



Federacja Konsumentów  
Pl. Powstańców Warszawy 1/3  
00-030 Warszawa  
tel. (22) 827 11 73  
fax (22) 827 90 59  
e-mail: [porady\\_prawne@federacja-konsumentow.org.pl](mailto:porady_prawne@federacja-konsumentow.org.pl)  
[www.federacja-konsumentow.org.pl](http://www.federacja-konsumentow.org.pl)

Ulotka została wykonana przez Federację Konsumentów oraz działającą w ramach Naukowej i Akademickiej Sieci Komputerowej (NASK) zespół CERT Polska. Ulotka powstała ze środków finansowych przekazanych przez Urząd Ochrony Konkurencji i Konsumentów.

- Nie ufaj listom wyglądającym, jakby wysłał je np. Twój bank, w których znajduje się prośba o potwierdzenie danych, haseł lub nawet numerów PIN czy CVV2, czy to przez e-mail, czy też na stronie, do której wskazuje link w wiadomości. Banki ani inne poważne instytucje nie gubią takich danych. W razie najmniejszych wątpliwości, skontaktuj się ze swoim bankiem w inny niż wskazany w wiadomości sposób, np. przez telefon.
- Nie daj się nabrać na historyjki o wielkim majątku, do którego odzyskania potrzebna jest właśnie Twoja drobna pomoc.
- To nieprawda, że ktoś dostaje parę centów za każdy wysłany mail – niestety, w ten sposób nie pomożesz nikomu, kogo dotknęło nieszczęście. Pomożesz za to zapchać skrzynki pocztowe swoich znajomych. Jeśli ktoś prosi o pomoc przez wpłatę na rachunek bankowy – zadaj sobie nieco trudu, by sprawdzić, czy rzeczywiście jest to ktoś potrzebujący.
- Wielu administratorów kont pocztowych oferuje jakiś rodzaj ochrony przed niechcianą korespondencją. Ze względu na niejasność kryteriów, co jest spamem, a co nie, większość mechanizmów wymaga współpracy użytkownika, który musi odpowiednio oznaczyć otrzymaną wiadomość jako niechcianą, aby ułatwić rozpoznawanie podobnych przesyłek w przyszłości. Trzeba zwrócić uwagę, że z filtrowaniem spamu związane jest ryzyko zarówno zawodności filtrów w odławianiu niepożądanych wiadomości, jak i możliwość, że list, który chcielibyśmy otrzymać, zostanie błędnie rozpoznany jako spam i zatrzymany.

## Gdzie interweniować?



Przepisy przewidują odpowiedzialność karną zarówno za bezprawne wykorzystywanie danych osobowych, jak i przesyłanie niezamówionych informacji handlowych. Kto przesyła za pomocą środków komunikacji elektronicznej niezamówione informacje handlowe, podlega karze grzywny (art. 24 ust. 1 ustawy o świadczeniu usług drogą elektroniczną). Ściganie wykroczenia przesyłania niezamówionych informacji handlowych następuje na wniosek pokrzywdzonego. Może się też okazać, że w następstwie otrzymania wielu niezamówionych wiadomości elektronicznych Twój komputer zostanie zablokowany a nawet uszkodzony. Jeżeli w takim przypadku poniesiesz materialną szkodę, której wysokość będziesz potrafił wykazać (np. przedstawiś rachunek za naprawę lub wymianę części), możesz żądać odszkodowania od nieuczciwego nadawcy. Należy jednak zaznaczyć, iż konieczne jest w tym celu wytoczenie powództwa na drodze cywilnoprawnej, a udowodnienie szkody może być w wielu przypadkach znacznie utrudnione. Przykład: Komputer, na którym wykonywałeś zamówioną pracę, został zablokowany spamem, przez co nie wykonałeś w terminie pracy i nie otrzymałeś zapłaty. W takim wypadku możesz żądać

5

od sprawcy szkody zapłaty, której nie otrzymałeś w związku z niedotrzymaniem terminu.

Jeżeli uważasz, że Twoje dane osobowe są wykorzystywane bezprawnie lub gdy otrzymujesz niezamówione informacje handlowe, możesz złożyć skargę do:

- Urzędu Ochrony Konkurencji i Konsumentów ([www.uokik.gov.pl](http://www.uokik.gov.pl)),
- Generalnego Inspektora Ochrony Danych Osobowych ([www.gioudo.gov.pl](http://www.gioudo.gov.pl)),
- Możesz również złożyć zawiadomienie na Policję w związku z popełnieniem wykroczenia,
- Federacji Konsumentów ([www.federacja-konsumentow.org.pl](http://www.federacja-konsumentow.org.pl)),
- Powiatowego (Miejskiego) Rzecznika Konsumentów.

