenia, jakie płynie z grup dyskusyjnych, nadal chcesz używać na nich swego podstawowego adresu e-mail, możesz skorzystać z innych metod zabezpieczenia się. Niestety, nie są one tak skuteczne, jak wykorzystanie innego konta. Jednak mimo to warto z nich korzystać.

#### • Odspamiacze

Najczęściej stosowanym zabezpieczeniem jest *odspamiacz* dodany do właściwego adresu. Użycie odspamiacza polega na dodaniu jakiegoś słowa lub ciągu znaków do właściwego adresu. Odspamiacz jest najprostszym i darmowym sposobem zabezpieczenia adresu przed spamerem. Jeżeli harvestery zdobędą taki adres i spamer będzie usiłował wysłać na niego wiadomości, to nie dotrą one do prawdziwego właściciela. Natomiast człowiek korzystający z usenetu w sytuacji, gdy zechce się z nami skontaktować, będzie wiedział, że musi wprowadzić modyfikację w adresie, aby poczta dotarła do adresata. Dodatkowo warto w stopce wiadomości wysyłanych na grupy dyskusyjne dopisać kilka słów z wyjaśnieniem tego, co dokładnie należy usunąć z adresu. Nie trzeba chyba nikomu mówić, jak kończy się wysyłka poczty

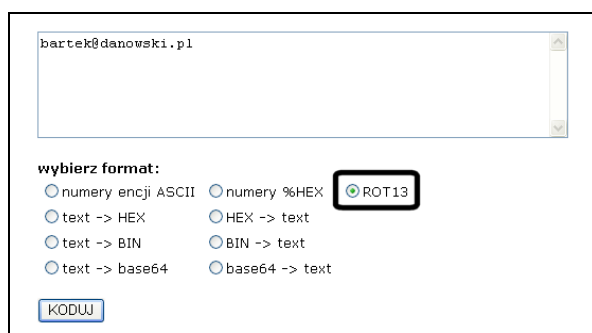
na nieistniejący lub niepoprawny adres – zostanie odbity do nadawcy z komunikatem, że odbiorca nie istnieje.

- ◆ Tworząc odspamiacz, dodawaj go wyłącznie po prawej stronie znaku @  
Prawidłowy odspamiacz to np. *login@odspamiacz.domena.pl*, *login@domena-odspamiacz-.pl*, *login@domena.usunto.pl*. Zanim jednak zastosujesz pierwszy sposób, upewnij się, czy Twój serwer pocztowy nie przyjmuje wszystkich przesyłek wysyłanych na adres *login@cokolwiek.domena.pl*  
– jeśli bowiem przyjmuje, ktoś będzie dostawał spam wysyłany na ten adres (prawdopodobnie trafi on do administratora). W drugim przypadku jako odspamiacz warto zastosować poza znakami literowymi kombinację innych znaków, mało prawdopodobnych do użycia w rzeczywistej domenie (np. „-”, „\_”). Ostatni przykład to przypadek, gdy wysłany e-mail będzie szukał właściciela domeny *usunto.pl*, do którego może trafić, jeśli ktoś wykupiłby taką właśnie domenę. Z tego powodu domena *usunto.pl* jest w zasadzie z góry „spalona” (zbyt popularna pułapka). Jeśli chcesz używać jako odspamiacza innego słowa, to powinno ono być możliwie dziwaczne lub nieprawdopodobne do zarejestrowania jako samodzielna nazwa domeny. Możliwym wyjściem z tej sytuacji wydaje się użycie np. jakiegoś stosunkowo długiego słowa pisanego wspak np *serdanetnusu*.
- ◆ Nie należy dodawać odspamiacza do nazwy użytkownika, jeśli nie ma się pewności, jaki będzie tego skutek, ponieważ na wielu serwerach poczta przysłana do nieistniejącego użytkownika trafia na konto administratora. Z pewnością nie ucieszy się on z dodatkowej porcji spamu... Nie stosuj zatem odspamiacza w postaci *login-odspamiacz@domena.pl*.

Niestety, zabezpieczenie to jest coraz częściej rozpoznawane i skutecznie eliminowane przez automaty do gromadzenia adresów. Zbyt popularne słowa (np. *usunto*, *nospam*, *remove*) są rozpoznawane przez roboty, które potrafią

automatycznie „naprawić” taki wadliwy adres. Dlatego decydując się na odspamiacz, należy wykazać się oryginalnością, gdyż tylko to może zapewnić możliwie skuteczną ochronę. Warto skorzystać też z bardziej zaawansowanych technik umożliwiających ochronę adresu na grupach dyskusyjnych.

Jednym z ciekawszych sposobów jest kodowanie adresu za pomocą *ROT13*<sup>3</sup> oraz połączenie kodowania *ROT13* i wspomnianego już odspamiacza. Wiele programów pocztowych posiada funkcję kodowania *ROT13*, jeśli jednak używany przez Ciebie program nie ma takiej możliwości, aby zakodować swój adres, możesz skorzystać z odpowiedniego formularza na stronie <http://nospam-pl.net/koduj.php>. Cała operacja nie jest skomplikowana i ogranicza się do wpisania adresu w odpowiednim polu, zaznaczenia sposobu kodowania oraz kliknięcia przycisku *KODUJ* – rysunek 5.1.



Rysunek 5.1. Kodowanie *ROT13* za pomocą wygodnego formularza na stronie <http://nospam-pl.net/koduj.php>

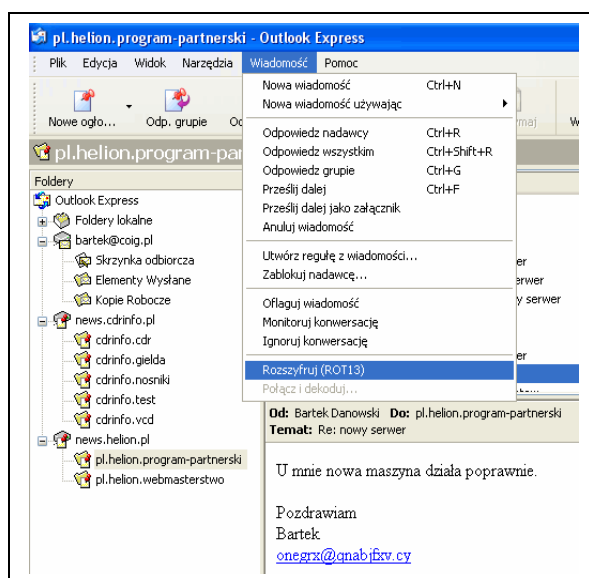
Zakodowany adres może mieć na przykład następującą postać *onegrx@qnabjfxv.cy*. Podobnie jak w przypadku zabezpieczenia odspamiaczem, adres nadal będzie zbierany przez roboty, ale w zakodowanej

---

<sup>3</sup>*ROT13* to prosty szyfr przesuwany polegający na zastąpieniu danego znaku przez inny występujący trzynastą liter dalej w alfabecie. Na przykład literę *A* zastępuje się literą *N*. W przypadku kodowania *ROT13* wielkość znaków nie ma najmniejszego znaczenia, a sam kod jest swoją odwrotnością. Wygodny mechanizm kodowania *ROT13* jest udostępniany na stronie <http://nospam-pl.net/koduj.php>.

postaci jest bezużyteczny – wysłanie na niego poczty będzie nieskuteczne. Natomiast użytkownicy większości popularnych programów do obsługi usenetu bez problemu będą mogli odkodować adres. Poniżej na rysunku 5.2 zamieszczamy przykład rozkodowania adresu w przypadku programu MS Outlook Express.

Wystarczy, że po zaznaczeniu wiadomości z zakodowanym adresem z menu *Wiadomość* wybierzesz opcję *Rozszyfruj (ROT13)* i w treści pojawi się właściwy adres e-mail.



Rysunek 5.2. Przykład rozkodowania ROT13 w MS Outlook Express

Inną równie ciekawą i skuteczną metodą jest umieszczenie jako nadawcy kompletnie fikcyjnego adresu (stworzonego jednak z głową – tak, by nie szkodzić innym użytkownikom internetu – tak, jak zostało to opisane nieco wyżej), a podanie właściwego adresu w stopce listu, wykorzystując albo kodowanie albo różnego rodzaju rebusy czy zagadki typu:

- ♦ mój adres: *login*, *at*, *domena*, kropka, *com*, kropka, *pl*;
- ♦ *login.domena.com.pl*, tylko pierwsza kropka to @;

- ◆ *login%domena.com:pl*, zamień znaki %=@, :=. (lub cokolwiek innego zamiast @);
- ◆ moja strona to *http://www.domena.com.pl/~login*, a adresu się domyśl;
- ◆ mój email: *lapaczka\_spamu@domena.com.pl*, a zamiast *lapaczka\_spamu* wpisz *login*;
- ◆ mój adres: *lEgin@dEmena.cEm.pl* (E = o);
- ◆ mój adres złoż z części: *user=login, domena=domena.com.pl*;
- ◆ *łqgin@dqmęńq.pl*, tylko zamień polskie literki.

