

Damian Daszkiewicz

Zwalcz spam

Profilaktyka antyspamowa

Darmowa publikacja, dostarczona przez

[Darmowe Ebooki](#)

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](#).

© Copyright for Polish edition by Damian Daszkiewicz & ZloteMysli.pl

Data: 24.04.2007

Tytuł: Zwalcz spam

Autor: Damian Daszkiewicz

Korekta: Anna Popis-Witkowska

Skład: Anna Popis-Witkowska

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](#).

Dystrybucja w Internecie, za zgodą Autora

Internetowe Wydawnictwo Złote Myśli

Netina Sp. z o. o.

ul. Daszyńskiego 5

44-100 Gliwice

WWW: www.ZloteMysli.pl

EMAIL: kontakt@zlotemysli.pl

Wszelkie prawa zastrzeżone.

All rights reserved.

SPIS TREŚCI

<u>WSTĘP</u>	4
<u>O AUTORZE</u>	5
<u>CO TO JEST SPAM?</u>	6
<u>UWAŻAJ, GDZIE PODAJESZ SWÓJ E-MAIL</u>	7
<u>FORMULARZ KONTAKTOWY</u>	10
<u>FORMULARZE</u>	14
<u>LINKI REFERENCYJNE</u>	16
<u>UWAŻAJ NA GRUPY DYSKUSYJNE!</u>	18
<u>ZAŁÓŻ DARMOWE KONTO POCZTOWE DO BIULETYNÓW</u>	20
<u>SERWISY OGŁOSZENIOWE</u>	21
<u>NIE ODPOWIADAJ NA E-MAILE OD SPAMERÓW</u>	22
<u>NIE CZYTAJ SPAMÓW</u>	23
Aktualizacja.....	25
<u>NIE WYSYŁAJ WIADOMOŚCI DO WIELU OSÓB</u>	27
<u>NIE WYSYŁAJ ŁAŃCUSZKÓW</u>	31
<u>UWAGA NA DOMENY!</u>	32
<u>CZY MASZ “ANTYWIRUSA”?</u>	34
<u>USUWAJ SPYWARE</u>	36
<u>SPAM NA FORACH INTERNETOWYCH, W KSIĘGACH GOŚCI ITP.</u>	38
<u>MATERIAŁY UZUPEŁNIAJĄCE</u>	42

Wstęp

Spam można najprościej zdefiniować jako niezamawianą przesyłkę reklamową. Pewnie często otrzymujesz różne reklamy inwestycji finansowych, Viagry, ziół powiększających penisa itp. Tego typu wiadomości to jest spam. Natomiast jeśli na jakiejś stronie zostawisz swój adres e-mail, aby otrzymywać informacje o nowych produktach (aktualizacji strony, promocjach, nowościach w danej firmie itp.), to dane e-maile nie są spamem, gdyż **świadomie** wyraziłeś zgodę na otrzymywanie tego typu wiadomości. W tym krótkim i darmowym ebooku mam zamiar udzielić Ci kilku porad, dzięki którym będziesz otrzymywał mniejszą ilość spamu. Porady te oparte są na moim doświadczeniu. W wielu różnych sytuacjach popełniałem błędy, które spowodowały, że dzisiaj otrzymuję dużą ilość spamu. **Najlepiej jest uczyć się nie na swoich błędach, tylko na błędach innych osób!** Ponieważ lepiej jest zapobiegać niż leczyć – ten ebook opisuje różne triki, dzięki którym spamerzy nie dowiedzą się o istnieniu Twojego adresu email.

O autorze

Uważam, że zanim zacznę się dzielić z Tobą swoją wiedzą, powinienem napisać kilka słów o sobie. Jako autor mam już za sobą swoje pierwsze sukcesy “literackie”. Dla wydawnictwa Helion napisałem dwie książki: “[Vademecum hakera. Edycja plików binarnych](#)” (książka opisuje, co ciekawego można robić z plikami binarnymi, głównie z plikami wykonywalnymi, zawiera też informacje o ukrywaniu plików na dyskietce bądź w plikach BMP) i “[PartitionMagic. Ćwiczenia](#)”.

Wydawnictwo Złote Myśli wydało już mojego pierwszego ebooka: “[Wirtualne płatności: E-gold i MoneyBookers](#)”.

Więcej informacji o mnie znajdziesz na moim [blogu](#).

Gdybyś odczuł silną potrzebę kontaktu, to kliknij w ten e-mail: zm@daszkiewicz.net

Co to jest spam?

SPAM to nazwa taniej konserwy (zobacz poniższy rysunek), która jest popularna w USA, często podawano ją żołnierzom podczas II Wojny Światowej, gdyż jest tania i pożywna. Spamem również określamy wiadomość reklamową, na której otrzymanie nie wyraziliśmy zgody. Pewnie zastanawiasz się, co wspólnego mają ze sobą: niechciana korespondencja i konserwa. Odpowiedź jest zaskakująca: te dwie rzeczy łączy pewien skecz Monty Pythona, w którym klient przychodzi do restauracji i po kolei zamawia różne dania, a grupa wikingów cały czas go zagłusza krzyząc: SPAM. Zapis skeczu znajduje się tutaj:

<http://spamming-warfare.de/english/index.php>



Uważaj, gdzie podajesz swój e-mail

Spamerzy bardzo często “przeglądają” strony WWW w poszukiwaniu adresów e-mailowych. Oczywiście “ręczne czytanie” strony jest bardzo niewygodne i pracochłonne. Dlatego spamerzy piszą specjalne programy, które korzystając z wyszukiwarek internetowych przeglądają strony WWW, szukając charakterystycznych ciągów znaków.

Jeśli taki program znajdzie na stronie internetowej znak @, a tuż za nim będzie kilkanaście liter (bez spacji i znaków specjalnych), a później kropka i 2-3 litery, a przed małpą będzie kilka liter – to z dużym prawdopodobieństwem ów charakterystyczny ciąg znaków będzie adresem e-mail. Ów ciąg znaków zostanie zapisany w bazie danych, a program dalej będzie przeglądał stronę w poszukiwaniu innych adresów. Pewnie teraz zastanawiasz się nad tym, czy warto podać na swojej stronie adres e-mail. Odpowiedź brzmi: warto!

Jednak trzeba zachować kilka zasad bezpieczeństwa. Po pierwsze, jeśli z kimś dyskutujesz na forum dyskusyjnym, to nie podawaj adresu w formie **email@serwer.pl**. Dużo lepszym rozwiązaniem jest “zakodowanie” adresu: np. **e-mail małpka serwer kropka pl** albo: **mój nick@serwer.pl**. Dzięki temu program spammera nie wykryje twojego adresu :-)

Wiem, że to jest niewygodne, ale warto się poświęcić. Sam czasami z lenistwa nie kodowałem adresu e-mail i po jakimś czasie otrzymywałem reklamy Viagry :-)

Niestety, na stronie WWW (szczególnie biznesowej) niezbyt dobrze – w dziale “Kontakt” – wyglądają adresy e-mail w stylu: **e-mail małpka serwer kropka pl**. Można zapisać adres e-mail tak, aby widoczny był normalny e-mail i po kliknięciu w niego włączał się domyślny program pocztowy z wpisanym adresem e-mail, a program spamera nie wykrywał go.

