Problemy Twojej domeny z powtarzalnością poczty

Spis treści

1. Skrzynka pocztowa jest pełna
2. Zbyt duża wiadomość (Message exceeds size limit)
3. Nieznany użytkownik
4. Problemy z domeną
5. Wiadomości od systemów antyspamowych (SPAM)
6. Zła reputacja domeny (czarne listy)

1. Skrzynka pocztowa jest pełna

Najczęstszym problemem użytkowników jest pełna skrzynka pocztowa. Większość systemów ma limit ilości e-maili, które mogą przebywać na serwerze dla każdego użytkownika, a po osiągnięciu tego limitu nie ma miejsca na przyjmowanie nowej poczty przychodzącej. Oto wszystkie przykłady komunikatów o błędach poczty e-mail spowodowanych przez pełną skrzynkę pocztową (możliwe zwrotki od serwerów pocztowych):

*<user@example.com>: User is over the **quota**. You can try again later.*

<user@example.com>: host in7.example.com said:
552 <user@example.com>... Mailbox is full

Mailbox limit exceeded while appending message
550 <user@example.com>... Can't create output

<user@example.com>: host mail9.example.com said:
552 Requested mail action aborted: exceeded storage allocation

Ten błąd zniknie, gdy tylko odbiorca zrobi dodatkowe miejsce w swojej skrzynce pocztowej (zwykle poprzez usunięcie starych wiadomości z serwera), więc prawdopodobnie powinieneś wysłać wiadomość nieco później. Jeśli skrzynka należy do Twojej organizacji możesz zwiększyć jej pojemność w panelu hostingu.

2. Zbyt duża wiadomość (Message exceeds size limit)

Możliwe błędy (zwrotki z serwerów pocztowych) w dostarczeniu:

<user1@example.com>: host host.example.com said:
*552 Message size exceeds fixed **maximum message size** (5000000)*

<user@example.com>: host mx2.mail.example.com said:
*552 message size exceeds **maximum message size***

<user@example.com>: host mx01.example.com said:
*552 Message size exceeds fixed **maximum message size**: 5242880 bytes*

Błędy te oznaczają, że rozmiar wiadomości, w tym wszystkie nagłówki, tekst i załączniki, przekracza maksymalny limit rozmiaru wiadomości w domenie — zasadniczo oznacza to, że Twój e-mail jest zbyt duży, aby mógł zostać zaakceptowany. Powinieneś spróbować zmniejszyć rozmiar wiadomości lub spróbować podzielić wiadomość e-mail na mniejsze części i wysłać ją ponownie.

3. Nieznany użytkownik

Częstym problemem użytkownika jest oczywiście użytkownik nieznany. Konto, które próbujesz wysłać pocztą, już nie istnieje — mogło zostać zamknięte lub błędnie wpisano nazwę użytkownika lub domenę (upewnij się, że dokładnie sprawdzasz wiadomości o błędach w wiadomościach e-mail). Poniżej znajdują się wszystkie przykłady wiadomości o nieznanym użytkowniku (zwrotki od serwerów pocztowych):

<user@example.com>: host host.example.com said:
550 <user@example.com>... ***User unknown***

<user@example.com>: host mail7.example.com said:
550 Requested action not taken: ***mailbox unavailable***

<user@example.com>: host mail.example.com said:
550 5.1.1 <user@example.com> ***is not a valid mailbox***

<user@example.com>: Sorry, ***no mailbox here by that name****. (#5.1.1)*

<user@example.com>: host example.com said:
550 ***Invalid recipient*** *<user@example.com>*

The message that you sent was undeliverable to the following:
*user@example.com (****user not found****)*

Jeśli otrzymasz zwrotkę o nieznanym użytkowniku i sprawdziłeś, czy adres jest poprawny, następną rzeczą, którą powinieneś zrobić, to spróbować skontaktować się z osobą, do której próbujesz wysłać e-mail w inny sposób. Często ludzie nie zdają sobie sprawy, że odbijają e-maile, dopóki ktoś im nie powie. Nie usuwaj też otrzymanej zwrotki. Może pomóc użytkownikowi i jego dostawcy usług internetowych w ustaleniu, dlaczego odbija pocztę.