Tego typu rozwiązanie nie jest możliwe do przejścia przez wyspecjalizowane oprogramowanie używane przez spamera, ponieważ nie warto pisać algorytmów dedykowanych tylko pod jeden rebus. Jeżeli każdy użytkownik wymyśli swój sposób na zabezpieczenie adresu albo wprowadzi modyfikację w rozwiązaniach przedstawionych przez kogoś innego, to żadne oprogramowanie nie będzie w stanie tego rozkodować i uzyskać poprawnego adresu.

Zaproponowane tutaj przykłady pochodzą ze strony dostępnej pod adresem *http://nospam-pl.net*.

## Ochrona adresów na stronie WWW

W przypadku adresów e-mail udostępnionych na stronie WWW również jesteś narażony na możliwość zdobycia Twojego adresu przez spamera. Dlatego decydując się na udostępnienie adresu, warto podjąć działania profilaktyczne, których celem jest utrudnienie lub uniemożliwienie przejęcia Twojego adresu. Niestety, w tym przypadku skuteczne zabezpieczenie adresu staje się bardziej skomplikowane.

Pierwszym, najprostszym, ale również najmniej pewnym sposobem zabezpieczenia adresu jest użycie odspamacza, o którym wspominaliśmy

w poprzednim podrozdziale. Jak wiesz, w przypadku strony WWW użycie na niej adresu wiąże się z zastosowaniem znacznika HTML zgodnie z przykładem.

```
<a href="mailto:adres@domena.pl">adres@domena.pl</a>
```

Po jego kliknięciu najczęściej otwiera się okno programu pocztowego pozwalające na rozpoczęcie pisania wiadomości. Automatycznie w polu *To:* (polu *Do:*) powinien znaleźć się adres wpisany w hipertączy. Jest to szalenie wygodne, ale jednocześnie stanowi przeszkodę w skutecznym zabezpieczeniu adresu. Oczywiście pomiędzy znacznikami `<a></a>` można wpisać inny dowolny ciąg znaków. W związku z tym, aby skutecznie zabezpieczyć adres za pomocą odspamiacza, musisz go użyć w każdym adresie występującym w kodzie stronie. Poniżej przedstawiamy konkretny przykład.

```
<a href="mailto:adres@domena.odspamiacz.pl">adres@domena.odspamiacz.pl</a>
```

- Kodowanie

Niestety, oprogramowanie używane przez spamerów do skanowania stron WWW oraz zbierania adresów e-mail coraz lepiej radzi sobie z zabezpieczeniami w postaci odspamiaczy. Dlatego warto pokusić się o coś znacznie bardziej skutecznego.

Mamy tutaj na myśli zakodowanie adresu e-mail. W przypadku stron WWW używa się innego sposobu kodowania. Możesz zapisać swój adres e-mail za pomocą tak zwanych *encji HTML*, czyli cyfrowych kodów znaków, zgodnie z poniższym przykładem.

- ◆ Nie zakodowany adres:

[bartek@danowski.pl](mailto:bartek@danowski.pl)

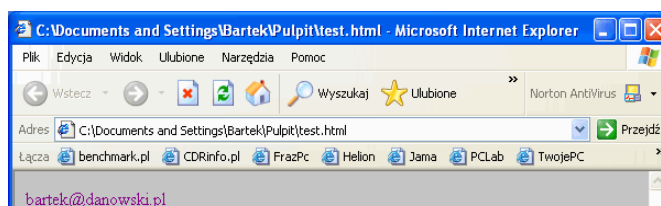
## ◆ Zakodowany adres:

```
&#98;&#97;&#114;&#116;&#101;&#107;&#64;&#100;&#97;&#110;&#111;&#119;&#115;&#107;&#105;&#46;&#112;&#108;
```

Bardzo wygodnym narzędziem służącym do kodowania adresu e-mail jest skrypt dostępny pod adresem <http://nospam-pl.net/koduj.php>. Wystarczy, że wejdiesz na stronę, w odpowiednim formularzu wpiszesz kodowany adres, a następnie określisz sposób kodowania i klikniesz przycisk **KODUJ**. Po chwili na stronie pojawi się zakodowany adres, który wystarczy wkleić do kodu strony jak na przykładzie.

```
<a  
href="&#109;&#97;&#105;&#108;&#116;&#111;&#58;&#98;&#97;&#114;&#116;&#101;&#107;&#64;&#100;&#97;&#110;&#111;&#119;&#115;&#107;&#105;&#46;&#112;&#108;&#98;&#97;&#114;&#116;&#101;&#107;&#64;&#100;&#97;&#110;&#111;&#119;&#115;&#107;&#105;&#46;&#112;&#108;>
```

Twoja przeglądarka taki adres pokaże w sposób poprawny – rysunek 5.3 – natomiast roboty skanujące i zbierające adresy e-mail w zdecydowanej większości przypadków nie znajdą adresu i nie będą potrafiły go rozkodować.



Rysunek 5.3. Widok zakodowanego adresu e-mail w oknie przeglądarki

Jeżeli zdecydujesz się zapisać swój adres e-mail za pomocą encji, to możesz zakodować pojedyncze znaki, np. @, lub cały ciąg poczynając od słowa

*mailto*. Wydaje się, że warto kodować cały ciąg znaków zaczynając od *mailto*, ponieważ wiele robotów używanych przez spamerów jest wyczulonych na występowania bądź to znaku @, bądź słowa *mailto*. Zakodowanie całego ciągu znaków pozwoli na oszukanie spamera i jego robota. Można również skorzystać z następującego zapisu:

```
<a  
href="&#109;&#97;&#105;&#108;&#116;&#111;&#58;&#98;&#97;&#114;&#11  
6;&#101;&#107 ;&#64;&#100;&#97;&#110;&#111;&#119;&#115;&#107;&#105  
&#46;&#112;&#108;">bartek(na) danowski.pl</a>
```

Adres występujący po słowie *mailto* można również zapisać za pomocą kodowania %HEX. Niestety, ten sposób kodowania jest często wykorzystywany do innych celów i istnieje duże prawdopodobieństwo, że tak zakodowany adres zostanie niejako „mimoходом” rozkodowany przez jakąś aplikację używaną przez spamera, a następnie wpisany do bazy danych. Dlatego naszym zdaniem nie warto używać tej metody do zwykłego zapisu adresu na stronie WWW. Oczywiście można pokusić się o użycie kodowania %HEX w połączeniu z odpamiaczem czy też encjami.

- ◆ Zwykły adres:

```
bartek@danowski.pl
```

- ◆ Adres kodowany za pomocą %HEX:

```
%62%61%72%74%65%6B%40%64%61%6E%6F%77%73%6B%69%2E%70%6C
```

Udostępniając adres e-mail na stronie WWW możesz go również zakodować za pomocą metody ROT13. Jednak rozwiązanie to nie jest zbyt wygodne dla odwiedzającego, który jest zmuszony do skorzystania z jakiegoś narzędzia do rozkodowania adresu lub „ręcznego” przeliczenia i podmiany liter. Niestety, większość użytkowników sieci jest przyzwyczajoną do tego, że klika adres e-mail dostępny na stronie i czeka na otwarcie się okna klienta pocztowego. Użycie ROT13 uniemożliwia użytkownikowi korzystanie z dotychczasowych przyzwyczajeń i z tego powodu nie warto sięgać po tę metodę.

Pamiętaj, że zabezpieczając się przed spamem nie możesz przesadzić i utrudnić innym użytkownikom pisania do Ciebie. Jeżeli gość Twojej strony w celu wysłania listu z informacją, że odwiedził stronę i że podobało mu się bardzo, będzie zmuszony do wykonania wielu magicznych sztuczek, raczej zrezygnuje z pisania do Ciebie. Dlatego zabezpieczając się przed spamem pamiętaj o wygodzie użytkownika Twojego zabezpieczenia.