Jak to jest możliwe? Otóż spamerzy piszą bardzo proste programy, które jedynie wyszukują charakterystycznych ciągów znaków wyglądających jak adres e-mail, natomiast rzadko im się udaje wyłowić “zakodowany” adres e-mail. Jak zakodować taki adres e-mail? Wystarczy wygenerować odpowiedni kod JavaScript, który bez problemu zinterpretuje przeglądarka internetowa, a program spamera pominie go, uważając za bezwartościową informację. Prosty program, który generuje odpowiednią wstawkę, możesz pobrać ze strony: <http://www.jelcyn.com/win/anty-spam.htm>. Dla adresu email: damian@daszkiewicz.net została wygenerowana następująca wstawka kodu HTML:

```
<p><script language="JavaScript"><!--  
var malpa='@';  
var kropka='.';  
var m1='mai';  
var m2='lto';  
document.write('<a href="'+m1+m2+'damian'+malpa  
+'daszkiewicz'+kropka+'.net'">&#100;&#97;&#109;&#1  
05;&#97;&#110;&#64;&#100;&#97;&#115;&#122;&#107;&#1  
05;&#101;&#119;&#105;  
&#99;&#122;&#46;&#110;&#101;&#116;</a>');  
// --></script></p>
```

Wiem, być może nie zawsze chce Ci się uruchomić program i wygenerować wstawkę. Ja też czasami z lenistwa wpisałem niezakodowany adres e-mail, a później żałowałem, że przychodzą do mnie niezamówione wiadomości reklamowe.

Dlatego musisz przewyciężyć lenistwo! Dzisiaj zaoszczędzisz 10 minut, a od jutra będziesz codziennie tracił 2 minuty na kasowanie spamu!

Jeśli prowadzisz własny serwis ogłoszeniowy (lub jakikolwiek inny, w którym podane są adresy e-mail do wielu osób), to **OBOWIĄZKOWO** zadbaj o ich kodowanie!

Formularz kontaktowy

Jeśli paranoicznie boisz się, że spamerzy piszą coraz lepsze wersje programów przeszukujących internet, które mogą przechwycić Twój adres e-mail, to możesz na swojej stronie WWW zamieścić jedynie formularz kontaktowy.

Być może programy skanujące internet i analizujące JavaScript są na razie mrzonką (lepiej się skupić na wyszukiwaniu niezakodowanych adresów e-mail, niż kilka razy dłużej analizować strony WWW, aby zebrać kilka procent więcej adresów e-mail), ale to, co dzisiaj jest nieosiągalne – jutro może być “standardem”.

Dlatego można rozważyć możliwość zamieszczenia na swojej stronie WWW prostego formularza kontaktowego. Formularz kontaktowy ma jeszcze jedną zaletę: czasami będąc w kawiarence internetowej nie chcę konfigurować programu pocztowego, a mam potrzebę napisania e-maila do webmastera danej strony internetowej.

Formularz kontaktowy ma tę zaletę, że mogę napisać wiadomość bez konfiguracji programu pocztowego. Z kolei webmaster wie, że spamer nie przechwyci jego adresu e-mail, ponieważ adres pozna tylko ten, kto napisze wiadomość z formularza i otrzyma odpowiedź.

Poniżej przedstawiam prosty formularz kontaktowy i skrypt wysyłający dane z formularza na adres e-mail (Twój serwer musi obsługiwać PHP).

kontakt.htm

```
<HTML>
<HEAD>
<meta http-equiv="Content-Type" content="text/html;
charset=windows-1250">
<TITLE>TYTUL TWOJEJ STRONY</TITLE>
</HEAD>
<BODY>
<h1>Kontakt</h1>
<form method="POST" action="send.php">

<p>Imie lub pseudonim: <input type="text"
name="imie"></p>
<p>Email kontaktowy: <input type="text"
name="email"></p>
<p>tytul wiadomosci: <input type="text" name="tytul"></p>
<p>tresc: <br><textarea rows=10 cols=60
name="tresc"></textarea>

</p>
<p><input type="submit" value="Wyslij"></p>
</form>
</BODY>
</HTML>
```

send.php

```
<HTML>
<HEAD>
<meta http-equiv="Content-Type" content="text/html;
charset=windows-1250">
<TITLE>TYTUŁ TWOJEJ STRONY</TITLE>
</HEAD>
<BODY>
<h1>Kontakt</h1>

<?
$blad=0;
if ($imie==""){echo("<B>BŁĄD:</b> podaj swoje
imie</B><br>");$blad=1;}
if ($email==""){echo("<B>BŁĄD:</b> podaj swój adres
email</B><br>");$blad=1;}
if ($tytul==""){echo("<B>BŁĄD:</b> podaj tytuł
wiadomości</B><br>"); $blad=1;}
if ($tresc==""){echo("<B>BŁĄD:</b> wpisz treść
wiadomości</B><br>");$blad=1;}

if ($blad==1){echo("Wciśnij przycisk wstecz w swojej
przeglądarce internetowej, aby skorygować formularz"); exit;}

echo("Dziękujemy za email. W ciągu 48 godzin otrzymasz
odpowiedź");

//tutaj podaj swój adres email !!
$webmaster="zm@daszkiewicz.net";
```

```
if(mail($webmaster, $tytul, $tresc, "From: $imie <$email>") )
{
    echo "Dziękujemy za email...";
}
else {
    echo "Przepraszamy, nie udało się wysłać maila";
}
?>

</form>
</BODY>
</HTML>
```

Uwaga: ten skrypt jest bardzo prosty (sam "silnik") i wymaga drobnych przeróbek (np. dopasowania do Twojej strony WWW).

Formularze

Początkujący webmasterzy, którzy nie znają się na pisaniu skryptów (np. w PHP, Perlu, ASP itp.) często tworzą na swoich stronach formularze kontaktowe (bądź np. formularz, w którym można wpisać swoje uwagi o stronie WWW), które są wysyłane przez domyślny program pocztowy.

Po pierwsze: takie formularze nie są profesjonalne (wzbudzają niechęć w nadawcy, gdyż zostanie ujawniony jego adres e-mail; oprócz tego – aby formularz był wysłany, użytkownik musi mieć skonfigurowany jakiś program pocztowy), a po drugie: konstrukcja takiego formularza wymaga, aby w kodzie HTML podać swój adres e-mail (!).

Poniżej przedstawiam kod prostego formularza wysyłanego na email:

```
<form action="mailto:adres@email.pl" method="POST"
enctype="text/plain">
Podaj swoje imie: <input type="text" size="16" name="Imie">
</form>
```

Jak widać – kod nie jest zbytnio skomplikowany, a co gorsze – adres e-mail nie jest zakodowany (i jest konieczny, aby w ogóle wiadomość doszła do Ciebie).