Przypadki zagrożenia lub naruszenia bezpieczeństwa, jak np. szczególnie dotkliwy spam, możesz też zgłosić do zespołu CERT Polska ([www.cert.pl](http://www.cert.pl)) lub swojego dostawcy usług, ale pamiętaj o tym, że sama treść wiadomości wyświetlana przez program pocztowy nie wystarcza do ustalenia rzeczywistego źródła listu. W szczególności wszystkie informacje zawarte w polu „Od” i „Do”, a więc dane nadawcy i odbiorcy, mogą być sfalszowane przez nieuczciwego wysyłającego. Dlatego nigdy pochopnie nie wysyłaj skarg na nadawcę, opierając się jedynie na tych informacjach. Przy przekazywaniu wiadomości dalej celem jej zbadania przez eksperta, załącz pełne nagłówki (szczegółowe instrukcje zależą od sposobu i oprogramowania używanego przez Ciebie do korzystania z poczty elektronicznej – patrz np.: <http://www.cert.pl/faq#4.4>) lub skorzystaj z opcji przesłania wiadomości jako załącznik, jeżeli Twój program ją oferuje.

## Co jeszcze można zrobić w walce ze spamem?



Spam jest ściśle powiązany z biznesem w sieci. Jeśli wspierasz ten biznes, kupując produkty i usługi reklamowane z wykorzystaniem spamu, to sprawiasz, że nieuczciwi sprzedawcy nadal będą z niego chętnie korzystali, a Twoja skrzynka pocztowa będzie coraz bardziej zapchana.

Podstawa prawna:

- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz U Nr 144 z 2002 r., poz. 1204 z późn. zm.),
- Ustawa z dnia 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny (Dz U nr 22, poz. 271 z późn. zm.),
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz U nr 133, poz. 883 z późn. zm.).

6

ABC konsumenta



Federacja Konsumentów

prywatność w sieci

## Czym jest spam?

Spam bardzo często utożsamiany jest z pojęciem niechcianej i niezamówionej wiadomości wysyłanej za pomocą poczty elektronicznej. Należy jednak pamiętać, że zjawisko to ma dużo szerszy zakres oddziaływania. Za spam należy bowiem uznać wszelką niechcianą korespondencję pojawiającą się na następujących platformach komunikacyjnych: poczta elektroniczna, telefony komórkowe (sms, mms), komunikatory internetowe (np. ICQ, Gadu-Gadu), czaty (IRC), fora dyskusyjne oraz strony WWW (i znajdujące się tam tzw. wyskakujące okienka). Definicja spamu w szerokim tego słowa znaczeniu powinna uwzględniać następujące elementy:

- jest to wiadomość, której treść jest niezależna od tożsamości odbiorcy w związku z tym, że wiadomość ta może być przesyłana do wielu niezależnych odbiorców;
- odbiorca nie wyraził wcześniej zgody na otrzymanie wiadomości, przy czym zgoda ta musi być wyrażona w sposób weryfikowalny, świadomy, wyraźny i możliwy do odwołania;
- z okoliczności wynika, że wysyłający odniósł niewspółmierną korzyść z faktu wysłania wiadomości w stosunku do korzyści, jaką odniósł odbiorca w związku z jej odbiorem.

Obecnie korespondencja zaliczana do spamu coraz częściej wykorzystywana jest posilkowo do działań kryminalnych w świecie cyfrowym, takich jak próby wyłudzeń informacji finansowych (numery kont oraz hasła dostępu) czy wysyłanie zamaskowanych wiadomości przez osoby podszywające się pod zaufanych nadawców („brand-spoofing”, „phishing”).