### • Użycie grafiki

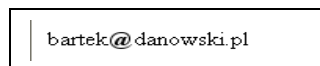
Używając obrazka można na stronie udostępnić cały adres zapisany w postaci gif, dzięki czemu adres będzie idealnie zabezpieczony. Na dzień dzisiejszy nie ma możliwości zeskanowania adresu z obrazka. Niestety, również tym razem problem pojawia się w chwili, gdy chcesz, aby klikając obrazek można było otworzyć okno programu pocztowego. Najprostszym i najskuteczniejszym zabezpieczeniem adresu e-mail jest zapisanie go w postaci obrazka – najlepiej do tego celu nadają się formaty *gif* lub *png* – i w takiej formie udostępnienie na stronie – oto przykład:

```

```

Wspominaliśmy, że roboty skanujące sieć i zbierające adresy e-mail są wyczułone na pewne znaki i słowa. Najważniejszym znakiem na który polują „źniwiarki” jest popularna małpa @ (poprawna nazwa to *at*). Poza tym bardziej zaawansowane roboty poszukują słowa *mailto* w kodzie strony. Można zatem skorzystać z prostego rozwiązania polegającego na zastąpieniu jedynie znaku @ przez obrazek zapisany w formacie *gif*. Przyjrzyj się naszemu przykładowi oraz rysunkowi 5.4.

```
bartek danowski.pl*



*Rysunek 5.4. Przykład zastosowania znaku @ w postaci obrazka w formacie gif*

Rozwiązanie takie jest bardzo bezpieczne, jednak należy pamiętać, że połączenie go z odnośnikiem uruchamianym kliknięciem powoduje obniżenie skuteczności. Dlatego jeżeli zależy Ci na tym, by można było kliknąć odnośnik na stronie WWW, warto obrazek połączyć z zakodowaniem słowa *mailto* oraz adresu występującego po nim używając do tego celu encji. Warto też dodać, że jest wskazane używanie nazw plików graficznych, które (w wypadku użycia „sprytnego” harwestera) nie kojarzyłyby się z plikiem zastępującym fragment adresu – dlatego w powyższym przykładzie grafika przedstawiająca znak @ nie nazywa się „at.gif” ani „malpa.gif”.

#### • Użycie JavaScriptu

Ciekawym sposobem zabezpieczenia adresu e-mail może być zastosowanie do tego celu JavaScript. Przedstawiliśmy kilka gotowych skryptów wraz z naszymi komentarzami. Niestety, żadne z opisanych przykładów zastosowania JavaScript do ochrony adresów nie będą działały w sytuacji, gdy odwiedzający stronę w swojej przeglądarce ma wyłączoną obsługę JavaScript lub przeglądarkę, która w ogóle nie go obsługuje. Na szczęście, zdecydowana większość ludzi korzysta z JavaScript – wedle stosunkowo wiarygodnych pomiarów z kilku witryn o bardzo różnej tematyce odsetek ten wynosi od 94% do 98%.

```
<SCRIPT language="JavaScript" type="text/javascript">
```

```
<!-- Original: CDR Software -->
<!-- Web Site: http://www.cdrsoft.com/ -->
<!-- This script and many more are available -->
<!-- free online at The JavaScript Source !! -->
<!-- http://javascript.internet.com/ -->
<!-- Begin
user = "xxx";
site = "yyy.zzz.pl";
document.write('<a href="\&#109;&#97;&#105;&#108;&#116;&#111;&#58;
'+user+'&#64;'+site+'\">');
document.write(user+'&#64;'+site+'</a>');
// End -->
</SCRIPT>
```

W tym przypadku adres e-mail będzie sklepany z dwóch części wypisanych na początku skryptu w liniach zaczynających się od *user* oraz *site*. W oryginalnym skrypcie wprowadzono kilka zmian polegających na zakodowaniu słowa *mailto* oraz znaku @ za pomocą encji – ma to na celu poprawienie skuteczności ochrony.

Jeżeli chcesz skorzystać z tego skryptu na swojej stronie, to musisz go w całości wkleić w miejscu, gdzie ma pojawić się adres e-mail. Następnie w polu *user* zamiast znaków *xxx* wpisz Twój login występujący przed znakiem @ w adresie. Natomiast w linii *site* zamiast *yyy.zzz.pl* wpisz domenę występującą po znaku @.

Przyjrzyj się kolejnemu przykładowi zastosowania JavaScriptu do zakodowania adresu e-mail.

```
<SCRIPT language="JavaScript" type="text/javascript">
```

```
<!-- Begin //
pr_1 = "mai";
pr_2 = "lto:";
login = "xxx";
at = "&#64;";
serwer = "yyy.zzz.pl";
document.write('<a href=\'\'+pr_1+pr_2+login+at+serwer+\'\'>');
document.write(login+at+serwer+\'</a>');
// End -->
</SCRIPT>
```

Tym razem jest to nieco bardziej zaawansowany skrypt, który skleja cały adres z pięciu części. Zaletą jest łączenie słowa *mailto* z dwóch części oraz zastąpienie znaku @ za pomocą encji. Aby wykorzystać ten skrypt na swojej stronie, musisz w linii *login* zastąpić xxx swoim loginem (to nazwa występująca przed znakiem @ oryginalnego adresu e-mail). Następnie w linii *serwer* zamiast *yyy.zzz.pl* wpisz domenę występującą po znaku @ w oryginalnym adresie e-mail. Zmodyfikowany skrypt wstaw w miejscu, w którym chcesz umieścić adres.

Jeszcze jeden przykład zastosowania JavaScriptu do zabezpieczenia adresu.