Wydawało mi się, że pewnym rozwiązaniem byłoby skorzystanie z popularnych skryptów form2mail, ale one mają tę samą wadę, co

formularze wysyłane na adres e-mail: w kodzie HTML jest podany niezakodowany adres e-mail (jako niewidzialny element formularza), więc odradzam korzystanie z tego typu usług (inne wady usługi form2mail to fakt, że skrypty są darmowe, więc nigdy nie masz gwarancji, że będą codziennie działały i – co najważniejsze – nie masz pewności, czy ktoś nie czyta wysyłanych przez formularz e-maili).

Jakie są skuteczne rozwiązania tego problemu? Ja znam dwa: pierwsze to napisanie formularza kontaktowego np. w PHP (zobacz powyższy rozdział) bądź zakodowanie kodu HTML.

Linki referencyjne

Często w różnych programach partnerskich loginem jest adres e-mail. Aby zidentyfikować osobę, która zachęciła do skorzystania z usług danego serwisu, tworzy się linki referencyjne, w których podany jest identyfikator polecającego, dzięki czemu można bardzo łatwo zidentyfikować osobę polecającą, która otrzyma jakąś premię (np. X% wartości zamówienia). Najlepiej sytuacja wygląda, gdy identyfikatorem partnera jest jakiś ciąg cyfr lub ciąg znaków. Problem pojawia się wtedy, gdy identyfikatorem jest adres e-mail (!). Wtedy taka osoba polecająca zmuszona jest zamieścić na stronie link w postaci:

<http://www.sklep.internetowy.pl/?pol=mój@adres.email.pl>.

Niektóre programy przeszukujące internet mogą z tego linku wyciągnąć adres email. I tutaj pojawia się dylemat: czy lepiej jest otrzymać co miesiąc kilka złotych prowizji i trochę spamu, czy nie mieć ani prowizji, ani spamu. Najlepiej byłoby mieć możliwość potencjalnego zarobku i nie otrzymywać spamu. Osobiście znam trzy ciekawe rozwiązania tego problemu:

- Można napisać skrypt (podobny do tego, jaki generuje program opisany w poprzednim rozdziale), który będzie wyświetlał na stronie link (ale link będzie zakodowany w źródle strony i nikt go nie odczyta, a przeglądarka internetowa poprawnie go wyświetli)
- Można dla tego jednego programu partnerskiego założyć osobne konto e-mail, z którego nie będziesz odbierał poczty, ale tutaj są dwa problemy: pierwszym jest fakt, iż musisz co pewien czas

kasować stare wiadomości, aby skrzynka nie została skasowana, a drugim problemem jest fakt, że nie będziesz na bieżąco otrzymywał informacji ze sklepu internetowego (np. info o nowych produktach, promocjach albo informacji, że ktoś dokonał zakupu z Twojego polecenia)

- Można skorzystać z usług serwisów “skraccających” linki. Dzięki temu w źródle strony nie będzie zapisany Twój adres e-mail, tylko normalny link. Oto adresy przykładowych serwisów skraccających linki:

- www.tinyurl.com
- www.skocz.pl
- www.gourl.org
- www.je.pl
- www.glinki.com
- www.tinyurl.rzeszow.net

Uważaj na grupy dyskusyjne!

Grupy dyskusyjne to świetne miejsce, gdzie można podyskutować z kimś na interesujące nas tematy. Chyba każdy lubi wymieniać swoje doświadczenia z innymi osobami. Spamerzy bardzo lubią grupy dyskusyjne, ponieważ łatwo można napisać program, który byłby czytnikiem grup dyskusyjnych, ale wyławiałby tylko i wyłącznie adresy e-mail. Dlatego na grupach dyskusyjnych panuje zwyczaj podawania adresów email z “pułapką”. Owa pułapka to jakiś dopisany ciąg znaków: np. e-mail@usuńto.serwer.pl lub e-mail@serwer.deleteMe.pl. Inteligentny człowiek widząc w adresie e-mail ciąg znaków „usuńto” na pewno usunie ów ciąg znaków. Spamer natomiast da sobie z tym spokój, gdyż nie będzie ręcznie czytał iluś milionów adresów, aby usunąć “pułapki”. Dlatego zalecam podawanie adresów e-mail z pułapkami, ale takimi, aby każdy wiedział, że to jest pułapka. Nie należy jednak dodawać takich popularnych członów jak nospam, no_spam, delete itp. gdyż programy spamerów są wyczulone na takie podstawowe pułapki. Dużo lepiej jest wymyślić oryginalną pułapkę. „Usuń-To” można uznać za bezpieczną pułapkę, gdyż spamerzy w głównej mierze nie znają języka polskiego. Innym rodzajem pułapki jest podanie fałszywego adresu (np. dxmixn@dxszkiewicz.net) i informacja: w moim adresie email zamień wszystkie litery **x** na litery **a**. Człowiek sobie z tym zadaniem poradzi bez problemu (pod warunkiem, że napiszesz o tym bardzo wyraźnie w stopce każdego postu), natomiast program spamera pobierze fałszywy adres e-mail :-)

W grupach dyskusyjnych warto jest używać innego konta pocztowego (możesz założyć na darmowym serwerze jakieś konto

pocztowe). Chodzi o to, aby na główne konto nie otrzymywać spamu (czasami – jeśli wymyślisz jakieś zabezpieczenie – może się okazać, że jakiś uciążliwy spamer usunie pułapkę z Twojego e-maila). Zaletą takiego darmowego konta do kontaktu z ludźmi z grup dyskusyjnych jest fakt, że darmowe konto możesz porzucić w dowolnej chwili.

Skoro już jestem przy grupach dyskusyjnych, to czuję się zmuszony omówić pewne zjawisko: jeśli już ktoś wyśle na grupę dyskusyjną jakiś spam, to nie pisz na grupie dyskusyjnej tekstów w stylu “spadaj spamerze na drzewo”. Po pierwsze – spamer mógł wysłać reklamę tylko po to, aby coś zareklamować i nie jest stałym bywalcem owej grupy dyskusyjnej (więc nie przeczyta twoich wypocin). Po drugie – inni marnują czas na pobranie Twojego pouczenia, które nie ma żadnej wartości merytorycznej. Dużo lepszą rzeczą jest kulturalne napisanie na e-mail nadawcy, że to, co zrobił, to jest spam, że tego nie tolerujesz i napisz, dlaczego spam jest zły. Edukując początkujących spamerów częściowo przyczyniasz się do mniejszej ilości spamu w grupach dyskusyjnych (zawsze jest nadzieja, że spamer weźmie sobie do serca Twoje porady).

Załącz darmowe konto pocztowe do biuletynów

Pewnie nieraz widziałeś w internecie informacje o jakimś e-mailowym newsletterze (spolszczona nazwa tego słowa to biuletyn), kursie, poradniku czy informatorze o aktualizacji strony WWW.

Jeśli w tych momentach miałeś wątpliwości, czy zostawić swój adres email, to świadczy to o tym, że panicznie boisz się udostępnić swój adres e-mail.

