ONYX POSTMASTER

FILTRY ANTYSPAMOWE

OPIS FUNKCJONALNOŚCI

INSTRUKCJA KONFIGURACJI

Wstęp

Poczta elektroniczna stała się dziś narzędziem, bez którego funkcjonowanie wielu firm byłoby niemożliwe, a przynajmniej bardzo utrudnione.

Rozwojowi tego typu komunikacji towarzyszy jednak działanie nieuczciwych firm oraz osób, które za pośrednictwem wiadomości e-mail próbują do nas dotrzeć z ofertą produktów lub usług wcale nam niepotrzebnych.

Spam – czyli masowo rozsyłane wiadomości reklamowe bez zgody odbiorców, stał się obecnie wielkim problemem użytkowników poczty elektronicznej. Nic tak przecież nie irytuje, jak szukanie ważnych wiadomości wśród setek wiadomości śmieci.

Onyx Postmaster wśród swoich funkcjonalności ma również pięć różnych filtrów antyspamowych. Można by powiedzieć po co aż pięć, wystarczyłby jeden a dobry. W przypadku walki ze spamem nie jest to jednak właściwe podejście.

Rozbudowywanie funkcji ochrony antyspamowej wymusza na spamerach tworzenie wiadomości, które w sprytny sposób ominą stosowane zabezpieczenia. W związku z tym każdy z filtrów klasyfikuje wiadomości pod różnymi kryteriami (np. adres e-mail nadawcy, adres IP serwera nadawcy, treść wiadomości itd.). Im więcej elementów wskazujących na to, że dana wiadomość jest spamem jesteśmy wstanie wyodrębnić i przeanalizować, tym większa skuteczność zastosowanej ochrony. Niestety nie ma takiego filtra, który w 100% wyeliminuje problem śmieci w naszej skrzynce. Przez zastosowanie dostępnych narzędzi sprawiamy, że spamu docierającego do naszej skrzynki bez żadnego oznaczenia jest już stosunkowo mało.

Trzeba mieć jednak tę świadomość, że to spamer wymyśla metodę oszukania filtrów, a dopiero potem firmy walczące ze spamem mogą szukać możliwości załatania luki, przez którą przedostał się spam.

Jest jeszcze jedna bardzo istotna kwestia związana z ograniczaniem niechcianych wiadomości w naszej skrzynce. Mam na myśli indywidualną konfigurację filtrów.

Tak jak każdy człowiek różni się od drugiego różnymi cechami, ma różne gusta, upodobania, nawyki, tak samo zarządzane przez człowieka organizacje nie są takie same. W kwestii walki ze spamem ma to duże znaczenie.

Wiadomość, która dla jednej firmy jest spamem (np. reklama zegarków – tak często przesyłana w formie spamu), dla drugiej może być ważna (np. hurtownia zegarków). Nie możemy zatem jednoznacznie określić, że wszystkie wiadomości zawierające w swej treści np. nazwę marki zegarków są dla użytkowników systemu Onyx Postmaster niepożądanymi.

Można więc przyjąć, że filtry antyspamowe bez dopasowania ich konfiguracji pod nasze potrzeby będą działały ograniczając ilość napływającego spamu, ale wśród wyników pracy filtrów znajdą się też pomyłki (np. wiadomość od naszego ważnego kontrahenta zostanie sklasyfikowana jako spam). Właściwa konfiguracja dostępnych narzędzi pozwoli natomiast ograniczyć ilość pomyłek do minimum.

Mam nadzieję, że informacje zawarte w tej broszurze pozwolą właściwie dostosować filtry antyspamowe do Państwa wymagań. Tym samym spam nie będzie już dla Państwa problem zauważalnym w codziennej pracy.

DYREKTOR
Działu Usług Hostingowych
Tomasz Borusiak

Logowanie do panelu www

Ustawienia większości opcji filtrów antyspamowych dokonuje się po zalogowaniu do swojej skrzynki poprzez panel www.