## W jaki sposób trafia do nas spam?

Pamiętaj, że spam jest dla nieuczciwego sprzedawcy jedną z najtańszych form dotarcia do konsumentów ze swoją ofertą, gdyż większość kosztów przerzucona jest na odbiorcę. Dlatego nadawcy nie muszą kierować listów do określonej grupy odbiorców, którzy mogą być zainteresowani ofertą, i godzą się na to, że ogromna większość kopii zostanie przez adresatów zignorowana bądź w ogóle do nich nie dotrze. W konsekwencji, każdy adres e-mail jest dla nich równie przydatny, niezależnie od drogi, jaką został pozyskany. Wyszukiwanie działających adresów e-mail

i tworzenie list, które następnie sprzedawane są nieuczciwym sprzedawcom, stało się jedną z gałęzi działalności internetowego podziemia. Na podstawie doświadczeń, przeprowadzanych m. in. przez Amerykańską Federalną Komisję Handlu (FTC) oraz Center for Democracy and Technology, uzyskano obraz metod działania „łowców adresów e-mail”. Wynika z niego, że:

- Najbardziej narażone na otrzymywanie niechcianej korespondencji są adresy umieszczone na publicznie dostępnych stronach WWW – podając swój adres w czytelnej formie, „zyskujesz” niemal pewność, że zostanie on odszukany przez programy przeszukujące zawartość sieci i umieszczony na listach dystrybucyjnych spamerów.
- Drugą grupą największego ryzyka są adresy używane na grupach dyskusyjnych. Ich przeglądanie dla programów jest równie łatwe jak w przypadku stron WWW i jest to źródło niemal równie popularne.
- Często, aby korzystać z serwisu WWW, musimy dokonać rejestracji z użyciem adresu e-mail. Dotyczy to zarówno rozmaitych forów dyskusyjnych, jak i dużych sklepów internetowych. Zazwyczaj przy rejestracji mamy możliwość zapoznania się z polityką prywatności stosowaną wobec udostępnianych danych. Choć w większości serwisów jest ona respektowana, czasem zawiera ona przyzwolenie na udostępnianie adresu innym podmiotom. Bywa także, że właściciel serwisu jest nieuczciwy i sprzedaje listy adresów swoich użytkowników.
- Adresy e-mail mogą być także odgadane przez generowanie kolejnych ciągów znaków – najczęściej z wykorzystaniem słowników imion i popularnych wyrazów.

Są to najczęstsze, choć nie jedyne, sposoby pozyskiwania adresów. Na przykład z komputera zaatakowanego przez wirus komputerowy mogą „wyciec”, a w konsekwencji trafić na listy używane przez spamerów, adresy osób znajdujące się w książce adresowej.

## Co na to prawo?

Zgodnie z Konstytucją Rzeczypospolitej Polskiej każdy ma prawo do ochrony prawnej życia prywatnego, zaś władze publiczne mają obowiązek chronić konsumentów przed działaniami zagrażającymi ich zdrowiu, prywatności i bezpieczeństwu oraz przed nieuczciwymi praktykami rynkowymi (art. 47 i 76 Konstytucji). Nie ulega wątpliwości, że spam godzi w interesy użytkowników Internetu, przede wszystkim w prawo do prywatności.

**Prywatność to prawo do bycia pozostawionym w spokoju**  
Spam jest nieuczciwą praktyką rynkową, którą prawo polskie i europejskie zwalczą.

Prawo europejskie to dyrektywy, czyli wskazówki dla krajów członkowskich, w jaki sposób mają one regulować dane zagadnienie. Polska zrealizowała postanowienia dyrektyw, uchwalając odpowiednie ustawy.

Najważniejsze dla naszego omówienia jest postanowienie, iż zakazane jest przysyłanie niezamówionej informacji handlowej (potocznie: spam) skierowanej do oznaczonego odbiorcy za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej.

**Przykład:** otrzymujesz drogą mailową propozycję zakupu oprogramowania od firmy, której nie wyraziłeś wcześniej zgody na przysyłanie informacji handlowych.

Informacje handlowe można przysyłać wyłącznie za zgodą odbiorcy, jednakże zgoda ta nie może być dorozumiana (za zgodę można jednak uznać udostępnienie adresu poczty elektronicznej w celu otrzymywania informacji handlowych).  
Przykład: otrzymujesz reklamę pewnej firmy za pośrednictwem portalu internetowego, który wcześniej udostępnił Ci bezpłatną skrzynkę poczty elektronicznej. Przy zakładaniu skrzynki zgodziłeś się dobrowolnie na otrzymywanie reklam i w treści informacji handlowej znajduje się dopisek: „List został wysłany za zgodą użytkowników Portalu Internetowego i zgodnie z jego regulaminem”.

Nadawca zamówionej informacji handlowej (a więc takiej, na którą wyraziłeś zgodę) zgodnie z prawem powinien udostępnić Ci informacje o sobie, w szczególności nazwę, adres siedziby firmy oraz adres elektroniczny. Niedopełnienie przez nadawcę obowiązku podania powyższych danych albo podanie danych nieprawdziwych/niepełnych podlega karze grzywny. Jeżeli informacja handlowa takich danych nie zawiera, możesz przypuszczać, że masz do czynienia ze spamerem.