Dobry sposób na taki strach to założenie darmowego konta pocztowego dla różnego rodzaju biuletynów i kursów. Gdy stwierdzisz, że na konto pocztowe przychodzi więcej spamu niż biuletynów, to zawsze je możesz porzucić i założyć nowe darmowe konto dla biuletynów :-)

Serwisy ogłoszeniowe

Jeśli chcesz zostawić ogłoszenie w jakimś serwisie, to może się okazać, że musisz zostawić swój adres e-mail i on nie jest kodowany!

Dlatego gdy chcesz zostawić jakieś ogłoszenie w serwisie ogłoszeniowym, to załóż darmowe konto e-mail tylko do tego celu, aby kontaktować się z osobami, które są zainteresowane ogłoszeniem. Gdy tylko upłynie ważność ogłoszenia, porzuć owo konto.

Zostawiłem kiedyś ogłoszenie w kilku serwisach i po 2 miesiącach na ów adres zaczęły do mnie przychodzić różne dziwne reklamy. Świadczy to o tym, że spamerzy wykorzystują serwisy ogłoszeniowe do wyławiania adresów e-mail.

Uwaga: Niektóre księgi gości również nie szyfrują adresów e-mail.

Nie odpowiadaj na e-maile od spamerów

Bardzo często zdarza się, że osoba, która otrzymuje spam, odpisuje na e-mail, prosząc o niewysyłanie takich e-maili. Jeśli spam pochodzi od Polaka, możesz śmiało poprosić o usunięcie Twojego adresu email z bazy danych (a jak to nie pomoże, to zawsze możesz wnieść zawiadomienie do prokuratury). Z zagranicznym spamerem jest trochę inaczej.

Często spam jest wysyłany np. z Chin, gdzie sprawa spamu nie jest prawnie uregulowana i nawet nie masz dobrych argumentów, aby postraszyć taką osobę ;-)

Odpisując na spam możesz się przekonać, że spamer zaznaczy w swojej bazie, że od tego adresata przyszedł e-mail z prośbą o usunięcie go z bazy danych (potwierdzający tym samym adres e-mail (!)) i zakwalifikuje go do tej “lepszej” bazy danych, dzięki czemu będzie jeszcze częściej spamowany.

Uwaga: ostatnim krzykiem mody jest fałszowanie adresu nadawcy. Spamerzy wysyłają wiadomości, w których adres nadawcy jest zmyślony. Spamer nie otrzyma od nas e-maila wysłanego na taki adres. Wirusy posuwają się jeszcze dalej: fałszują adres podając jako adres nadawcy losowo wybrany adres z książki adresowej ofiary, dzięki czemu osoba otrzymująca wirusa nie dowie się, kto tak naprawdę ma zainfekowany komputer.

Nie czytaj spamów

Czy wiesz, że spamer może wiedzieć, kto czyta jego e-maile? Nie trudno się domyślić, że osoby, które czytają maile, trafiają do lepszej bazy (czyli będą częściej otrzymywały e-maile, gdyż spamerzy wymieniają się tymi “lepszymi” adresami e-mail).

Pojawia się pytanie: skąd spamer wie, że czytasz jego e-mail, skoro nie napisałeś do niego, że nie życzysz sobie otrzymywania takich wiadomości? Odpowiedź jest prosta: w każdym tego typu e-mailu jest taki malutki niewidzialny obrazek, który zacznie się ładować, gdy tylko otworzysz wiadomość.

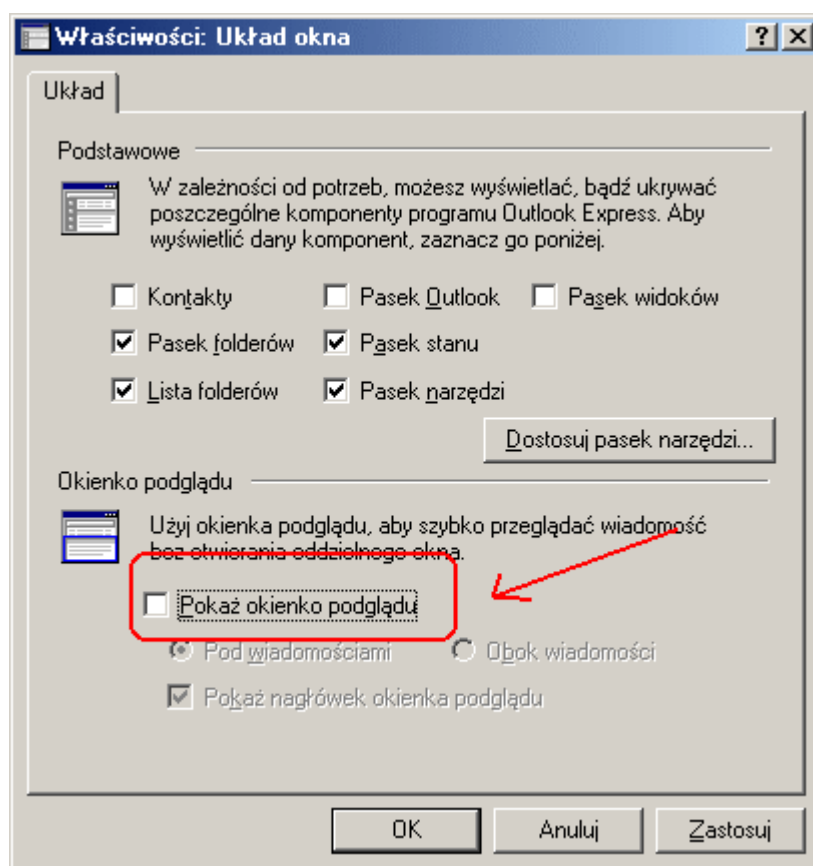
Każda ofiara spamu ma nieco inny e-mail, którego treść różni się nazwą ładowanego obrazka (czasem może to być ten sam plik, ale wywołany z innym parametrem). Po jakimś czasie spamer może w logach serwera sprawdzić, jakie obrazki zostały pobrane i na tej podstawie “odfajkować” w bazie danych osoby, które czytają jego e-maile. Dzięki temu spamer wie, że te adresy e-mail istnieją i może skupić się na wysyłaniu na nie reklam!

Jeśli używasz programu pocztowego Microsoft Outlook Express, to dobrym rozwiązaniem będzie wyłączenie podglądu wiadomości. Być może trochę niewygodnie będzie Ci przeczytać e-mail, ale za to będziesz mógł skasować wiadomość bez jej czytania (nawet jeśli od razu klikniesz na wiadomość i naciśniesz przycisk DEL, to program pocztowy w oknie podglądu zdąży załadować wiadomość i spamer będzie wiedział, że e-mail do Ciebie dotarł).

Ja nie mam włączonego okna podglądu i pierwszą czynnością, jaką wykonuję po ściągnięciu poczty, jest usuwanie wiadomości, które ewidentnie wyglądają na spam. Dopiero później otwieram pozostałe wiadomości i je czytam. Dzięki temu nieznacznie ograniczyłem ilość otrzymywanego spamu.

Aby wyłączyć okno podglądu wiadomości należy wykonać następujące czynności:

- Wybierz z menu **Widok** opcję **Układ**
- Zaznacz opcję **Pokaż okienko podglądu** (zobacz rysunek)



- Kliknij w przycisk **OK**.