Jeśli nie masz innych możliwości skontaktowania się z osobą, która odbija pocztę, prawdopodobnie masz niedziałający adres e-mail. Spróbuj wysłać je jeszcze raz (najlepiej co najmniej dzień później), na wypadek gdyby był to problem techniczny, ale potem przestań używać tego adresu e-mail. Jeśli prowadzisz listę mailingową i jeden z Twoich subskrybentów zaczyna odbijać pocztę z tym błędem, usuń go z listy – możesz przez to trafić na czarną listę.

4. Problemy z domeną

W większości przypadków, gdy domena ma problem z pocztą e-mail, bardzo szybko dowiadujesz się o tym od swoich użytkowników, a ponadto stosunkowo rzadko zdarza się, że cała domena po prostu znika, więc większość błędów domeny należy uznać za tymczasowy problem i prawdopodobnie wkrótce zostanie naprawiony — ponowne wysłanie poczty nieco później jest zwykle najlepszą opcją.

Connection Timed Out / Connection Refused

<user@172.16.22.213>: connect to 172.16.22.213: ***Connection timed out***

Wiadomość „odrzucono połączenie” lub „przekroczono limit czasu połączenia” jest zwykle wynikiem przetwarzania dużej ilości poczty w momencie odebrania wiadomości. Może to być spowodowane tym, że serwer otrzymuje więcej poczty niż jest do tego przyzwyczajony, zewnętrzny atak na domenę lub problem z wewnętrzną konfiguracją, powodujący, że serwery pocztowe domeny odrzucają połączenia lub przerywają połączenia, zanim wiadomość zostanie w pełni wysłana. Usługi wymiany poczty są skonfigurowane tak, aby akceptować tylko tyle poczty, ile mogą obsłużyć, więc gdy problem zostanie rozwiązany, będziesz mógł bez problemu wysłać pocztę.

Domain Not Found

<sheabu@domain.com>: Name service error for domain domain.com:
Host not found*, try again*

Błąd „nie znaleziono domeny” oznacza, że nazwa domeny, do której wysłałeś wiadomość, nie istnieje. Zwykle oznacza to błędną pisownię nazwy domeny, ale może to wskazywać na problem z rekordem domeny, który uniemożliwia jej znalezienie.

Relay Access Denied

Innym błędem domeny, który może być spowodowany domeną nadawcy lub adresata, jest błąd odmowy dostępu do przekaźnika:

<receipient@example.com> host wormwood.example.com said:
554 <receipient@example.com>: Recipient Address rejected:
Relay access denied

Ten błąd wskazuje, że w jakiś sposób wiadomość przeznaczona na adres np. Yahoo.com trafiła na nasz serwer pocztowy example.com, a ponieważ nasz serwer nie akceptuje poczty z yahoo.com, wiadomość została odrzucona. W rzeczywistości dość rzadko zdarza się, aby podczas wysyłania wiadomości e-mail do domeny dotrzeć do całkowicie nieprawidłowego serwera pocztowego, więc jeśli otrzymasz tę wiadomość, problem jest zwykle błędem konfiguracji domeny odbierającej (na przykład, jeśli otrzymasz powiadomienie, że wiadomość została wysłana do użytkownika A został odrzucony przez serwer pocztowy A z błędem „Odrzucono adres odbiorcy", może to wskazywać na problem z serwerami pocztowymi, ponieważ serwery pocztowe A oczywiście powinny akceptować wiadomości e-mail od użytkowników A.

Innym powodem otrzymania tego błędu jest możliwość, że domena niedawno zmieniła hosta i chociaż zmiana miała miejsce, nowy rekord domeny nie został jeszcze w pełni rozpowszechniony, a Twoja wiadomość dotarła do starej firmy hostingowej, która nie akceptuje już poczty dla starej domeny. Jeśli pojawi się ten błąd, spróbuj ponownie wysłać wiadomość dwadzieścia cztery godziny później.