## Jak więc chronić swój adres e-mail?

- Umieszczając swój adres na stronie WWW – niezależnie czy jest to Twoja strona domowa, czy np. komentarz na blogu – zamaskuj go. W przypadku Twojej strony możesz umieścić adres w formie obrazka zamiast tekstu lub posłużyć się specjalnym zapisem używanym w HTML, który uczyni adres nieczytelnym w treści strony, ale widocznym przy jej wyświetleniu (np. <http://www.cert.pl/tools/mailencode.php>). Jeżeli podajesz adres, np. w komentarzu na forum, możesz wstawić ciąg znaków, który będzie umożliwiał chętnym do korespondencji łatwe zorientowanie się w prawdziwym adresie, ale zmyli programy wyszukujące, np.: jan@WYT-NIJTOpoczta.isp.pl.
- Rozważ posługiwanie się dwoma (lub więcej) adresami e-mail. Oddzielnym adresem posługuj się w korespondencji z przyjaciółmi i znajomymi, którym ufasz, a innym tam, gdzie zachodzi ryzyko, że adres trafi w niepowołane ręce (np. przy zakładaniu kont w serwisach WWW). Jeżeli okaże się, że na konto „publiczne” zaczynasz otrzymywać duże ilości spamu, po prostu z niego zrezygnuj i załóż nowe. W każdym przypadku wskazane jest oddzielenie konta służbowego, używanego w firmie, w której pracujesz, od prywatnego.

- Czytaj dokładnie politykę prywatności serwisu WWW, w którym zmuszony jesteś podać swój adres e-mail. Jeżeli taki dokument nie jest dostępny w żadnej formie, powinieneś potraktować serwis jako mało godny zaufania. Dotyczy to także serwisów oferujących bezpłatne konta pocztowe. Często rejestrując się w nich, wyrażamy zgodę na otrzymywanie korespondencji od firm trzecich. Takiej korespondencji nie możemy uznać za niezamawianą.

- Unikaj prostych i krótkich adresów. Choć są one wygodniejsze w stosowaniu, łatwo mogą paść ofiarą ataku słownikowego. Lepiej więc wybrać adres dłuższy, zawierający cyfry lub znaki specjalne, np. [Imie.Nazwisko@poczta.isp.pl](mailto:Imie.Nazwisko@poczta.isp.pl).

## Co zrobić gdy otrzymujesz spam?

- Przede wszystkim upewnij się, że nie wyraziłeś zgody na otrzymywanie korespondencji od nadawcy lub Twój adres nie został mu przekazany przez inną firmę, której pozwoliłeś na udostępnianie go osobom trzecim. Jeżeli

informacja o udzieleniu przez Ciebie zgody znajduje się w otrzymanym liście i jest ona prawdziwa, masz prawo w każdej chwili, bez podawania przyczyny, zgodę tę odwołać. Wystarczy przesłać pocztą elektroniczną następującą treść: „Sprzeciwiam się dalszemu wykorzystywaniu przez Waszą firmę moich danych osobowych do celów marketingowych i przekazywania tych danych innym podmiotom”.  
Ale uwaga: zdarza się, że po złożeniu protestu przeciwko przesyłaniu niechcianych informacji handlowych następują groźby ze strony nadawcy. Groźby takie mogą mieć charakter karalny; należy wówczas złożyć zawiadomienie na Policję.

- Jeżeli list został wysłany bez Twojej zgody, także jeśli nadawca twierdzi, że miał taką zgodę, lecz jesteś pewien, że jest to nieprawda, w żadnym wypadku nie odpowiadaj na list drogą elektroniczną. Odpowiedź od Ciebie będzie dla spamera sygnałem, że jego list rzeczywiście dotarł, a Ty przeczytałeś jego treść. To upewni go, że adres działa i warto na niego wysłać kolejne oferty. Ta sama zasada dotyczy możliwości wypisania się z list dystrybucyjnych przez kliknięcie odnośnika w liście (np. dostajesz informację handlową z dopiskiem: „Jeżeli nie zgadzasz się na otrzymywanie następujących wiadomości, odpisz na adres „xxx@spam.com.pl”) – zazwyczaj zamiast pożądanego skutku, zaowocuje to większą ilością niechcianej korespondencji.