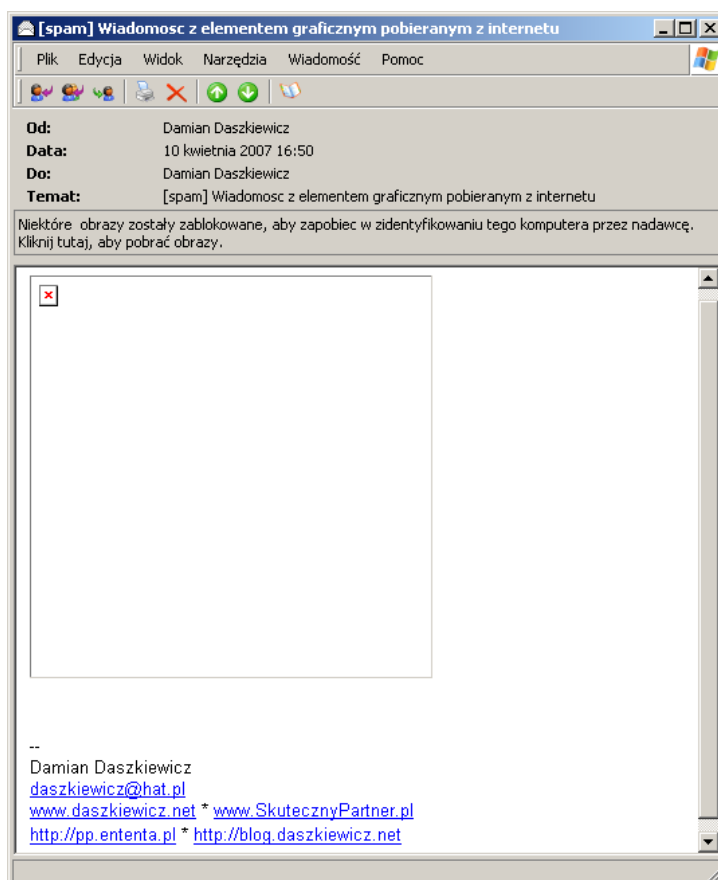
To proste rozwiązanie ma inną zaletę: około roku 2001 w sieci grasował groźny wirus, który wykorzystywał pewną lukę OE: nie trzeba było otwierać załącznika, wirus sam się aktywował, wystarczyło mieć włączony podgląd wiadomości. Jedynym lekarstwem na tego wirusa było wyłączenie podglądu wiadomości i kasowanie e-maili z załącznikami.

Inne rozwiązanie problemu ładujących się obrazków (które tak naprawdę są informacją “ten gość przeczytał wiadomość”) jest zmiana programu pocztowego. Gorąco polecam Operę, która jest przeglądarką internetową ze świetnym, wbudowanym klientem pocztowym.

Ten program ma dwie zalety: pierwsza to fakt, że poczta jest ściągana ze wszystkich kont pocztowych jednocześnie, a drugą zaletą jest zablokowane ładowanie się obrazków w wiadomościach. Dzięki temu nie musimy w Operze wyłączać podglądu wiadomości, a spamer i tak się nie dowie, że właśnie przeczytaliśmy jego wiadomość.

Aktualizacja

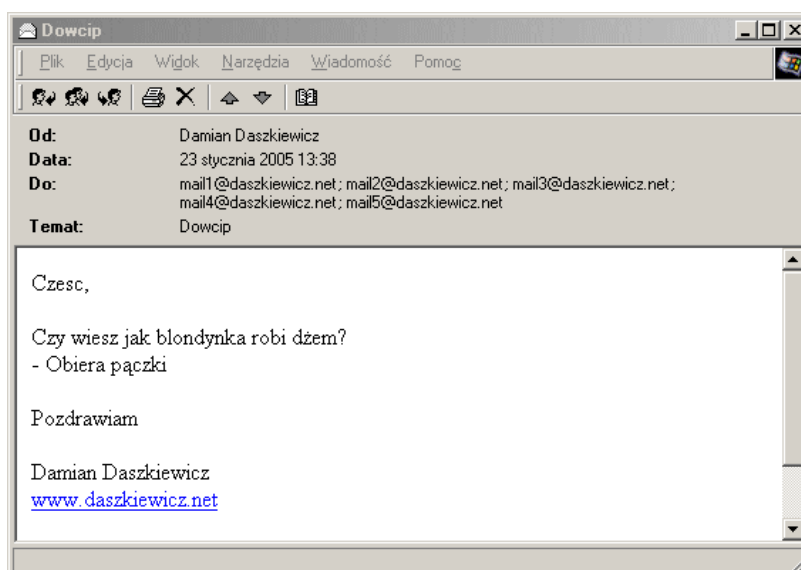
Obecnie nowsze wersje programu pocztowego Outlook Express mają zabezpieczenie – nie ładują z sieci obrazków, do których odnośniki są umieszczone w wiadomości e-mail, do czasu, aż użytkownik nie kliknie w informację o potencjalnym zagrożeniu (zobacz poniższy rysunek)



Nie wysyłaj wiadomości do wielu osób

Bardzo często otrzymuję różne wiadomości (np. świetny dowcip), które adresowane są do wielu osób. W polu **Do:** jest wpisanych kilka, czasem nawet kilkanaście adresów e-mail różnych osób, które zna nadawca.

Tego typu postępowanie jest nieodpowiednie, gdyż ten nadawca nie ma gwarancji, że ktoś z odbiorców nie zapisze tych adresów e-mail, aby wysłać na nie jakiś spam (odczytanie adresów odbiorców wiadomości jest bardzo łatwe, o czym świadczy poniższy rysunek).



Nawet jeśli masz zaufanie do tych osób, to nie masz gwarancji, że któraś z nich nie ma wirusa, którego celem jest sczytywanie adresów e-mail z otrzymywanych wiadomości i wysyłanie ich do autora.