5. Wiadomości od systemów antyspamowych (SPAM)

Administratorzy systemu często konfigurują swoje systemy tak, aby odrzucały pocztę od spamerów, ale ponieważ żaden system filtrowania spamu nie jest doskonały, Twoja wiadomość mogła zostać zablokowana w powodu spamu. Niektóre z najczęstszych:

Spam blocks

<user@example.com>: host ntserver.example.com refused to talk to me:
550 Permission denied

albo bardziej kreatywna odpowiedź:

<user@domain.net>:
connect to domain.net: 550 Connection refused - we hate spammers!

Błędy te oznaczają, że nazwa domeny Twojego dostawcy (a konkretnie Twój adres e-mail) jest wyraźnie wymieniona jako znany spamer na czarnej liście. Może to być oparte na zewnętrznej usłudze, która udostępnia czarne listy znanych spamerów dostawcom usług internetowych, lub administrator może zablokować dużą ilość poczty przychodzącej z Twojej domeny. W większości przypadków dostawca poczty e-mail będzie musiał skontaktować się z administratorem systemu, aby usunąć blokadę, więc powinieneś natychmiast skontaktować się z dostawcą. Zakładając, że Twój dostawca w rzeczywistości nie jest usługą spamującą, będą chcieli działać szybko, aby usunąć się z tych czarnych list. W większości wypadków jednak nieświadomi użytkownicy sami rozsyłają spam, czy to z newsletterów czy z innych systemów, co w konsekwencji prowadzi do obniżenia „zaufania" do ich domeny, a co za tym idzie do cyklicznego trafiania na czarne listy. Bez edukacji użytkowników i zmiany ich zachowania problem będzie powracał i się nasilał.

Istnieją dwa inne komunikaty o błędach antyspamowych, które są bardzo podobne do niektórych błędów domeny przedstawionych powyżej. Pierwszy to błąd „domain not found", w którym nie można znaleźć domeny nadawcy:

<recipient@example.com>:host img10.ppi.net said: 554
<user@fake_domain.com>: Sender Address Rejected: domain not found

W przeciwieństwie do błędu „Domain Not Found" pokazanego powyżej jako błąd domeny, jest to odrzucenie antyspamowe. Zwróć uwagę na „Sender Address Rejected" - oznacza to, że problem dotyczy w rzeczywistości adresu e-mail nadawcy – a konkretnie, że domena użyta w adresie e-mail nadawcy nie była prawidłową domeną. Gdy serwer pocztowy otrzymuje wiadomość e-mail od jednego ze swoich użytkowników, serwer sprawdza, czy domena nadawcy jest prawdziwą domeną — jeśli nazwa domeny nie zostanie rozwiązana, wiadomość zostanie odrzucona z błędem „Sender Address Rejected". Jest to błąd antyspamowy, ponieważ uniemożliwia serwerom pocztowym przyjmowanie spamu w przypadku, gdy domena jest całkowicie fałszywa, co oznacza, że wiadomość nie mogła z niej pochodzić bo po prostu np. nie istnieje.

Innym rodzajem błędu „554 Relay Access Denied” jest problem z nadawcą używającym niewłaściwego serwera pocztowego do wysłania wiadomości:

<sender@example.com> host smtp-gw-4.example.com said:
554 <sender@example.com>: Sender Address rejected:
Relay access denied

Zasadniczo ten komunikat o błędzie jest podobny do odrzuconego adresu odbiorcy, ponieważ serwer zgłaszający błąd „nie lubi” nazwy domeny. Jednak w tym przypadku problem polega na tym, że serwer poczty wychodzącej „nie polubił” domeny adresu e-mail nadawcy (w przeciwieństwie do powyższych błędów odbiorcy, gdzie serwer poczty przychodzącej nie lubi domeny odbiorcy).

Ten błąd ogólnie wskazuje, że używany serwer poczty wychodzącej (zazwyczaj ten przypisany do Ciebie przez dostawcę usług internetowych) nie akceptuje wiadomości e-mail z adresem Od: podanym w wiadomości e-mail.

Pierwszą rzeczą, którą powinieneś zrobić, to zweryfikować ustawienia poczty e-mail u swojego dostawcy poczty e-mail. Upewnij się, że masz prawidłowy serwer pocztowy, nazwę użytkownika i hasło. Sprawdź również, czy musisz używać uwierzytelniania SMTP, czy też musisz używać protokołu POP przed SMTP.