```
<SCRIPT language="JavaScript" type="text/javascript">
<!-- // Begin
document.write("<A HREF=\"mailto:xxx\"+String.fromCharCode(64));
document.write("yyy.zzz.pl\">mój adres</A>");
// End -->
</SCRIPT>
```

Tym razem musisz odszukać ciąg znaków xxx i zastąpić go nazwą występującą przed znakiem @ w oryginalnym adresie. Następnie zamiast *yyy.zzz.pl* wpisz

domenę występującą w oryginalnym adresie po znaku @. Tak zmodyfikowany skrypt wstaw do kodu strony w miejscu, w którym ma być adres e-mail.

Na koniec zostawiliśmy prawdziwą perłkę, jeśli chodzi o zabezpieczenie adresu e-mail za pomocą JavaScriptu.

Na stronie <http://www.jracademy.com/~jtucek/email/> jest dostępny specjalny generator kodu JavaScript, korzystający z szyfrowania RSA. Rozwiązanie to jest w stu procentach bezpieczne i nie ma możliwości, by tak zabezpieczony adres trafił w ręce spamera. Dlatego pozwoliliśmy sobie szerzej opisać wykorzystanie tego generatora oraz skryptu na stronie WWW.

Najpierw wejdź na stronę

<http://www.jracademy.com/~jtucek/email/download.php>.

Następnie odzyskaj część formularza widoczną na rysunku 5.5.

**Make a key:**

First you need to select 2 prime numbers that will make up the encryption/decryption key. They must be different numbers, and their product, N, must be greater than 255.

P: 197 The first prime number used to make the key.  
Q: 2 The second prime number used to make the key.

**Enter your Email Address:**

bartek@coig.pl

I need this in order for the JavaScript to encrypt it. In no way is your email address stored or given away. All the calculations are run on *your* computer, not the server. Once it's been encrypted, the address is forgotten, so don't worry about me giving it out to spammers or something evil like that.

**Subject Line (optional)**

A lot of people have requested this, so here it is. Anything you put there will automatically be put into the subject line when somebody clicks on your "Mail Me" link. If you don't want to do that, just leave this field blank. If you do type something there, please only use letters, numbers, and spaces in the subject line. Single quotes are ok too, but not double quotes. And question marks are sure to mess things up.

**Encrypt It**

Click the button, and you're almost done!

Encrypt

**Rysunek 5.5. Zabezpieczenia adresu e-mail za pomocą JS i RSA – etap pierwszy**

W polach oznaczonych literami *P* oraz *Q* ustaw dwie liczby, a następnie poniżej wpisz adres e-mail, który chcesz zabezpieczyć. Dodatkowo możesz podać stały temat wiadomości, ale nie jest to konieczne.

Po kliknięciu przycisku *Encrypt* rozpocznie się generowanie Twojego klucza, za pomocą którego adres będzie szyfrowany.

W polach widocznych na rysunku 5.6 znajduje się Twój prywatny i publiczny klucz RAS, za pomocą którego zostanie zakodowany adres e-mail.

**Encrypt It**

Click the button, and you're almost done!

**The Technical Stuff:**

| Public                                   | Private                             |
|------------------------------------------|-------------------------------------|
| N: <input type="text" value="1379"/>     | P: <input type="text" value="197"/> |
| E: <input type="text" value="5"/>        | Q: <input type="text" value="7"/>   |
| C: <input type="text" value="868 1119"/> | D: <input type="text" value="941"/> |

In case you wanted to know, N is equal to P\*Q. N, the public key, only has 2 possible factors other than itself and 1, so finding out P and Q from N can take a long time, depending on how large N is. P and Q are private keys, which are needed to break the encryption. E is an exponent used in creating the encrypted string C, and in creating the decryption key, D.

*Rysunek 5.6. Zabezpieczenia adresu e-mail za pomocą JS i RSA – etap drugi*

Na rysunku 5.7 widać kolejny formularz dostępny na stronie. Tym razem kliknij przycisk *Decrypt* i sprawdź, czy Twój adres został poprawnie rozkodowany. Jeżeli tak, to możesz przejść dalej.

**Test Decryption:**

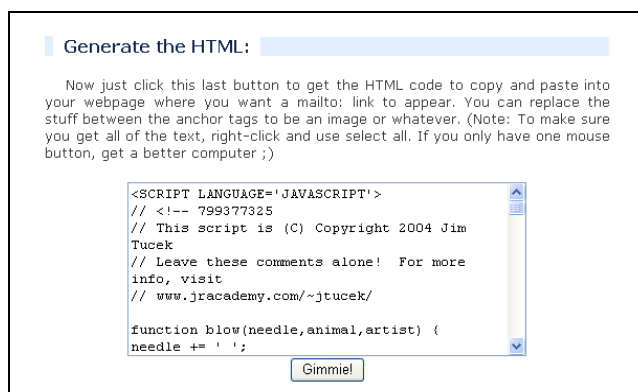
Just to make sure everything worked out all right. If not, [contact me](#) or try changing the prime numbers.

Encrypted:

Decrypted:

*Rysunek 5.7. Zabezpieczenia adresu e-mail za pomocą JS i RSA – etap trzeci*

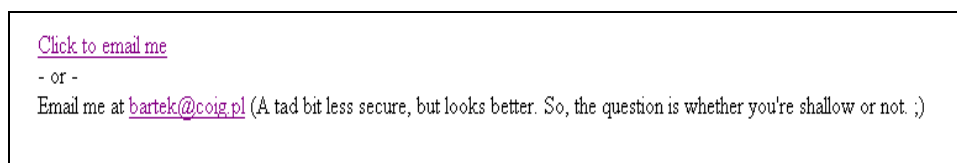
Ostatnią czynnością, jaką musisz wykonać, jest wygenerowanie kodu HTML, który musisz wstawić na swojej stronie. W tym celu odszukaj formularz widoczny na rysunku 5.8, a następnie kliknij przycisk *Gimmie*.



*Rysunek 5.8. Zabezpieczenia adresu e-mail za pomocą JS i RSA – etap czwarty*

Po chwili w oknie formularza pojawi się gotowy JavaScript. Wystarczy, że go skopiujesz i wkleisz na swojej stronie WWW, a Twój adres będzie profesjonalnie zabezpieczony i niemożliwy do pozyskania przez spammerskie roboty.

Na rysunku 5.9 zamieściliśmy wyniki działania domyślnie wygenerowanego skryptu. Oczywiście dodatkowy opis widoczny na rysunku można poddać zmianie, ale jest to rzecz bardzo prosta i każdy użytkownik poradzi sobie z tym bez większych problemów nawet bez znajomości JavaScript.



*Rysunek 5.9. Wynik działania domyślnego skryptu*

- **Flash, formularze, CGI**

Innym sposobem zabezpieczenia adresu e-mail na stronie WWW jest zapisanie go w postaci animacji Flash. Rozwiązanie to pozwala na stworzenie uruchomianego kliknięciem odnośnika do adresu, a przy tym całkowitą eliminację adresu e-mail oraz słowa *mailto* z kodu HTML strony WWW. Minusem tego rozwiązania jest konieczność instalacji specjalnej wtyczki pozwalającej na odtwarzanie animacji. Dodatek taki jest dostarczany każdej chyba przeglądarce graficznej, jednak trzeba pamiętać, że nie wszyscy go instalują. Na nasze szczęście jest to bardzo niewielki odsetek internautów.

Kolejnym sposobem ochrony adresu e-mail jest jego całkowite oddzielenie od strony przy wykorzystaniu zaawansowanych skryptów pisanych w PHP czy CGI. Skrypt powinien pobierać adres bezpośrednio ze swojego pliku konfiguracyjnego i adres odbiorcy powinien być w nim zdefiniowany na sztywno, aby uniemożliwić wykorzystanie formularza do wysyłania spamu.

Wiele gotowych skryptów znajdziesz na stronie <http://php.resourceindex.com> oraz <http://cgi.resourceindex.com>, a jednym z najpopularniejszych jest FormMail. Należy jednak pamiętać o tym, by nie wpaść z deszczu pod rynną. Okazuje się bowiem, że źle napisane skrypty typu FormMail mogą posłużyć jako bramka do wysyłania spamu, co może spowodować nieprzyjemności na właściciela strony, na której zamieszczono taki dziurawy formularz. Dlatego trzeba sprawdzić w opisie wybranego skryptu, czy ma on odpowiednie zabezpieczenia i wtedy ewentualnie z nich skorzystać.

Jeżeli znasz się na programowaniu, możesz samodzielnie napisać własny skrypt, którego zadaniem będzie oddzielenie adresu e-mail od strony WWW.

Pamiętaj, że formularz kontaktowy na stronie jest sporym ułatwieniem dla właściciela strony, jednak utrudnieniem dla odwiedzających i dlatego nie każdy z niego korzysta. W związku z tym na stronie firmowej musisz przewidzieć inne możliwości nawiązania kontaktu. Natomiast na stronie

prywatnej możesz pozwolić sobie na odrobinę luksusu i udostępnienie tylko jednej metody kontaktu.

W przypadku każdej strony warto przygotować sobie regulamin wykorzystania swojego adresu. Regulamin taki powinien zawierać definicję tego, co uznajesz za spam, określać, w jakim celu udostępniłeś swój adres, ostrzegać o konsekwencjach, jakie płyną z przysyłania do Ciebie spamu. Taki regulamin może być bardzo krótki, np. „na ten adres prosimy przysyłać tylko zapytania o nasze towary”, albo bardzo rozbudowany. Przykład takiego rozbudowanego regulaminu znajdziesz na stronie <http://nospam-pl.net/kontakt.php>.