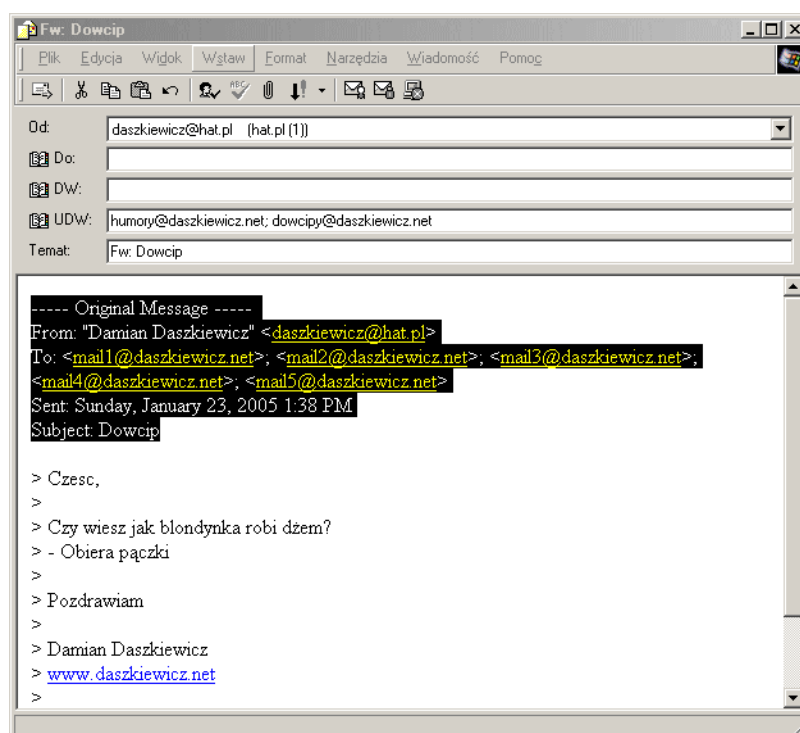
Jeśli chcesz wysłać e-mail do kilku osób (bo dowcip jest naprawdę śmieszny), to adresy e-mail możesz wpisać w polu **UWD (BCC)**, a nikt nie będzie wiedział, kto otrzymał wiadomość (nie da się tego odczytać nawet zaglądając do źródła wiadomości, więc nawet wirus nie odczyta tych adresów). Jednak nie zawsze pole **UWD** jest widoczne. Jeśli w swoim programie pocztowym widzisz jedynie pola **Do**, **DW** i **Temat**, to musisz je uaktywnić. Aby to zrobić, należy wykonać następujące kroki:

- W oknie nowej wiadomości z menu z menu **Widok** wybierz opcję **Wszystkie nagłówki**
- Od teraz za każdym razem, gdy redagujesz nową wiadomość, powinno być widoczne pole **UWD**

Dzięki tej prostej poradzie możesz nieznacznie utrudnić życie spamerom, a także znajomi przestaną Ciebie uważać za spamera.

Często spamerzy sami wysyłają grupowe e-maile do wielu osób (np. z dowcipem), gdyż z dużym prawdopodobieństwem ktoś, kto otrzyma wiadomość, zrobi to samo i wiadomość może “wrócić” do nadawcy “wzbogacona” o nowe adresy w polu **Do**.

Gdy otrzymasz wiadomość, w której w polu **Do** jest dużo adresów i będziesz chciał przesłać ją dalej, koniecznie usuń pola wygenerowane przez program pocztowy (zobacz poniższy rysunek), ponieważ nie każdy, komu przesyłasz wiadomość, musi znać adresy osób, które ją wcześniej otrzymały.



Usuwanie te informacje uzyskasz następujące korzyści:

- Chronisz innych przed spamem, gdyż nikt nie będzie znał ich adresów email, bo je usunąłeś.
- Wiadomość będzie zajmowała mniej miejsca, więc odbiorcy szybciej ją ściągną z serwera.
- Nikt nie nazwie Ciebie spammerem (pod warunkiem, że usuniesz ów nagłówek, a jeśli wiadomość wysyłasz do kilku osób, to adresy wpiszesz w polu **UWD**)
- Wiadomość będzie się czytało dużo wygodniej, gdyż nie trzeba będzie przedzierać się przez kilka stron nagłówek.

Wskazówka: często wiadomości, które są kilka razy przesyłane do wielu osób (np. świetny dowcip, który dostałeś od swojego kolegi, który on dostał od kogoś innego i który wyślesz do kogoś innego), mają tę niedogodność, iż oryginalny tekst zostaje poprzedzony

znakiem >. Im więcej osób przesyłało ten tekst do kolejnych osób, tym więcej jest tych znaków w każdej linijce, co znacznie utrudnia czytanie dowcipu.

Jeśli chcesz być uważany za poważną osobę, to warto, żebyś usunął owe znaki. Ręczne usuwanie może być niewygodne, ale można skorzystać z darmowego programu, który to zrobi za Ciebie: <http://www.jelcyn.com/win/cytaty.htm>

Nie wysyłaj łańcuszków

Czym są łańcuszki? Odpowiedź jest prosta: są to wiadomości (zazwyczaj zabawne, czasem jakieś mądrości życiowe), których celem jest przesyłanie ich dalej. Zazwyczaj na końcu takiej wiadomości znajdują się słowa zachęcające do wysłania wiadomości dalej (np. “gdy wyślesz wiadomość do 10 osób, to niedługo będziesz szczęśliwy, a gdy skasujesz tę wiadomość, to wpadniesz pod autobus”). Autorami takich wiadomości są żartownisie zerujący na ludzkiej naiwności, których bawi fakt, że ludzie wysyłają sobie jakieś głupoty. Oczywiście zabawę w wysyłanie łańcuszków podłapali spamerzy: wysyłając taki e-mail do wszystkich swoich znajomych można liczyć na to, że ktoś ze znajomych moich znajomych wyśle tę wiadomość do mnie, ale wpisze wszystkie adresy do pola **Do** i będę miał kilka nowych adresów do spamowania. Dlatego warto jest od razu kasować takie wiadomości (ja ich nigdy nie puszczam dalej i jakoś nie wpadłem pod autobus). Często w takich łańcuszkach pojawiają się dramatyczne prośby, np. informacja, że pilnie potrzebna jest krew dla dziecka (tu numer telefonu), prześlij mail do wszystkich znajomych. Z dobroci serca ludzie wysyłają wiadomość dalej, ale jakoś mało kto jest do tego stopnia dobry, że poświęci 2 zł i zadzwoni pod podany numer telefonu, aby zweryfikować ową wiadomość (a ona krąży dalej i tak co pół roku ją dostaję). Jeśli chcesz komuś pomóc, to dużo lepszym rozwiązaniem jest wpłacenie nawet niewielkiej sumy na konto jakiejś akcji charytatywnej.

Uwaga na domeny!

Rok temu kupiłem domenę www.daszkiewicz.net. Z początku bardzo się cieszyłem, że moja strona będzie miała krótki i profesjonalny adres (a nie jakieś tam republika.pl czy prv.pl). Jednak po pewnym czasie otrzymałem pierwszy spam. To dziwne, bo adresu e-mail przypisanego do domeny nikomu nie udostępniałem.

Po dokładnej analizie wiadomości okazało się, że wiadomość trafiła na adres: sales@daszkiewicz.net. Pewnie zadajesz sobie pytanie: jak taka wiadomość mogła do mnie trafić. Odpowiedź jest prosta: spamerzy sprawdzają, jakie są zarejestrowane domeny i próbują wysyłać e-maile do webmasterów tych stron. Znając domenę i wpisując cokolwiek przed @nazwa domeny, masz pewność, że e-mail i tak trafi do jej posiadacza. Jest to bardzo dobre rozwiązanie, gdyż mogę komuś podać adres program@daszkiewicz.net, zm@daszkiewicz.net lub biznes@daszkiewicz.net i po adresie, na który przyszła wiadomość, będę wiedział, o czym może być ta wiadomość.