W tym celu należy w przeglądarce internetowej wybrać adres www.postmaster.onyx.pl , następnie w pole login trzeba wpisać pełen adres skrzynki, której ustawienia chce się zmienić, a w pole hasło – hasło do skrzynki. Po wprowadzeniu wymaganych danych należy kliknąć przycisk LOGIN.

Jeżeli wprowadzone dane są poprawne pojawi się komunikat „Zostałeś zalogowany", a link „Twoje konto" stanie się aktywny. Później trzeba wybrać kolejno TWOJE KONTO > EDYTUJ PARAMETRY i przewinąć otwartą stronę w dół do części nr 5 „Parametry filtrów antyspamowych".

OPIS POSZCZEGÓLNYCH FILTRÓW ANTYSPAMOWYCH DZIAŁAJĄCYCH W SYSTEMIE ONYX POSTMASTER

Filtr antyspamowy WBBL

Opis. Filtr WBBL (czarna – biała lista) klasyfikuje wiadomości przychodzące po nazwach domenowych, ma przy tym najwyższy priorytet w stosunku do innych filtrów antyspamowych. Oznacza to, że wpisanie adresu e-mail nadawcy na białą listę, powoduje wyłączenie skanowania przez inne filtry antyspamowe wiadomości przychodzących z tego konkretnego adresu – przyjmuje się, że wiadomości z tego adresu nie są spamem. Natomiast gdy wpiszemy adres e-mail nadawcy na czarną listę, wszystkie wiadomości z tego adresu będą traktowane jako niepożądane i bez skanowania przez inne filtry nie będą przyjmowane przez serwer.

Przykłady zastosowań. Jeżeli nie możesz wypisać się z newslettera, który kiedyś chciałaś/-eś/ otrzymywać, pomimo Twoich próśb cały czas wysyłane są do Ciebie wiadomości reklamowe, wpisz adres nadawcy na czarną listę, a problem zniknie.

Gdy Twój bank wysyła do Ciebie wyciągi z konta drogą mailową, i chcesz być pewna /-ien/, że e-mail nie zawieruszy się wśród spamów, wpisz adres e-mail banku na białą listę. Od tego momentu wiadomości wysyłane z tego adresu nie będą sprawdzane przez inne filtry antyspamowe.

Sposób konfiguracji. Dopisywanie lub usuwanie adresów e-mail lub nazw domen na czarną lub białą listę odbywa się poprzez panel www. Aby to zrobić należy zalogować się do swojego konta (patrz w części „Logowanie do panelu www") .

Pod hasłem „Konfiguracja modułu WBBL" w części nr 5, znajdują się opcje konfiguracyjne tego filtra.

W „**Ufaj nadawcom**" przewidziano trzy możliwe ustawienia:

a) **nikomu** – wszystkie wiadomości przychodzące na skrzynkę, skanowane są przez włączone filtry anyspamowe,
b) **z Twojego serwera pocztowego** – filtry antyspamowe skanują wszystkie wiadomości przychodzące do skrzynki, z wyjątkiem tych, które pochodzą ze skrzynek założonych na tym samym serwerze (wiadomości przesyłane pomiędzy pracownikami naszej firmy nie będą oznaczane jako [SPAM]).
c) **z każdego serwera Onyx Postmaster** (**ustawienie zalecane**)– filtry antyspamowe skanują wszystkie wiadomości przychodzące do skrzynki, z wyjątkiem wiadomości wysyłanych z wszystkich skrzynek założonych na serwerze firmy Onyx. Jeżeli Państwa firma korzysta z kilku odrębnych serwerów Onyx Postmaster, ustawienie tej opcji spowoduje, że wszystkie wiadomości przesyłane pomiędzy skrzynkami z tych serwerów nie będą oznaczane jako [SPAM].

Pod tekstem „Lista wzorców adresów filtra WBBL:" znajduje się pole, w które należy wpisywać adresy na białą lub czarną listę. Format w jakim należy wpisywać adresy wraz z przykładami znajduje się w linku „Opis wzorców adresów" poniżej tabeli.