#### • Aliasy pocztowe

Jeżeli uznałeś, że wszystkie opisane przez nas metody zabezpieczenia adresu na stronie WWW oraz grupach dyskusyjnych są zbyt skomplikowane, czasochłonne i pracochłonne, to pozostaje Ci jeszcze jedna możliwość zabezpieczenia swojego adresu. Rozwiązanie to polega na ukryciu prawdziwego adresu przed spamerem i udostępnienie aliasu<sup>4</sup>. Alias pocztowy to dodatkowy adres skrzynki e-mailowej. Często jest on oferowany za darmo jako dodatek do kont komercyjnych. Zamiast właściwego adresu można posługiwać się wtedy aliasem, który może być dowolnie zmieniany. W ten sposób nikt nie pozna prawdziwego adresu, a mimo to poczta od osób znających aktualnie obowiązujący alias będzie cały czas służyła na to samo konto. Nawet, jeżeli nie masz możliwości korzystania z aliasów przy swoim koncie – nic straconego, w wielu miejscach można za darmo lub za niewielką opłatą uzyskać aliasy. Aliasem można posługiwać się tak samo jak adresem publicznym, a co lepsze, przy takim rozwiązaniu poczta będzie cały czas służyła na to samo konto podstawowe – trzeba tylko pamiętać, by odpowiadając na e-mail zawsze używać aktualnego aliasu i nikomu nie ujawnić adresu podstawowego.

---

<sup>4</sup>*Alias* – adres e-mailowy, który nie jest sam w sobie kontem e-mailowym, a jedynie przekierowuje pocztę wysyłaną na konto, z którego poczta jest odbierana.

Alias nie zabezpiecza Cię przed otrzymywaniem spamu, a jedynie pozwala na ukrycie przed spamerem Twojego prawdziwego adresu. Stosowanie aliasu w ochronie przed spamem powinno wyglądać mniej więcej tak, że danego aliasu używa się do chwili, gdy zaczniesz na niego dostawać duże ilości spamu. Wtedy zmieniasz alias na inny, a „spalony” adres można przekonfigurować tak, by zwracał pocztę do nadawcy. Wszystkim zainteresowanym pozwoliliśmy sobie podać adresy kilku firm oferujących darmowe bądź odpłatne aliasy.

<http://www.prv.pl>

<http://www.spammotel.com/spammotel>

<http://www.spamgourmet.com>

<http://www.spamcon.org>

<http://sneakemail.com>

Na koniec przygotowaliśmy jeszcze kilka ważnych rad i ostrzeżeń dla wszystkich użytkowników poczty elektronicznej. Jeżeli zastosujesz się do punktów zamieszczonych poniżej, poprawisz bezpieczeństwo Twojego adresu.

- ◆ Nigdy nie podawaj swojego adresu nieznanym bez wyraźnej konieczności. Często nieznanymi zbierają adresy, a następnie wysyłają na nie spam lub sprzedają je jako towar większym spammerom.
- ◆ Zanim wpiszesz swój adres do formularza na stronie, zastanów się dwa razy, czy to jest konieczne. Wiele stron stanowi jedynie przykrywkę do zbierania adresów i spamowania ich.
- ◆ Nigdy nie odpisuj na spam i nie staraj się wypisywać z list, ponieważ wielu spammerów stosuje oszustwa w celu sprawdzenia, czy dany adres działa. Jeżeli w stopce spamu widzisz instrukcję wypisania się z listy, w praktyce oznacza to, że po wykonaniu poleceń tam zawartych trafisz do bazy zweryfikowanych adresów i zaczniesz dostawać jeszcze więcej spamu.
- ◆ Nie odpowiadaj na spam spamem, gdyż staniesz się taki jak spamerzy.

## ROZDZIAŁ 9.

### Rady dla stawiających pierwsze kroki w e-biznesie

Do tej pory pisaliśmy o tym, jak zachowują się spamerzy i jak z nimi walczyć. Jednak zdajemy sobie sprawę z tego, że sieć jest doskonałym miejscem do prowadzenia biznesu. Każdego dnia powstają tysiące nowych witryn, przybywa nowych użytkowników oraz osób startujących w e-biznesie. Każdemu, kto stawia pierwsze kroki, zdarza się popełniać błędy. Aby uchronić przedsiębiorców przed łatką spamera, w niniejszym rozdziale opisujemy, w jaki sposób zbierać adresy e-mailowe i rozsyłać reklamy w sposób zgodny z obowiązującym prawem i dobrymi obyczajami.

Zachęcamy do uważnego przeczytania tego rozdziału szczególnie przez wszystkich e-biznesmenów liczących na szybki zysk w sieci. Warto zastosować się do poniższych porad, bo ułatwia to zbudowanie solidnej marki i pomaga zarobić w internecie nie narażając się na zszarganie opinii firmy. Jednak zbudowanie dobrej marki zawsze trwa, a „szybki zysk” najczęściej oznacza dalekosiężną stratę.

Postanowiliśmy skupić się tylko na jednym przykładzie. Nasz wybór padł na zasady gromadzenia adresów e-mailowych oraz wysyłkę na te adresy przesyłek reklamowych. Uznaliśmy, iż to główne pole do nadużyć i nieprawidłowości ze względu na ogromną popularność tej formy informowania o produktach, promocjach i ofertach.

Jeżeli stawiasz pierwsze kroki w sieciowym biznesie, to prędzej czy później zaczniesz myśleć o wykorzystaniu poczty elektronicznej do informowania

potencjalnych klientów o swoich usługach i oferowanych produktach. Zamierzenie słuszne i pozwalające na skorzystanie z dobrodziejstw nowoczesnej komunikacji, jednak wiele osób w tym momencie zaczyna popełniać błędy, które w przyszłości zaczną się mścić. Wynika to z faktu, iż wielu początkujących e-biznesmenów zaczyna pozyskiwać adresy e-mailowe w nieprawidłowy sposób. Zazwyczaj do bazy dodają jak leci adresy, jakie mają w skrzynce e-mailowej, jakie znajdą na grupach dyskusyjnych lub stronach WWW lub kupują bazy danych adresowe.

Taki sposób działania jest nieprawidłowy – w ten sposób narusza się dobre obyczaje i łamie prawo. Aby działać zgodnie z prawem, należy zadbać o to, by potencjalni klienci sami zapisali się i zamówili Twój biuletyn informacyjny. Wbrew pozorom, nie jest to takie trudne, a i zainteresowani powoli dopisują swoje adresy do odpowiedniej bazy. Ta forma działania musi przebiegać według ściśle określonych zasad, o których napisaliśmy w następnych podrozdziałach.

## Listy opt-in i opt-out

Jeśli już masz witrynę, która będzie za darmo promowana przez wyszukiwarki internetowe, trzeba zatroszczyć się o osoby, które się nią zainteresują i witrynę odwiedzą. Możliwe, że nie znajdą na niej od razu tego, co potrzebują, ale można im zaproponować, że będą informowani o nowościach w ofercie poprzez mniej lub bardziej regularnie rozsyłany biuletyn informacyjny. Taki biuletyn rozsyła się najczęściej za pomocą programu obsługującego *listę mailingową*.

W sieci spotykasz dwa typy list mailingowych. Pierwszy rodzaj list mailingowych to listy typu *opt-out*, które nie cieszą się dobrą opinią i w wielu przypadkach stanowią naruszenie prawa obowiązującego w naszym kraju. Zasada działania takiej listy wygląda tak, że jej właściciel sam dodaje do bazy adresy e-mailowe, a właściciel tak dopisanego adresu musi się wypisać z listy, jeśli nie jest zainteresowany przesyłkami (następnie znów jest dopisywany do

kolejnej listy, z której znów musi się wypisać, i znów, i znów, i znów...). W takim przypadku właściciel listy nie wie, czy osoba dodana do listy życzy sobie odbierać przesyłki. Wydawać by się mogło, że lista typu opt-out może zostać wykorzystana w zgodzie z prawem do wysłania zapytania o zgodę na przesłanie materiałów reklamowych. W praktyce tak nie jest, gdyż zgodnie z *Ustawą o świadczeniu usług drogą elektroniczną* wolno wysyłać materiały promocyjne tylko do tych adresatów, którzy wyrazili na to zgodę **przed jakąkolwiek** wysyłką – w praktyce do tych odbiorców, którzy albo o takie materiały poprosili, albo którzy wyrazili zainteresowanie przy okazji innych kontaktów. Dodatkowo odbiorca ma prawo zażądać okazania dowodu (potwierdzenia) wyrażonej przez siebie zgody, a więc nadawca musi taki dowód posiadać. Inaczej mówiąc, nie można użyć listy opt-out do wysłania zapytania o zgodę na przesłanie materiałów firmy do właścicieli wszystkich adresów z listy, gdyż czyn taki jest naruszeniem prawa.



Zakup bazy danych z adresami e-mailowymi oraz jej wykorzystanie jest przykładem użycia metody opt-out.

---

Drugim typem listy, tym razem jednak zgodnym z prawem i dobrymi obyczajami, jest rozwiązanie o nazwie *opt-in*. Ten rodzaj listy polega na tym, że każda zainteresowana osoba sama zapisuje się i zamawia materiały reklamowe. Sam sposób pozyskiwania adresów do listy opt-in został przez nas szerzej opisany w następnym podrozdziale.

Lista opt-in jest zgodna z prawem i zalecana m. in. przez odpowiednie dyrektywy Unii Europejskiej, a przy okazji rozwiązuje problem indywidualnej zgody na otrzymywanie materiałów reklamowych, jaka jest wymaga przez wielokrotnie wspomnianą ustawę o świadczeniu usług drogą elektroniczną. Wystarczy, że obok mechanizmu pozwalającego na zapisanie się do listy zamieścisz stosowny regulamin, w myśl którego zapisanie się do listy będzie równoznaczne z wyrażeniem zgody na otrzymywanie Twoich reklam.