Jeśli korzystasz z protokołu POP przed SMTP, możesz napotkać sporadyczne problemy z urządzeniami mobilnymi. Jest to spowodowane zmianą sieci danych z powodu słabego zasięgu lub zmianą jednego hotspotu Wi-Fi na inny. To, co się dzieje, to fakt, że Twój adres IP może się zmieniać, więc teraz wysyłasz e-maile z nowego adresu IP zamiast adresu IP, za pomocą którego pierwotnie uwierzytelniono. Aby temu zapobiec, możesz spróbować przełączyć się na uwierzytelnianie SMTP, aby sprawdzić, czy Twój dostawca poczty e-mail również ma to włączone. Jeśli to się nie powiedzie, może być konieczne skontaktowanie się z dostawcą poczty e-mail i poproszenie go o włączenie uwierzytelniania SMTP na serwerze pocztowym.

Wreszcie, na serwerze odbiorcy mogą pojawić się filtry antyspamowe. W takim przypadku powinieneś poprosić swojego dostawcę poczty e-mail o przejrzenie plików dziennika serwerów pocztowych, aby uzyskać więcej informacji o tym, jak temu zapobiec.

6. Zła reputacja domeny (czarne listy)

Przykładowe wiadomości zwrotne informujące o złej reputacji domeny:

550 Mail from <IP adress> refused by rbl-plus.mail-abuse.org.
Please refer to http://mail-abuse.org/rbl+ for an explanation

550 Mail from <IP adress> refused by rbl-plus.mail-abuse.org.
Please refer to http://mail-abuse.com/rbl for an explanation

550 Service unavailable; Client host [<IP adress>] blocked using Trend Micro RBL+.
Please see http://www.mail-abuse.com/cgi-bin/lookup?ip_address=<IP adress>

<rr@xxx.xx>: host mail.xxx.xx[xxx.xxx.xxx.xxx] said:
550-delivery from xxx.xxx.xxx.xxx is rejected. Check at
*550-**http://www.cyren.com/security-center/ip-reputation-check.** Reference 550*
code:tid=0001.0A782F96.60C30021.001E (in reply to RCPT TO command)

Jeśli występuje jeden z powyższych komunikatów to prawdodpodobnie adres IP Twojej poczty trafił na czarne listy antyspamowe. Sprawdź w panelu hostingu jaki adres IP wykorzystywany jest do rozsyłki poczty. Będzie on występował w formacie np. xxx.xxx.xxx.xxx

Gdy już posiadasz wspomniany adres, wpisz go na stronie:

https://mxtoolbox.com/blacklists.aspx

Otrzymasz listę serwerów antyspamowych i jeśli wśród nich widzisz czerwoną ikoną z krzyżykiem to znajdujesz się na tej czarnej liście. Kolejnym krokiem będzie usunięcie z czarnej listy Twojego adresu IP.

Najpopularniejsze czarne listy:

http://www.sorbs.net/ - należy założyć konto na adres e-mail, który wykorzystuje ów adres IP, o którym mówiono wyżej. Po założeniu konta należy wykorzystać zakładkę „delisting” i dalej postępować wg instrukcji. Po około 48h Twój adres IP powinien zostać wykluczony z czarnej listy.

https://check.spamhaus.org/ - wpisujemy nasz adres IP i jeśli wykryto jakieś problemy należy postępować wg dalszych instrukcji.

1. Dowiedz się, dlaczego Twój adres IP znajduje się na liście zablokowanych. (Przeczytaj o przyczynie na stronie wyników)
2. Wypełnij formularz usunięcia czarnej listy Spamhaus.
3. Sprawdź po 24h czy nastąpiło usunięcie z czarnej listy.

Przykładowy komunikat:

Jan 30 14:07:36 psa001 postfix/smtpd[31677]: NOQUEUE: reject: RCPT from unknown[185.143.223.97]: 554 5.7.1 Service unavailable; Client host [185.143.223.97] blocked using zen.spamhaus.org; https://www.spamhaus.org/sbl/query/SBL420772 / https://www.spamhaus.org/sbl/query/SBL442610; from=<spammer@spam.com> to=<someone@somewhere.com> proto=ESMTP helo= <[185.143.223.160]>

Dokładny błąd w odrzuceniu wiadomości e-mail różni się, ponieważ serwer odbiorcy może ustawić niestandardowe wiadomości, ale zwykle zobaczysz odniesienie do witryny http://www.spamhaus.org lub wzmiankę o konkretnej liście, zwykle zen.spamhaus.org .