Filtr antyspamowy RBLL

Opis. Spamerzy do rozsyłania wiadomości używają oczywiście wielu różnych adresów e-mail. Dlatego w tym wypadku możliwości, które daje filtr WBBL (czyli możliwość wpisania adresu e-mail na czarną listę) są mało skuteczne. Musielibyśmy cały czas dopisywać nowe adresy na listę, a kolejny spam przyszedłby i tak z nowego konta. Filtr RBLL po pierwsze korzysta z ogólnoświatowej bazy trefnych adresów, która to baza jest aktualizowana na bieżąco bez naszego udziału. Po drugie baza ta zawiera adresy IP (czyli numeryczne) komputerów, z których rozsyłany jest spam. Dzięki temu niezależnie jakim adresem e-mail posłuży się spamer, jeżeli adres IP jego komputera lub serwera pocztowego za pośrednictwem którego działa został już wpisany do bazy, filtr zidentyfikuje wiadomości wysyłane przez niego jako spam.

Sposób konfiguracji. Z uwagi na to, że filtr RBLL jest bezpłatny, a możliwość pomyłki mało prawdopodobna filtr ten zapewne będzie na Państwa serwerze włączony. Istnieje jednak możliwość wyboru jednego z dwóch dostępnych sposobów postępowania z wiadomościami zidentyfikowanymi przez filtr RBLL jako spam. Wyboru opcji dokonuje się indywidualnie dla każdej skrzynki. W celu zmiany ustawień należy zalogować się do swojej skrzynki (patrz w części „Logowanie do panelu www").

Pod hasłem „Parametry filtrów antyspamowych" (część nr 5) znajdują się pola wyboru opcji poszczególnych filtrów, które w zależności od ustawień wybranych przez osobę administrującą Państwa serwerem mogą być aktywne lub zablokowane. Wśród parametrów znajduje się parametr „Akcja RBLL" z możliwością wyboru jednej z dwóch opcji:

a) **oznakuj spam** – wybór tej opcji spowoduje, że wszystkie wiadomości zidentyfikowane przez filtr RBLL zostaną oznaczone w temacie hasłem [SPAM]. Dzięki oznaczeniu wiadomości jako [SPAM] w temacie, istnieje możliwość ustawienia w programie pocztowym tzw. reguły wiadomości (czyli np. ustawienie, że wszystkie wiadomości oznaczone przez filtr mają wpadać do oddzielnego folderu). *Więcej informacji na temat reguł wiadomości, wraz z instrukcjami ich ustawień w zawarto dalszej części.*

b) **usuń spam** – po wybraniu tej opcji, wiadomości zidentyfikowane przez filtr RBLL jako spam będą usuwane na poziomie serwera (nie będą ściągane przez program pocztowy).

Można powiedzieć, że filtr RBLL jest w zasadzie nieomylny – oznacza tylko te wiadomości, wysłane z adresów IP komputerów (lub serwerów pocztowych), z których rozsyłano spam. Błędne oznaczenie może więc wystąpić tylko wtedy, gdy nadawca wiadomości z jakiejś przyczyny znalazł się na ogólnoświatowej liście spamerów. Wybór ustawień pozostawiamy jednak Państwu.