## Po pierwsze – witryna internetowa

Potrzebna jest zatem lista typu *opt-in*. Aby uruchomić taką listę, będzie przede wszystkim potrzebna witryna internetowa, która pozwoli na dotarcie przez internet do potencjalnych klientów. Witryna, która w sposób możliwie dokładny, precyzyjny i przystępny będzie objaśniała, co dany przedsiębiorca ma do zaoferowania. Jest to niezwykle ważny etap i nie warto wykonania strony internetowej powierzać „znajomemu studentowi”, który być może wykona ją za niewielkie pieniądze – ale też witryna taka nie ściągnie do jej właściciela dużych pieniędzy albo drogie będzie jej wypromowanie. Natomiast dobrze przygotowana strona będzie promować się sama lub można ją promować za darmo. Na rynku jest wiele niewielkich firm robiących witryny internetowe za niewielką nawet opłatą, można zwrócić się do kilku z nich, przede wszystkim prosząc o przedstawienie stron już zrobionych.

Dobra strona internetowa to nie znaczy strona „atrakcyjna” – z migającymi napisami, kolorowymi obrazkami i animowanym menu. Dobra strona internetowa to taka, którą łatwo znaleźć w internecie, zatem strona powinna być przyjazna dla serwisów wyszukiwawczych (takich jak Google <http://www.google.pl/>) oraz dla osób odwiedzających ją. Taka strona powinna posiadać czytelnie uszeregowane informacje, z wykorzystaniem wszystkich elementów kodu HTML<sup>5</sup>, a więc z odpowiednimi nazwami stron, tytułami, podtytułami akapitami tekstu, które będą opisywały oferowane produkty i usługi. Tak przygotowaną stronę należy zarejestrować w wyszukiwarkach internetowych i w prowadzonych przez popularne portale internetowe katalogach tematycznych stron – oczywiście, w precyzyjnie dobranych kategoriach, których zwykle możesz wykorzystać nie więcej niż 2 lub 3. Dzięki temu zapewnisz sobie zupełnie darmową promocję witryny.

Gdy ktoś szuka w tych serwisach określonej witryny, zwykle są one porządkowane według zawartości merytorycznej, dlatego niezmiernie ważne jest, by strona była na temat. Za każdy element strony wyszukiwarka

<sup>5</sup>Język, w którym pisze się strony internetowe. Więcej na ten temat na stronie <http://www.w3c.org>.

internetowa dolicza punkty, przypisywane występującym na stronie słowom. Wyszukiwarka ta następnie analizuje teksty znajdujące się na stronie i w sposób statystyczny „wylicza”, czego ta strona dotyczy. Jeśli na stronie często będzie powtarzało się słowo „super”, wyszukiwarka wyliczy, że strona jest na temat „super” – i tę stronę zaproponuje komuś, kto w internecie będzie szukał „czegoś super” (mało precyzyjne, nieprawdaż?). Jeśli w odnośnikach prowadzących do witryny oraz w tytułach i treści będą się powtarzały w różnych formach słowa „różowe słonie” – wyszukiwarka wyliczy, że strona dotyczy właśnie tych zagadnień i osobie szukającej takich usług tę właśnie stronę zaproponuje. Jakkolwiek egzotyczna byłaby Twoja oferta, można w ten sposób dotrzeć wprost do osób zainteresowanych, nie marnując środków marketingowych i czasu na promocję trafiającą często do osób, które nie są zainteresowane zwierzętami.

Skoro już klient dotarł na tę stronę, trzeba zadbać o to, by nie zapomniał o Twojej ofercie. Zaproponuj mu zatem, by powierzył Ci swój adres, upoważniając Cię do regularnej wysyłki Twoich biuletynów z promocjami, cenników itp.

### **Uruchamiasz listę opt-in**

Trzeba wiedzieć, że nie wystarczy na stronie WWW zamieścić okienka pozwalającego na dodanie dowolnego adresu e-mailowego, gdyż daje to pole do nadużyć i w prostej linii prowadzi do tego, że trafisz na publiczne czarne listy. Nie martw się jednak zbytnio, gdyż stworzenie prawidłowo działającej listy opt-in nie jest skomplikowane i doskonale nadają się do tego darmowe skrypty dostępne w sieci. W dalszej części pokażemy, gdzie szukać dobrych i gotowych rozwiązań.

Każda lista typu opt-in musi posiadać zabezpieczenia uniemożliwiające wykorzystanie jej do zrobienia komuś głupiego żartu lub wykorzystania bazy adresów przez spamera. W związku z tym proces subskrypcji musi składać się z kilku etapów. Poniżej w punktach wypisaliśmy poszczególne etapy:

1. Osoba chcąc zapisać się na listę (zarejestrować się w bazie mailingowej) w celu otrzymywania zamówionych materiałów marketingowych wpisuje swój adres w polu formularza na stronie WWW.
2. Na wpisany do formularza adres e-mailowy jest wysyłany list z prośbą o potwierdzenie chęci otrzymywania takich materiałów. List zawiera pewne istotne informacje, o których za chwilę, oraz unikalny i niemożliwy do odgadnięcia kod aktywacyjny (hasło), który trzeba odesłać, by rejestracja była ważna.
3. Osoba zapisująca się musi potwierdzić chęć otrzymywania informacji reklamowych, odsyłając kod lub wpisując go na stronie WWW. Kod może być podany w postaci odnośnika hipertekstowego (linku), który wystarczy po prostu kliknąć.
4. Po dokonaniu potwierdzenia na adres nowego subskrybenta można wysłać potwierdzenie pomyślnego zakończenia procesu rejestracji.

Jak widzisz, cała operacja składa się z kilku etapów, dzięki czemu likwiduje się możliwość powstania nadużyć. Kod aktywacyjny jest wysyłany wyłącznie na adres wpisany do formularza i tylko właściciel tego adresu może odczytać odpowiednią pocztę i aktywować wpis w bazie.

Newralgiczny dla całej operacji jest etap 2. tego procesu. List, który trafi do osoby chcącej się zapisać, poza kodem aktywnym musi zawierać następujące informacje:

1. Kilka słów na temat tego, dlaczego list trafił na to konto. Warto napisać, że wiadomość została jednorazowo wysłana w celu weryfikacji na adres wpisany do formularza na stronie dostępnej pod konkretnym adresem. W treści wstępu należy podać adres e-mail oraz adres strony WWW, na której rozpoczęto procedurę aktywacji.

2. Koniecznie zaznacz, że jeżeli ktoś zrobił głupi żart, to aby uniknąć zapisania się do listy, należy zignorować wiadomość i nie klikać żadnych odnośników widocznych w dalszej części. Nie zaszkodzi przeprosić za kłopot, jaki sprawiła Twoja wiadomość, a z całą pewnością zostawisz po sobie dobre wrażenie i być może zachęcisz część osób, by jednak zamówiły Twoje oferty.
3. Celem umożliwienia weryfikacji podaj niektóre okoliczności dokonania rejestracji: dzień, dokładna godzina, adres IP komputera, z którego dokonano wpisu. Dane te nie tylko Cię uwiarygodnią, ale również pozwolą wyśledzić sprawcę ewentualnej próby dopisania do bazy cudzego adresu.
4. W kilku słowach opisz, jakiego typu informacje będziesz wysyłał. Wyraźnie zaznacz, ile razy w miesiącu są rozsyłane Twoje reklamy. W ten sposób unikniesz problemów związanych z niedoinformowaniem osób, które się zapisały, bo myślały, że będą dostawać jedną reklamę raz na pół roku. Lepiej napisać, że rozsyłasz więcej reklam niż ma to miejsce faktycznie.
5. Bardzo dokładnie opisz, jak wygląda procedura rezygnacji i wypisania się z Twojej listy mailingowej. Przedstaw przynajmniej dwa warianty rezygnacji.
6. Opisz, co należy zrobić, aby aktywować zgłoszenie. Umieść odpowiedni odnośnik aktywujący wpis w bazie. Pamiętaj, że jego konstrukcja musi być taka, aby działała poprawnie w każdych warunkach. W przeciwnym wypadku stracisz potencjalnego klienta.
7. Napisz kilka słów o tym, jaka jest Twoja polityka odnośnie gromadzonej bazy adresów. Nie zapomnij powiadomić osoby, która chce się zapisać na Twoją listę, że baza jest przeznaczona wyłącznie na Twój użytek i nie będzie udostępniania nikomu innemu. Pamiętaj, że zgoda, jaka została Tobie udzielona, dotyczy otrzymywania ofert reklamowych tylko z Twojej listy i nie obowiązuje ona w żadnym innym przypadku.

8. Podaj adres e-mail, z jakiego będzie przychodzić poczta reklamowa. Pamiętaj, że tego adresu nie możesz zmienić. Jeżeli zajdzie nieprzewidziana okoliczność i zostaniesz zmuszony do zmiany, to odpowiednio wcześniej powiadom o tym odbiorców Twojej oferty.
9. Podaj dane kontaktowe do osoby administrującej listą. Pamiętaj o tym, że wielu adresatów Twoich ofert będzie miało problemy i warto poświęcić chwilę, aby im pomóc.

Wiadomość, jaka zostanie wysłana do nowego subskrybenta po zakończeniu rejestracji, nie musi być już tak długa, wystarczy, że za jej pomocą powiadomisz o pomyślnym zakończeniu całego procesu.