Mało tego, jeśli w jakimś serwisie ogłoszeniowym zostawię ogłoszenie i podam adres ogloszenia@daszkiewicz.net, a po pewnym czasie na ten adres zacznie przychodzić spam (a ogłoszenie już nie będzie aktualne), to mogę zablokować ten adres. Niestety, spamerzy o tym też wiedzą i szukają w internecie informacji o nowych zarejestrowanych domenach, a później generują adresy e-mail, dodając jakiś człon – i wysyłają wiadomości. Oto adresy, jakie warto zablokować w panelu administracyjnym domeny:

- sales@domena (ang. sprzedaż)
- info@domena
- contact@domena
- webmaster@domena
- office@domena (ang. biuro)

Pewnie tego typu nazw jest więcej, ale ja spam otrzymuję tylko na te adresy. Dlatego warto nie używać tych adresów i od razu je zablokować.

Czy masz “antywirusa”?

Pewnie się teraz zastanawiasz, co mają wspólnego wirusy ze spamem. Odpowiedź jest prosta: po pierwsze – wirusy można porównać do spamu (z dużym prawdopodobieństwem mogę stwierdzić, że nie wyraziłeś nigdzie zgody na to, aby ktoś przesyłał Ci wirusy), a po drugie – często sami spamerzy piszą wirusy.

Jaki to ma sens? Odpowiedź jest prosta: wirus często rozsyła się sam do wszystkich osób, które znajdzie w książce adresowej (te “lepsze” wirusy potrafią przeszukać wszystkie pliki tekstowe w poszukiwaniu adresów e-mail).

Oprócz “rozmnażania się” niektóre wirusy wysyłają do samego twórcy wszystkie znalezione adresy e-mailowe. Jak widzisz, napisanie wirusa to świetny sposób na zdobycie wielu adresów, na które będzie można później wysłać wiele różnych reklam.

Dlatego bardzo ważną rzeczą jest posiadanie dobrego programu antywirusowego, który stale monitorując komputer nie pozwoli, aby wirus się uaktywnił. Dzięki temu Ty nie będziesz miał wirusa, spamer będzie miał chudsza bazę i co najważniejsze: nie zarazisz komputerów innych osób wirusem.

Oczywiście samo posiadanie dobrego programu antywirusowego nie wystarczy. Musisz mieć aktualne definicje wirusów. Dobry, ale “stary” program antywirusowy jest bezużyteczny, gdyż obecnie w sieci krążą tylko najnowsze wirusy, te starsze praktycznie zostały

wyeliminowane (najwięcej komputerów zarażają te najnowsze wirusy, bo programy antywirusowe albo ich jeszcze nie wykrywają, albo wiele osób nie zdążyło pobrać nowych definicji wirusów, a stare wirusy są wykrywane przez prawie każde oprogramowanie antywirusowe, więc nie mogą zbyt wiele “zwojować”).

Dlatego minimum raz na tydzień **musisz** pobierać aktualne definicje wirusów.

Usuwanie spyware

Spyware to programy szpiegujące działania użytkownika komputera. Często “normalne” programy (głównie te wyświetlające banery reklamowe) zawierają w swoim wnętrzu moduły szpiegujące. Takie programy są groźne, gdyż mogą szukać na dysku twardym plików, w których mogą być zapisane numery kart kredytowych. Oprócz tego takie programy mogą skanować dysk w poszukiwaniu adresów e-mail. Warto od czasu do czasu sprawdzić, czy przypadkiem nie posiadamy programu szpiegującego (lepiej poświęcić godzinę na ściągnięcie odpowiedniego programu usuwającego szpiega, zainstalować go i przeskanować system, niż otrzymywać dodatkowy spam). Do usuwania programów szpiegujących polecam cztery programy:

- Ad-aware: <http://www.lavasoftusa.com/>
- Spybot Search & Destroy:
<http://spybot.eon.net.au/en/index.html>
- CWSHredder:
<http://www.adwarereport.com/mt/archives/cwshredder.php>
- SpywareTerminator: <http://www.spywareterminator.com/>

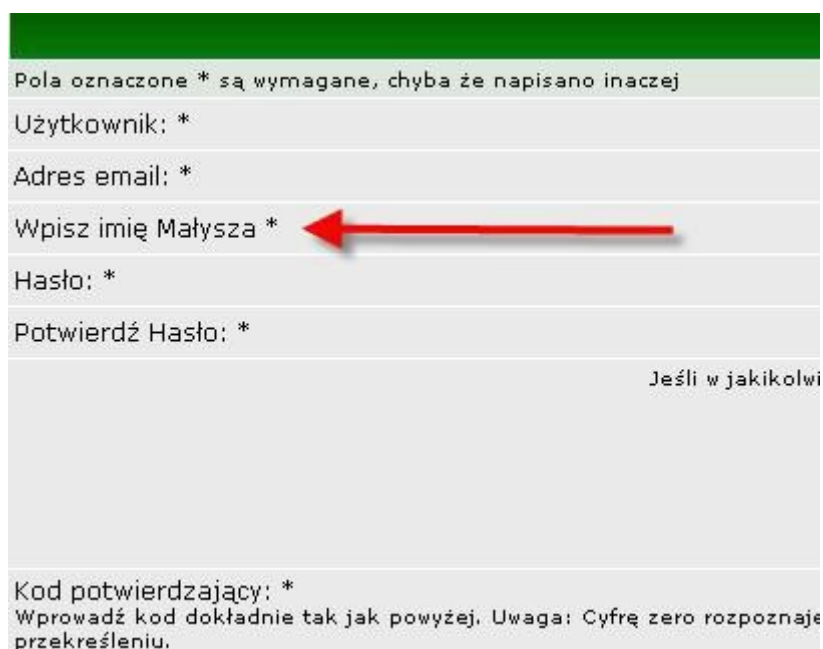
Najlepiej jest skanować system przynajmniej raz w tygodniu (przed skanowaniem upewnij się, czy są nowe definicje “wirusów”). Używaj minimum tych czterech programów, gdyż raz mi się zdarzyło, że złapałem jakiegoś szkodnika i dopiero czwarty program go usunął (trzy pozostałe nawet go nie wykryły).

Uwaga: Naprawdę zachęcam do częstego skanowania systemu programami antywirusowymi i programami do usuwania spyware. Ostatnio sporo wirusów działa w ten sposób, że siedzi w tle i komunikuje się z serwerem spamera. Spamer podaje listę e-maili i treść e-maila, a program w ukryciu z naszego komputera wysyła SPAM! Taki spamer ma pod sobą całą armię zarażonych komputerów, które są w stanie wysyłać miliony wiadomości dziennie. Mało tego, czasami natrafiam w internecie na artykuły, że Polska jest w czołówce pod względem wysyłanego spamu (niestety, te promocje neostrady za złotówkę spowodowały, że internet ma zbyt wiele osób, które nie są obyte z komputerami, a TP SA nie edukuje swoich klientów ani nie próbuje jakoś przeciwdziałać temu zjawisku). Przykładowy artykuł poruszający ten temat jest dostępny na stronie: <http://cso.cxo.pl/news/94106.html>

Spam na forach internetowych, w księgach gości itp.