Filtr antyspamowy ASBA

Opis. Niechciane wiadomości reklamowe często charakteryzują się podobną treścią. Można by więc powiedzieć, że problem łatwo wyeliminować za pomocą reguł wiadomości ustawianych w programie pocztowym. Teoretycznie wystarczyłoby ustawić regułę, która wszystkie wiadomości zawierające słowo np. „viagra" usuwałaby bezpośrednio z serwera.
Sprawa nie jest jednak taka prosta. Bliższe przeanalizowanie takich wiadomości pokazuje, że słowo „viagra" wpisywane jest w treści wiadomości na wiele różnych sposobów (ze spacjami między literami, z myślnikami pomiędzy literami, z gwiazdkami pomiędzy literami lub celowo z literówką), a to z kolei powoduje, że dla każdego nowego przypadku musielibyśmy tworzyć nową regułę. Jest to oczywiście celowe działanie wykonywane właśnie po to, aby utrudnić wyłapanie takich wiadomości. Filtr ASBA ma tę właśnie wyższość, że większość dostępnych sposobów różnego wpisywania tekstu wskazującego na to, że wiadomość jest spamem, ma już w swojej bazie.
Co więcej ? Filtr ASBA analizuje treść wiadomości po dwójkach lub też trójkach wyrazów, które w wiadomościach spamowych umieszczane są w bliskim sąsiedztwie. ASBA analizuje ponadto treść tematu, a nawet tzw. logi wiadomości. Tak szczegółowa analiza wiadomości pozwala na odizolowanie dużej części niechcianej poczty.
Poza niewątpliwie wielką skutecznością tego filtra, jest jednak prawdopodobieństwo błędnego oznaczenia wiadomości, która oznaczona być nie powinna. Może się tak zdarzyć gdy treść maila podobna jest to treści zawieranych często w spamie. Z uwagi na to, że większość spamu zawiera treści w języku angielskim, korespondencja w tym właśnie języku częściej ulega błędnej identyfikacji.
Ilość pomyłek filtra ASBA w dużej mierze zależy również od Państwa – szczegóły w części „sposób konfiguracji".

Podstawową możliwością jaką daje filtr ASBA jest jego nauka. Filtr ten zgodnie z wcześniejszym opisem posiada całą bazę przykładów, na podstawie których ocenia czy dana wiadomość jest spamem. Jak wiadomo spamerzy często zmieniają metody i treści zawarte w spamach, dlatego skuteczność filtra ASBA (czyli również ilość pomyłek) zależy w dużym stopniu od nauki filtra. Im więcej błędów filtra będą nam Państwo przesyłali, tym mniejsze prawdopodobieństwo wystąpienia błędu w przyszłości.

Sposób konfiguracji.

W jaki sposób zgłaszać błędy popełnione przez filtr ?

W przypadku gdy wiadomość, która spamem nie jest, a została oznaczona przez filtr hasłem [SPAM] w temacie, ewentualnie gdy wiadomości reklamowe przedzierają się przez filtr bez oznaczenia, należy przesłać taką wiadomość w postaci załącznika (w formacie *.eml) na adres **klasyfikacjaspamu@onyx.pl** . Im więcej błędów będzie przez Państwa zgłaszanych, tym mniej powinno być ich w przyszłości. *Podpowiedź jak przesłać wiadomość w postaci załącznika *.eml zawarto w dalszej części.*

Filtr ASBA jest narzędziem opcjonalnym, dlatego jego dostępność na Państwa koncie uzależniona jest od ustawień wybranych przez osobę administrującą Państwa serwerem.
Aby sprawdzić czy filtr ASBA jest włączony, należy zalogować się do swojej skrzynki (patrz w części „Logowanie do panelu www").

W cześci nr 5, „Parametry filtrów antyspamowych" znajduje się pozycja „Filtr antyspamowy ASBA". Pozycja ta w zależności od ustawień może nie mieć możliwości przestawienia, pełni wtedy rolę informacyjną czy filtr ten jest dla nas włączony, czy też wyłączony. Ewentualnie administrator mógł pozostawić wybór włączenia lub wyłączenia filtra, każdemu użytkownikowi indywidualnie.
W przypadku gdy filtr ASBA dla skrzynki jest włączony, każdy użytkownik ma możliwość wyboru co system pocztowy ma robić, z wiadomościami zidentyfikowanymi przez filtr ASBA jako spam.
Podobnie jak w przypadku ustawień filtra RBLL, również przy filtrze ASBA występuje parametr „Akcja ASBA" umożliwiający wybór jednej z dwóch opcji:

a) **oznakuj spam** – wybór tej opcji spowoduje, że wszystkie wiadomości zidentyfikowane przez filtr ASBA zostaną oznaczone w temacie hasłem [SPAM]. Dzięki oznaczeniu wiadomości jako [SPAM] w temacie, istnieje możliwość ustawienia w programie pocztowym tzw. reguły wiadomości (czyli np. ustawienie, że wszystkie wiadomości oznaczone przez filtr mają wpadać do oddzielnego folderu). *Więcej informacji na temat reguł wiadomości, wraz z instrukcjami ich ustawień w zawarto dalszej części.*
b) **usuń spam** – po wybraniu tej opcji, wiadomości zidentyfikowane przez filtr ASBA jako spam będą usuwane na poziomie serwera (nie będą ściągane przez program pocztowy).