Jak widzisz, proces dodawania oraz weryfikacji jest dość skomplikowany, ale w praktyce da się to tak zrobić, by całość operacji odbywała się automatycznie. Nie oznacza to jednak, że osoba administrująca listą jest zbędna. Wręcz przeciwnie, musi ona bowiem nadzorować pracę skryptów i sprawdzać, czy nie występują jakieś nieprawidłowości.

Bardzo ważne jest, aby odbiorcy Twoich ofert zapewnić *skuteczne* metody wypisania się z listy mailingowej. Koniecznie musisz przygotować przynajmniej dwa możliwe sposoby wypisania się z bazy. W podpunktach opisaliśmy, w jaki sposób powinien wyglądać profesjonalnie przygotowany system rezygnacji.

1. Każdy rozestany biuletyn informacyjny powinien zawierać informacje o sposobie rezygnacji z otrzymywania kolejnych wiadomości. W praktyce powinno to być zrobione w ten sposób, że na końcu wiadomości znajduje się krótka notatka na temat wypisania się z listy oraz hipertączę o podobnej konstrukcji do tego, jaki zastosowano podczas weryfikacji dodawanego adresu – tyle, że tym razem odnośnik ten będzie zgłaszał chęć wypisania się z listy.

2. Po kliknięciu odsyłacza osoba, która chce zrezygnować z dalszej subskrypcji, otrzyma e-mail na adres zapisany w bazie. W wiadomości powinna znajdować się informacja o tym, dlaczego ten e-mail trafił na adres odbiorcy. Po kilku słowach wyjaśnienia przyczyny otrzymania tej wiadomości musisz opisać, w jaki sposób dalej należy postępować w celu usunięcia adresu z bazy. Pod instrukcją zamieść kod potwierdzający chęć usunięcia adresu. Po jego kliknięciu adres powinien zostać usunięty z Twojej listy mailingowej, a osoba rezygnująca powinna otrzymać kolejną wiadomość e-mail z informacją o pomyślnym zakończeniu całej operacji.
3. Poza automatycznym sposobem usunięcia adresu z bazy musisz przewidzieć również metodę awaryjną. W każdej rozсланej ofercie zamieść informacje na ten temat. Możesz to rozwiązać poprzez podanie adresu kontaktowego do administratora bazy mailingowej. Przedstaw zasady postępowania i dopilnuj, aby ta metoda działała szybko i skutecznie.

Pamiętaj, że *skuteczny i działający* system wypisywania się z listy mailingowej jest rzeczą szalenie ważną. Nie ma rzeczy bardziej denerwującej użytkowników internetu niż listy mailingowe, z których nie da się wypisać. Jeżeli doprowadzisz do takiej sytuacji, to musisz się liczyć z tym, że prędzej czy później zostaniesz wpisany na czarne listy lub jakiś zniecierpliwiony internauta wytoczy Ci proces, który z dużym prawdopodobieństwem przegrasz.

Wiesz już, w jaki sposób powinny działać mechanizmy odpowiedzialne za dodawanie i usuwanie adresów z Twojej listy mailingowej. Teraz przyszła pora, abyś dowiedział się, co powinno obowiązkowo znajdować się w każdej z ofert. Oczywiście nie będziemy tutaj poruszać sprawy samej treści reklamowej, gdyż jest to Twoją indywidualną sprawą, ale mamy na myśli elementy stałe każdej oferty. Przyjrzyj się punktom, jakie zamieściliśmy, i pamiętaj, że w tym przypadku ich kolejność ma istotne znaczenie.

1. Zaczynij od przywitania się z czytelnikiem.
2. Napisz, skąd pochodzi biuletyn i dlaczego znalazł się w skrzynce odbiorcy. Może się zdarzyć, że Twój subskrybent zapomniał, że zamawiał u Ciebie informacje o ofercie i dlatego należy mu to przypomnieć na samym początku wiadomości, najlepiej wraz z datą rejestracji w bazie.
3. Umieść treść swojej oferty.
4. Podaj informacje na temat sposobu wypisania się z Twojej listy mailingowej. Opisz przynajmniej dwa rozwiązania.
5. Umieść dane kontaktowe osoby zarządzającej listą.
6. Podziękuj za poświęcony Ci czas.

Pamiętaj o tym, aby zabezpieczyć dostęp do bazy danych oraz systemu wysyłki biuletynów, tak by niepowołane osoby nie miały do niego dostępu. To bardzo ważne, gdyż wpadka może Cię drogo kosztować. Z tego względu również bezwzględnie musisz zadbać o to, by w wysyłanych mailingach nie było zawartych adresów innych odbiorców – zatem mailingi muszą być wysyłane albo na zasadzie „każdy list do jednego odbiorcy” (adres odbiorcy w polu *To:* i brak innych adresów w jednym liście) lub na zasadzie „jeden list do wszystkich, ale nikt nie wie, do kogo” (w polu *To:* znajduje się adres *nadawcy* listu, a wszystkie adresy odbiorców wpisane są w polach *BCC:*).

Nie dodawaj do swojej listy adresów e-mailowych niewiadomego pochodzenia, gdyż z tego powodu będziesz miał wyłącznie problemy. Unikaj również zakupu baz od wyspecjalizowanych firm. Pomimo zapewnień o legalności przedsięwzięcia oraz doborze zainteresowań właścicieli adresów zamieszczonych w bazie, masz sporą szansę dostać niezweryfikowaną bazę pełną przypadkowych adresów niewiadomego pochodzenia, a przede wszystkim zawierającą adresy osób, które nie zarejestrowały się dobrowolnie na Twojej liście mailingowej. W takim wypadku stracisz jedynie pieniądze i nabawisz się reputacji spamera. O ile na drodze sądowej istnieje szansa na

odzyskanie straconych pieniędzy, to z pozbyciem się miana spamera będziesz miał ogromny problem.

Przestrzegając zasad opisanych przez nas w niniejszym podrozdziale nie narazisz się na gniew internautów i nikt przy zdrowych zmysłach nie dopisze Cię do publicznych czarnych list i spokojnie będziesz mógł rozwijać swój e-biznes, czego życzymy z całego serca.

Tymczasem praktyka wskazuje, że nawet w przypadku produktu bardzo „niszowego” można liczyć na kilka rejestracji dziennie, co w ciągu kilku miesięcy pozwala na zbudowanie bazy zawierającej kilkaset adresów – najcenniejszych, bo należących do osób zainteresowanych ofertą firmy.

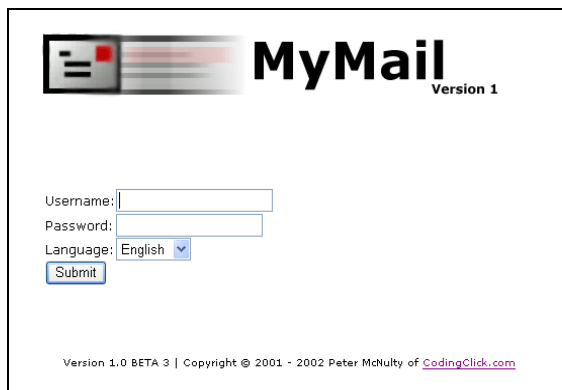
### **Przykład gotowego systemu mailingowego**

Prowadzenie własnej listy mailingowej nie jest trudne, jednak wymaga, byś trzymał się przyjętych standardów. W przypadku mało popularnej strony domowej cały proces weryfikacji, dodawania, usuwania adresów oraz wysyłania biuletynów możesz przeprowadzić ręcznie – *nawet* po prostu konstruuując formularz w taki sposób, by automat na stronie WWW wysyłał do Ciebie e-mail, na który będziesz odpowiadać osobiście. Niestety w sytuacji, gdy zamierzasz ruszyć z poważnym e-biznesem do zarządzania listą mailingową będziesz potrzebował własnego systemu, który większość operacji przeprowadzi w sposób automatyczny. Być może najlepszym wyjściem jest napisanie własnego systemu od podstaw, ale nie jest to proste, dlatego na początek warto sięgnąć po gotowe rozwiązania.

W niniejszym podrozdziale opisaliśmy prosty, a przy tym funkcjonalny system do obsługi wielu list mailingowych, który spełnia wszystkie wymagania, o jakich wspominaliśmy nieco wcześniej. Mamy tutaj na myśli darmowy skrypt o nazwie MyMail, który można pobrać ze strony <http://www.codingclick.com>. System MyMail do poprawnej pracy wymaga obsługi PHP oraz bazy MySQL. Nie

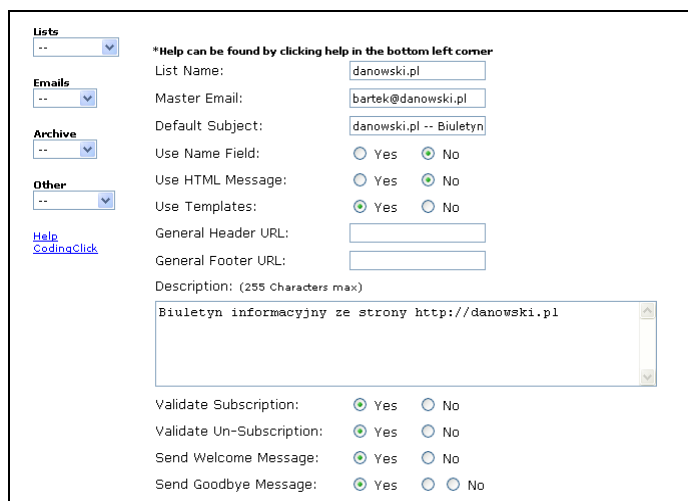
będziemy opisywać tutaj samej instalacji systemu, ale skupimy się na prezentacji rozwiązań zastosowanych w MyMail.

Dostęp do panelu administracyjnego jest chroniony za pomocą hasła i loginu – rysunek 9.1.



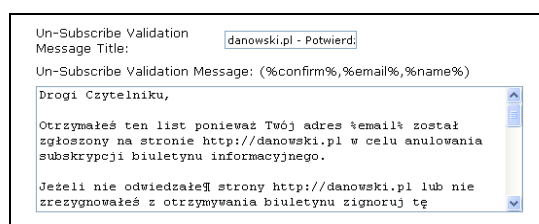
**Rysunek 9.1.** Dostęp zabezpieczony skutecznym systemem logowania

Dodając nową listę, masz możliwość określić sposób, w jaki będzie ona dodawać nowe adresy. System może bazować w oparciu o weryfikację dodanego adresu – rysunek 9.2.



**Rysunek 9.2.** Możliwość kontroli sposobu dopisywania się do listy

Dodawanie adresów przebiega automatycznie, a wiadomości wysyłane do osoby zapisującej się na listę są generowane na podstawie szablonów – rysunek 9.3. Treść domyślnych wiadomości można opracować w trybie tekstowym lub HTML. Za wstawienia odnośników weryfikujących lub usuwających odpowiadają specjalne kody, dzięki czemu jeden szablon nadaje się do obsługi wszystkich subskrybentów.



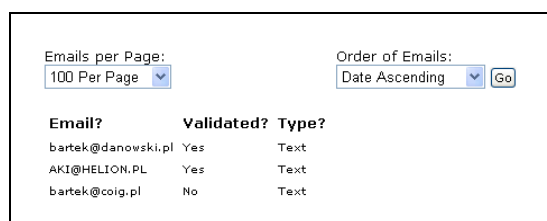
The screenshot shows a web form for creating an email template. The form has the following fields and content:

- Un-Subscribe Validation: danowski.pl - Potwierdź
- Message Title: (empty)
- Un-Subscribe Validation Message: (%confirm%,%email%,%name%)
- Text area containing:

```
Drogi Czytelniku,  
  
Otrzymałeś ten list ponieważ Twój adres %email% został zgłoszony na stronie http://danowski.pl w celu anulowania subskrypcji biuletynu informacyjnego.  
  
Jeżeli nie odwiedzałeś strony http://danowski.pl lub nie zrezygnowałeś z otrzymywania biuletynu zignoruj tę
```

**Rysunek 9.3.** Szablony pomagają w tworzeniu automatycznie wysyłanych wiadomości do nowych zapisujących się czytelników

Przykładowy system posiada wygodne rozwiązania pozwalające na przeglądanie, dodawanie, zarządzania i usuwanie adresu e-mail z bazy – rysunek 9.4.



The screenshot shows a web interface for managing an email list. It includes the following elements:

- Control panel: "Emails per Page:" with a dropdown set to "100 Per Page" and "Order of Emails:" with a dropdown set to "Date Ascending" and a "Go" button.
- Table with columns: "Email?", "Validated?", and "Type?".

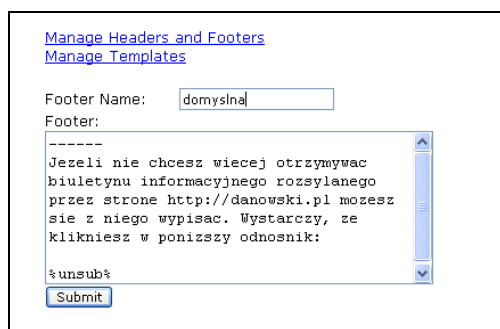
| Email?             | Validated? | Type? |
|--------------------|------------|-------|
| bartek@danowski.pl | Yes        | Text  |
| AKI@HELLION.PL     | Yes        | Text  |
| bartek@coig.pl     | No         | Text  |

**Rysunek 9.4.** Zarządzanie bazą adresów

Bez problemu możesz poprzez panel administracyjny dodać większą partię adresów e-mailowych pozyskanych w wyniku działań marketingowych, np. konkursu, którego byłeś organizatorem.

Poprzez mechanizm zarządzania adresami istnieje możliwość kontroli stanu adresu zweryfikowanych oraz nie zweryfikowanych.

Dla wysyłanych wiadomości możesz przygotować szereg standardowych nagłówek oraz stopek – rysunek 9.5.



Manage Headers and Footers  
Manage Templates

Footer Name:

Footer:

```
-----  
Jeżeli nie chcesz więcej otrzymywać  
biuletynu informacyjnego rozsyłanego  
przez stronę http://danowski.pl możesz  
się z niego wypisać. Wystarczy, że  
klikniesz w poniższy odnośnik:  
% unsub %
```

**Rysunek 9.5.** System umożliwia przygotowanie kilku rodzajów nagłówek oraz stopek

Uprzednio przygotowując stopki i nagłówki, znacznie uprościsz tworzenie kolejnych wiadomości. Wystarczy, że wpiszesz jedynie treść biuletynu, a stałe treści zostaną domyślnie doklejone podczas wysyłki. W ten sposób każdy biuletyn będzie miał stały wygląd, co zapewni profesjonalny wygląd.

MyMail posiada wygodny mechanizm pozwalający na rozsyłanie biuletynów – rysunek 9.6.

Wystarczy, że odpowiednim polu wkleisz treść biuletynu, a następnie uzupełnisz nazwę nadawcy wiadomości oraz zdecydujesz, z jakich nagłówek i stopek chcesz skorzystać. Przed rozpoczęciem wysyłki możesz jeszcze określić sposób rozsyłania wiadomości, aby nie zapchać serwera, z którego korzystasz.

Przykładowy system posiada dokładnie statystyki pracy, dzięki czemu będziesz mógł sprawdzić, ile wiadomości zostało wysłane, ilu posiadasz subskrybentów i jaki jest ich status.

Use the form below to send out your email. If HTML is allowed you'll see two boxes. To send out just a text message to everyone while HTML is allowed select 'No' for the Use HTML checkboxes.

From Email:  Subject:

From Name:

Text Header:  Text Footer:

Archive:  Yes  No Issue ID:

Word Wrap:

Plain Message: %unsub% %email% %name%

Send  then wait  seconds

**Rysunek 9.6.** Wygodny mechanizm do rozsyłania biuletynów

MyMail jest wygodnym narzędziem dla małych list mailingowych i doskonale się na tym polu sprawdza. Jednak aby obsługiwać naprawdę duże listy, warto sięgnąć po bardziej zaawansowane narzędzia, np. PHPlist – <http://www.phplist.com> – lub stworzyć własnoręcznie odpowiednie rozwiązanie uszyte na miarę.

# Dlaczego warto mieć pełną wersję?



Pełną wersję książki zamówisz na stronie wydawnictwa  
Złote Myśli

<http://www.zlotemysli.pl/prod/6318/spam-profilaktyka-i-obrona.html>