Ostatnio istną plagą jest spam na forach internetowych, w księgach gości czy w komentarzach na blogach. Taki spamer wchodzi na forum i w dowolnym temacie pisze, że “pewna część Twojego ciała jest malutka, ale można ją powiększyć” i daje link do strony oferującej tego typu usługi. Spamer nawet się nie przejmuje tym, że na forum rozmawiamy po polsku, on i tak wie, że wiele osób zna język angielski, poza tym te spammerskie posty wrzuci na setki forów internetowych, więc zawsze ktoś kliknie w link. Taki spamer bez problemu da sobie radę z założeniem konta na forum, gdyż większość osób używa standardowego forum opartego na PHPBB2 i nawet jeśli przetłumaczymy skrypt na rodzimy język, to spamer dobrze wie, że: w pierwszym polu od góry wpisuje się login, w drugim adres e-mail, a w trzecim i czwartym hasło. Mało tego – taki spamer może nawet napisać program, który wyszukuje fora dyskusyjne (od czego są Google) i automatycznie zakłada nowe konta, loguje się i tworzy nowe wątki (SPAM). Jednak są skuteczne formy walki z takimi spamerami. Jakiś czas temu napisałem prosty skrypt, który po zauważeniu zakazanego słowa nie publikował wiadomości na forum. Jednak tutaj musiałem ostrożnie dodawać słowa, bo nie każdy, kto pisze viagra, ma na celu zareklamować stronę, na której można kupić ten specyfik (wyobraź sobie, że na forum medycznym dwóch lekarzy rozmawia o negatywnych skutkach stosowania tego specyfiku, a tu ich wypowiedzi nie są publikowane, gdyż w ich wypowiedziach pojawia się zakazane słowo: “viagra”). Dlatego też do czarnej listy dodawałem adresy spammerskich stron. Jednak spamerzy co chwilę zakładali nowe domeny i taka zabawa

w kotka i myszkę nie przynosiła dobrych efektów. Jednak postanowiłem troszkę namieszać: dodałem w formularzu rejestracyjnym nowe pole, w którym trzeba wpisać imię Małysza. Prawie każdy Polak wie ,jak ma na imię Małysz i bez problemu odpowie na to pytanie, a obcokrajowiec nieznający języka polskiego nawet nie będzie wiedział, o co chodzi (co prawda ludzie się czepiali, że zawsze znajdzie się ten 1% Polaków, którzy nie znają imienia Małysza, ale można zadawać inne pytania – np. “Jakiego koloru jest niebo”).



The image shows a registration form with several fields. A red arrow points to the field labeled "Wpisz imię Małysza *". The form includes the following fields and labels:

- Pola oznaczone * są wymagane, chyba że napisano inaczej
- Użytkownik: *
- Adres email: *
- Wpisz imię Małysza *
- Hasło: *
- Potwierdź Hasło: *
- Jeśli w jakikolwi
- Kod potwierdzający: *
- Wprowadź kod dokładnie tak jak powyżej. Uwaga: Cyfrę zero rozpoznaje
- przekreśleniu.

Efekt? Zabezpieczenie wprowadziłem w okolicach 13 stycznia. Do dzisiaj (10 maja) na forum nie pojawił się ani jeden spam. To zabezpieczenie można wykorzystać również w serwisach internetowych, w których pod artykułami można zamieścić swój komentarz itp. Odnośnie mojego [blogu](#), to stosuję inne zabezpieczenie: wtyczkę [Akismet](#), która usunęła kilka tysięcy spamów, a przepuściła może pięć (instalacja tej wtyczki jest banalnie

prosta – wystarczy tylko skopiować odpowiedni plik do odpowiedniego katalogu).

Jak wdrożyć to zabezpieczenie na swoim forum (opartym na skrypcie phpBB2)?

1. W pliku **usercp_register.php** znajdź ciąg znaków: // **Get current date** i w następnej linii dopisz następujący kod:

```
if (trim(strtolower($_HTTP_POST_VARS['malysz']))!="adam")
{
message_die(GENERAL_ERROR, 'Nie wpidałeś imienia
Małyszka (lub wpisałeś błędne imie). Prawdopodobnie jesteś
spammerskim robotem', "", __LINE__, __FILE__, "");
}
```

2. W pliku **templates/subSilver/profile_add_body.tpl** znajdź następujący ciąg znaków:

```
<tr>
<td class="row1"><span
class="gen">{L_EMAIL_ADDRESS}: *</span></td>
<td class="row2"><input type="text" class="post"
style="width:200px" name="email" size="25"
maxlength="255" value="lukasz@ww.pl" /></td>
</tr>
```

3. i po nim dodaj następujący kod:

```
<tr>
<td class="row1"><span class="gen">Wpisz imię Małysza
* </span></td>
<td class="row2"><input type="text" class="post"
style="width:200px" name="małysz" size="10"
maxlength="255" value="" /></td>
</tr>
```

Jeśli nie korzystasz z forum opartego na phpBB2, ale z innego skryptu, a znasz choć trochę PHP, to wprowadzenie podobnego zabezpieczenia nie będzie stanowiło wielkiego problemu, a zaoszczędzisz masę czasu na usuwaniu spamu.

Materiały uzupełniające

Ten ebook nie wyczerpuje tematu, jakim jest spam. Chciałem jedynie udzielić kilku prostych i skutecznych wskazówek, dzięki którym nie będziesz musiał szukać ważnej wiadomości wśród sterty reklam różnych medykamentów albo inwestycji finansowych. Poniżej prezentuję kilka ciekawych serwisów internetowych, które są świetnym uzupełnieniem tego ebooka:

- <http://nospam-pl.net> – obszerny serwis poświęcony spamowi, dość często jest aktualizowany i można stracić poczucie czasu w trakcie czytania różnych artykułów :-)
- <http://pl.wikipedia.org/wiki/Spam> – Wikipedia to darmowa encyklopedia, którą tworzą internauci. Każdy może podzielić się swoją wiedzą. To konkretne hasło ogólnie omawia, czym jest spam, a także informuje, co ma wspólnego konserwa z niechcianymi e-mailami reklamowymi.
- <http://www.antyspam.prv.pl> – strona (rzadko aktualizowana) zawierająca praktyczne porady, jak walczyć ze spamerami. Szata graficzna jest bardzo skromna, ale od wyglądu ważniejsza jest zawartość.
- http://daszkiewicz.net/spam_u.php – strona z dodatkami do tego ebooka (są tam wszystkie omawiane pliki). Na tej podstronie dodatkowo znajduje się darmowy raport “Jak nie zostać spamerem”, który powinien przeczytać każdy, kto chce wysyłać mailingi (maile z informacją o aktualizacji swojej strony WWW bądź nowych produktach w sklepie internetowym).

- [Spam. Profilaktyka i obrona](#) – książka wydawnictwa Helion, obszernie opisująca zjawisko spamu (są tam opisane bardziej zaawansowane problemy, np. jak namierzyć spamera, jak mu uprzykrzyć życie). Znajdziemy tam również opisy programów m.in. do filtrowania poczty oraz informacje o profilaktyce. Książka skupia się też na innych rodzajach spamu – np. niechcianych reklamach w komunikatorach internetowych bądź ulotkach reklamowych. Gorąco polecam.