Jak zapisać wiadomość w formacie *.eml umożliwiającym uczenie filtra ASBA ?

W każdym z programów pocztowych zapisywanie i przesyłanie wiadomości w formacie *.eml wykonuje się trochę inaczej. W związku z powyższym poniżej znajdą Państwo instrukcję do dwóch najpopularniejszych programów pocztowych (Outlook Express, Mozilla Thunderbird).

Outlook Express

W tym programie przesłanie błędnie oznaczonego maila na adres klasyfikacjaspamu@onyx.pl jest bardzo prosta. Wystarczy kliknąć prawym klawiszem myszy na błędnie oznaczonej wiadomości (lub nieoznaczonej) znajdującej się np. w folderze „Skrzynka odbiorcza", następnie z rozwiniętego menu proszę wybrać „Prześlij dalej jako załącznik". Spowoduje to utworzenie nowej wiadomości, do której wystarczy wpisać adres odbiorcy, czyli klasyfikacjaspamu@onyx.pl i kliknąć wyślij.

Mozilla Thunderbird

1. Aby wysłać błędnie oznaczoną wiadomość w postaci załącznika *.eml należy kliknąć prawym klawiszem myszy na wybranej wiadomości, a następnie z rozwiniętego w ten sposób menu wybrać opcję „Zapisz jako". UWAGA ! W polu „zapisz jako typ" powinno być wybrane „Wszystkie pliki" lub „Pliki poczty". Po wybraniu odpowiedniego formatu zapisujemy tę wiadomość na swój twardy dysk.

   Po zapisaniu przystępujemy do stworzenia nowej wiadomości, w której jako odbiorcę wpisujemy adres klasyfikacjaspamu@onyx.pl , a następnie z górnego menu wybieramy „Załącz" i wybieramy zapisany wcześniej plik ze swojego dysku. Tak przygotowany mail gotowy jest do wysłania.

2. Jest też drugi sposób. W opcjach programu można ustawić na stałe, aby wszystkie wiadomości przesyłane za pomocą opcji „Przekaż" były przesyłane w formie załącznika. Oczywiście do uczenia filtra ASBA jest to ustawienie wygodniejsze (nie wymaga wcześniejszego zapisywania wiadomości w postaci pliku aby później dołączać go do tworzonej wiadomości). Trzeba jednak pamiętać, że przy zastosowaniu takiego rozwiązania wszystkie wiadomości przesyłane dalej za pomocą funkcji „Przekaż" będą wysyłane nie w postaci tekstowej lecz jako załącznik.
   Aby na stałe ustawić przesyłanie wiadomości jako załącznik po wybraniu opcji „Przekaż" należy kolejno: z głównego menu wybrać NARZĘDZIA > OPCJE > TWORZENIE > OGÓLNE. Przy zwrocie „Przekaż wiadomości" należy z listy wybrać „Jako załącznik".

Filtr antyspamowy IRBL

Opis. Kolejny rodzaj spamu z jakim mamy do czynienia od pewnego czasu, to wiadomości zawierające krótki tekst (nie więcej niż jedno lub dwa zdania) oraz link do strony internetowej. Tekst zawarty w mailu nie jest tekstem, który opisywany wcześniej analizator tekstu (filtr ASBA) mógł rozpoznać jako spam. Filtr IRBL analizuje jednak wiadomość jeszcze głębiej. Sprawdza adres internetowy strony zawarty w wiadomości, tłumaczy go sobie z nazwy domenowej (czyli np. www.onyx.pl na adres IP np. 11.11.11.11. Następnie adres IP weryfikowany jest w ogólnoświatowej bazie trefnych adresów IP serwerów WWW.
Linki do stron internetowych zawarte w wiadomościach spamowych, najczęściej prowadzą do serwerów WWW, których adres IP znalazł się już na czarnej liście. Można więc powiedzić, że filtr dosyć szczelnie blokuje spam tego rodzaju.