**Nie bójmy się Internetu,  
poznajmy go  
dla bezpieczeństwa  
naszych dzieci**

[www.onlinechildprotection.org](http://www.onlinechildprotection.org)

**Nasze dzieci  
bezpieczne  
w Sieci**

Więcej informacji na temat  
Stowarzyszenia  
Konsumentów Polskich:

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

Stowarzyszenie  
Konsumentów Polskich

ul. Gizów 6,  
01-249 Warszawa  
Tel. (022) 634 06 68

Fax (022) 634 06 67

E-mail: [sekretariat@skp.pl](mailto:sekretariat@skp.pl)

Więcej informacji na temat  
programu Socrates:

[www.socrates.org.pl](http://www.socrates.org.pl)

Fundacja Rozwoju Systemu  
Edukacji  
Narodowa Agencja Programu  
Socrates

ul. Mokotowska 43,  
00-551 Warszawa

Tel. (022) 622 37 12

Fax (022) 622 37 10

E-mail: [kontakt@frse.org.pl](mailto:kontakt@frse.org.pl)

8 9 5 4 2 2

9 9 0 5 6 2

9 4 4 5 9 8

0 4 3 2 1 3 6

7 8 9 0 2 2 1

2 2 3 9 7 3

7 4 4 0 0 1 1

7 3 2 2 4 4

6 8 8 6 2 1

0 4 6 8 1 1

6 8 9 5 3 0



1 0 0 3 5

3 3 2 1

1 2 3 4

5 6 7 8

2 2 1 2 0

8 9 6 6 3

4 9 9 5

4 0 6 7

9 9 0 0 4

2 7 0 5

9 7 5 2 7

Niniejszy projekt został zrealizowany przy wsparciu finansowym Wspólnoty Europejskiej w ramach programu Socrates. Treści samego projektu lub materiałów nie odzwierciedlają stanowiska Komisji Europejskiej czy Agencji Narodowej w danej sprawie, a w związku z tym ani Komisja Europejska, ani Agencja Narodowa nie ponosi za nie odpowiedzialności.



Stowarzyszenie  
Konsumentów Polskich



Edukacja i Kultura

Socrates  
Grundtvig

Internet stał się nieodłącznym elementem naszego życia. Za pośrednictwem sieci internetowej wyszukiujemy informacje, kontaktujemy się ze znajomymi, dokonujemy zakupów.

Największą grupę użytkowników Internetu stanowią dzieci i młodzież. Sieć jest dla nich znakomitym narzędziem edukacji i zabawy. Internet to jednak nie tylko nowe, interesujące możliwości ale również zagrożenia, zwłaszcza dla najmłodszych użytkowników. W sieci, podobnie jak w realnym życiu, grasują przestępcy. Posługują się jedynie bardziej nowoczesnymi i wyrafinowanymi metodami.

Pierwszym krokiem w skutecznej walce z każdym przeciwnikiem jest zdobycie o nim jak najwięcej informacji. Niestety, jak pokazują liczne badania, świadomość zagrożeń internetowych i sposobów radzenia sobie z nimi jest wśród dorosłych nadal niewystarczająca.

Dlatego Stowarzyszenie Konsumentów Polskich we współpracy z organizacjami konsumenckimi z Bulgarii, Czech, Słowacji i Litwy uruchomiło stronę internetową [www.onlinechildprotection.org](http://www.onlinechildprotection.org) zawierającą materiały i narzędzia edukacyjne adresowane do rodziców, opiekunów, nauczycieli i szkoleniowców.



Na stronie dostępny jest między innymi podręcznik edukacyjny „Nasze dzieci bezpieczne w Sieci”. Znajdziecie w nim:

- objaśnienie podstawowych informacji i pojęć związanych z Internetem,
- wskazówki, jak w prosty sposób przekazywać dziecku wiedzę o niebezpieczeństwach w sieci,
- praktyczne porady, jak rozpoznać i skutecznie zwalczać internetowe zagrożenia,
- opisy darmowego oprogramowania zabezpieczającego,
- dane kontaktowe instytucji, zajmujących się problemem bezpieczeństwa w sieci,
- odnośniki do stron edukacyjnych i innych projektów poświęconych ochronie najmłodszych użytkowników Internetu.

**Pojęcia takie, jak „phishing”, „spyware” lub „cyberprzemoc” nic Ci nie mówią?**

**Nie wiesz, na czym polega kontrola rodzicielska i czym się różni robak od wirusa?**

**Zajrzyj na:**

**[www.onlinechildprotection.org](http://www.onlinechildprotection.org)**