Aby potwierdzić, że Twój adres IP znajduje się na liście zablokowanych, musisz przeprowadzić kontrolę czarnej listy Spamhaus.

BARRACUDA - https://www.barracudacentral.org/lookups/lookup-reputation

Aby zażądać korekty reputacji adresu IP

(https://www.barracudacentral.org/rbl/removal-request) w Systemie Barracuda, wprowadź poniżej adres IP serwera poczty e-mail, adres e-mail, numer telefonu i wiadomość potwierdzającą usunięcie problemu, który był powodem blokady. Należy pamiętać, że BRBL jest generowany przez zautomatyzowane systemy. Żądania bez prawidłowych informacji będą ignorowane. Prośby o usunięcie są zazwyczaj badane i przetwarzane w ciągu 12 godzin od przesłania, jeśli zostaną przesłane prawidłowe wyjaśnienie.

Co ciekawsze, większość innych czarnych list bazuje na systemie Barracuda, co oznacza, że usunięcie adres IP z tej listy spowoduje kaskadowe usunięcie z innych, podrzędnych czarnych list.

Jak zmniejszyć ryzyko trafienia na czarną listę e-maili

Monitorowanie reputacji jest kluczem do maksymalnej dostarczalności wiadomości e-mail. Ściśle monitorując liczbę czarnych list, możesz zapobiec awariom zanim się pojawią. Sprawdź swoją reputacje przy każdym wdrożeniu kampanii i monitoruj spadki dostarczalności i niskie wskaźniki zaangażowania.

Musisz również wiedzieć, w jaki sposób dodajesz nowych subskrybentów do swojej listy e-mailowej, aby upewnić się, że nie padniesz ofiarą pułapek spamowych. Jest kilka rzeczy, które możesz zrobić, aby ich uniknąć:

1. Potwierdzona akceptacja: Przed dodaniem nowego adresu odbiorcy do aktywnych list mailingowych wyślij wiadomość e-mail z potwierdzeniem. Użytkownik w ten sposób musi kliknąć w link potwierdzający – roboty tego nie zrobią.
2. Weryfikacja adresu w czasie rzeczywistym: Sprawdź adresy e-mail w momencie rejestracji pod kątem ważności i typowych literówek.
3. Nie wysyłaj w treści mejla linków do niezweryfikowanych stron. Ogranicz pobieranie zasobów zewnętrznych takich jak obrazki. Linki w treści wiadomości powinny być widoczne i łatwe do zrozumienia. Odbiorcy powinni wiedzieć, dokąd trafią po kliknięciu linku.
4. Nie podszywaj się pod inne domeny ani innego nadawcę bez pozwolenia. Mogłoby to spowodować, że Gmail oznaczałby wiadomości jako spam.
5. Opublikuj rekord SPF dla swojej domeny. SPF uniemożliwia spamerom wysyłanie nieautoryzowanych wiadomości, które wyglądają tak, jakby pochodziły z Twojej domeny.
6. Włącz podpisywanie DKIM swoich wiadomości. Serwery odbierające używają DKIM do sprawdzania, czy właściciel domeny rzeczywiście wysłał wiadomość. Ważne: Gmail wymaga 1024-bitowego lub dłuższego klucza DKIM.
7. Opublikuj rekord DMARC dla swojej domeny. DMARC pomaga nadawcom chronić swoją domenę przed podszywaniem się pod nich w e-mailach.
8. Nie korzystaj ze słów zawierających ciągi znaków jak „eval”, „base”, „post”, „virus” etc.
9. Daj odbiorcom możliwość anulowania subskrypcji Twoich wiadomości i zadbaj o to, aby było to łatwe. Umożliwienie użytkownikom rezygnacji z e-maili od Ciebie może poprawić współczynnik otwarć wiadomości, współczynnik klikalności i efektywność wysyłania.

Jeśli potrzebujesz pomocy w konfiguracji domeny skontaktuj się z nami.