Sposób konfiguracji. Filtr IRBL należy również do grupy filtrów bezpłatnych. Dlatego zapewne będzie na Państwa serwerze włączony. Istnieje jednak możliwość wyboru jednego z dwóch dostępnych sposobów postępowania z wiadomościami zidentyfikowanymi przez filtr IRBL jako spam. Wyboru opcji dokonuje się indywidualnie dla każdej skrzynki. W celu zmiany ustawień należy zalogować się do swojej skrzynki (patrz w części „Logowanie do panelu www").

Pod hasłem „Parametry filtrów antyspamowych" (część nr 5) znajdują się pola wyboru opcji poszczególnych filtrów, które w zależności od ustawień wybranych przez osobę administrującą Państwa serwerem mogą być aktywne lub zablokowane. Wśród parametrów znajduje się parametr „Akcja IRBL" z możliwością wyboru jednej z dwóch opcji:

c) **oznakuj spam** – wybór tej opcji spowoduje, że wszystkie wiadomości zidentyfikowane przez filtr IRBL zostaną oznaczone w temacie hasłem [SPAM]. Dzięki oznaczeniu wiadomości jako [SPAM] w temacie, istnieje możliwość ustawienia w programie pocztowym tzw. reguły wiadomości (czyli np. ustawienie, że wszystkie wiadomości oznaczone przez filtr mają wpadać do oddzielnego folderu). *Więcej informacji na temat reguł wiadomości, wraz z instrukcjami ich ustawień w zawarto dalszej części.*
d) **usuń spam** – po wybraniu tej opcji, wiadomości zidentyfikowane przez filtr IRBL jako spam będą usuwane na poziomie serwera (nie będą ściągane przez program pocztowy).

Filtr antyspamowy FRET

Opis. Czy zdarzyło się Państwu odbierać setki wiadomości zwrotnych z różnych serwerów pocztowych? Jeżeli nie to macie Państwo szczęście.
Dokuczliwość tego rodzaju spamu jest duża z uwagi na to, że w ciągu jednego dnia można otrzymać na swoją skrzynkę nawet tysiąc zwrotów.
Problem z tym typem spamu polega na tym, że w zasadzie są to prawdziwe wiadomości zwrotne z serwerów pocztowych, tylko wygenerowane przez spamerów i skierowane na konkretne skrzynki. Nie możemy więc usuwać ich wszystkich, ponieważ może wśród nich znaleźć się zwrot dotyczący wiadomości faktycznie wysłanej przez Państwa. Bez możliwości odczytania takiego zwrotu, po pierwsze nasi klienci nie wiedzieliby o tym, że jest jakiś problem z dostarczeniem wiadomości przez nich wysłanej, a po drugie utrudniłoby to zdefiniowanie przyczyny problemu.
Filtr FRET weryfikuje więc czy zwrot, który dodarł do skrzynki dotyczy wiadomości wysłanej z naszego serwera pocztowego, a w przypadku stwierdzenia że nie, klasyfikuje wiadomość jako spam.

Sposób konfiguracji. Filtr FRET to też darmowe wyposażenie serwera pocztowego Onyx Postmaster. Dlatego zapewne będzie na Państwa serwerze włączony. Istnieje jednak możliwość wyboru jednego z dwóch dostępnych sposobów postępowania z wiadomościami zidentyfikowanymi przez filtr FRET jako spam. Wyboru opcji dokonuje się indywidualnie dla każdej skrzynki. W celu zmiany ustawień należy zalogować się do swojej skrzynki (patrz w części „Logowanie do panelu www").

Pod hasłem „Parametry filtrów antyspamowych" (część nr 5) znajdują się pola wyboru opcji poszczególnych filtrów, które w zależności od ustawień wybranych przez osobę administrującą Państwa serwerem mogą być aktywne lub zablokowane. Wśród parametrów znajduje się parametr „Akcja FRET" z możliwością wyboru jednej z dwóch opcji:

e) **oznakuj spam** – wybór tej opcji spowoduje, że wszystkie wiadomości zidentyfikowane przez filtr FRET zostaną oznaczone w temacie hasłem [SPAM]. Dzięki oznaczeniu wiadomości jako [SPAM] w temacie, istnieje możliwość ustawienia w programie pocztowym tzw. reguły wiadomości (czyli np. ustawienie, że wszystkie wiadomości oznaczone przez filtr mają wpadać do oddzielnego folderu). *Więcej informacji na temat reguł wiadomości, wraz z instrukcjami ich ustawień w zawarto dalszej części.*
f) **usuń spam** – po wybraniu tej opcji, wiadomości zidentyfikowane przez filtr FRET jako spam będą usuwane na poziomie serwera (nie będą ściągane przez program pocztowy).

Filtr FRET jest na tyle nieomylny, że sugerujemy ustawienie opcji „Akcja FRET" na „usuń spam".

W jaki sposób stworzyć regułę wiadomości w programie pocztowym ?

Outlook Express

W celu przekierowania wiadomości oznaczonych jako [SPAM] do oddzielnego folderu w programie pocztowym Outlook Express (aby nie zaśmiecał skrzynki odbiorczej) należy:

- z głównego menu wybrać "Narzędzia"
- potem kolejno "Reguły wiadomości" - "Poczta",
- przy zaznaczonej zakładce "Reguły poczty" proszę kliknąć "Nowa",

W tym miejscu musimy wybrać warunki i akcje dla tworzonej reguły.

- w pkt. 1 należy zaznaczyć opcję "Kiedy w polu temat znajdują się określone wyrazy"
- w pkt. 2 należy zaznaczyć opcję "Przenieś ją do folderu",
- w pkt. 3 po kliknięciu na niebieski link "znajdują się określone wyrazy" trzeba w wolne pole wpisać [SPAM]. Koniecznie w „kwadratowym” nawiasie i dużymi literami ! Zatwierdzić "OK".
- następnie klikamy na niebieski link "folderu", klikamy przycisk „Nowy folder”, wpisujemy jego nazwę np. Spam i zatwierdzamy utworzenie „OK”, a następnie potwierdzamy ponownie „OK” wybór tego folderu.

Reguła jest w tym momencie utworzona. Wszystkie wiadomości oznaczone przez filtry antyspamowe jako [SPAM] będą trafiały do oddzielnego folderu. Raz na jakiś czas sugerujemy sprawdzenie czy przypadkiem jako spam nie została zaznaczona ważna dla Państwa wiadomość.

Microsoft Outlook 2007

W celu przekierowania wiadomości oznaczonych jako [SPAM] do oddzielnego folderu w programie pocztowym Microsoft Outlook 2007 (aby nie zaśmiecał skrzynki odbiorczej) należy:

- z głównego menu wybrać "Narzędzia"
- potem kolejno „Reguły i alerty”, „Nowa reguła”,
- otworzy się nowe okno, w pierwszej jego części „Krok 1 – Wybierz szablon” proszę wybrać „Przenoszenie wiadomości zawierających określone wyrazy w temacie do folderu”,
- następnie przejdź dolnej części okna, w części „Krok 2 – Edytuj opis reguły” należy kliknąć na podświetlony na niebiesko tekst „określone słowa”,
- otworzy się kolejne okno, w które u góry należy pisać SPAM w kwadratowym nawiasie (czyli: [SPAM]) i kliknąć „dodaj”, a następnie zatwierdzić „OK”,
- teraz po powrocie do okna głównego proszę kliknąć w podświetlony na niebiesko tekst „wybierz folder” i przy zaznaczonej w lewej części otwartego właśnie okna folderze „Skrzynka odbiorcza” należy kliknąć z prawej strony „Nowy” i nazwać go np. SPAM zatwierdzając następnie „OK”.
- teraz wystarczy na dole kliknąć parę razy przycisk „dalej”, aż do momentu gdy pojawi się przycisk „zakończ”,
- należy kliknąć „zakończ”, a potem jeszcze zamknąć okno tworzenia reguł klikając „OK”