sare

Dlaczego SMS-y trafiają do spamu?

Praktyczny poradnik bezpiecznych kampanii mobilnych

Spis treści:

1. Dlaczego SMS-y trafiają do spamu? 3
2. SMS a bezpieczeństwo komunikacji w Polsce 4
3. Najważniejsza zasada: rozdziel marketing i transakcje 4
    Nasza rekomendacja: 5
4. Jak SARE wspiera separację ruchu SMS? 5
    Cel: 6
5. Linki w SMS-ach: nie mieszaj domen między kanałami 6
    Dobre praktyki 6
    Skracacz linków w SARE 6
6. Dlaczego SMS-y są oznaczane jako spam? 7
7. Budowanie dobrego ruchu: edukuj odbiorców 7
    Przykład komunikatu 8
8. Higiena treści: drobne błędy, duże znaczenie 8
9. Kody autoryzacyjne: prostota działa na korzyść 9
10. Co zrobić, gdy nadawca został oznaczony jako spam? 9
    Rekomendowane działania 10
11. Zgłoszenie do zewnętrznych baz reputacyjnych, np. Hiya 10
12. SMS-y binarne jako opcja dla aplikacji mobilnej 11
13. A może RCS? 11
14. Checklista przed wysyłką SMS 12
15. Najważniejsze zasady w skrócie 12
16. Podsumowanie 13

Źródła i dodatkowe materiały 13

.

Praktyczny przewodnik po bezpiecznej i skutecznej komunikacji SMS

SMS pozostaje jednym z najskuteczniejszych kanałów kontaktu z odbiorcą. Jest szybki, bezpośredni i dobrze sprawdza się zarówno w komunikacji marketingowej, jak i transakcyjnej: przy kodach autoryzacyjnych, przypomnieniach, potwierdzeniach, alertach bezpieczeństwa czy komunikatach operacyjnych.

Jednocześnie SMS jest dziś kanałem coraz mocniej chronionym przed nadużyciami, phishingiem i smishingiem. Wiadomości są oceniane nie tylko przez odbiorców, ale także przez aplikacje wiadomości, systemy antyspamowe, operatorów oraz mechanizmy wynikające z przepisów i wzorców CSIRT NASK / CERT Polska.

Dlatego skuteczna komunikacja SMS wymaga czegoś więcej niż poprawnie napisanej treści. Liczy się reputacja nadawcy, historia wysyłek, typ komunikacji, linki, domeny, tempo kampanii, jakość bazy i reakcje odbiorców.

W SARE traktujemy SMS jako element bezpiecznej komunikacji cyfrowej — taki, który powinien być odpowiednio zaprojektowany, monitorowany i optymalizowany.

1. Dlaczego SMS-y trafiają do spamu?

SMS może zostać oznaczony jako spam na kilku poziomach. Wiadomość może trafić do folderu spam w aplikacji odbiorcy, zostać opatrzona ostrzeżeniem, mieć obniżoną reputację nadawcy albo — w skrajnych przypadkach — **zostać zablokowana na poziomie operatora lub systemu filtrującego**.

Na klasyfikację SMS-a wpływają m.in.:

- zgłoszenia użytkowników,
- automatyczna ocena aplikacji SMS i systemów antyspamowych,
- historia wcześniejszych kampanii,
- dotychczasowa reputacja nadawcy,
- nazwa nadawcy,
- treść wiadomości,
- linki i domeny użyte w SMS-ie,
- tempo i skala wysyłki,
- jakość bazy numerów,
- podobieństwo treści do znanych wzorców spamu lub smishingu.

W praktyce nawet legalna i oczekiwana wiadomość może zostać oceniona negatywnie, jeśli z perspektywy filtrów wygląda podobnie do ruchu niechcianego lub podejrzanego.

2. SMS a bezpieczeństwo komunikacji w Polsce

W Polsce bezpieczeństwo komunikacji SMS jest częścią systemu przeciwdziałania nadużyciom w komunikacji elektronicznej. CSIRT NASK / CERT Polska **tworzy wzorce wiadomości smishingowych**, a przedsiębiorcy telekomunikacyjni są zobowiązani do blokowania SMS-ów zgodnych z takimi wzorcami.

Oznacza to, że na ocenę wiadomości wpływa nie tylko sam nadawca. Znaczenie mają także treść, linki, układ komunikatu, kontekst wysyłki i podobieństwo SMS-a do schematów wykorzystywanych przez oszustów.

W praktyce SMS może być oceniany na kilku poziomach: **przez mechanizmy wynikające z przepisów i wzorców CSIRT NASK, przez systemy antyspamowe operatorów i aplikacji wiadomości, a także przez dodatkowe reguły bezpieczeństwa** stosowane przez dostawców technologii wysyłkowych.

Wniosek:
SMS powinien być projektowany tak, aby był jednoznaczny, przewidywalny i łatwy do odróżnienia od komunikacji podejrzanej.

3. Najważniejsza zasada: rozdziel marketing i transakcje

Jednym z kluczowych elementów ochrony reputacji SMS jest separacja ruchu. Komunikacja marketingowa i komunikacja transakcyjna lub autoryzacyjna **nie powinny wychodzić z tego samego nadawcy ani korzystać z tych samych domen**.

To szczególnie ważne w przypadku wiadomości krytycznych, takich jak:

- kody autoryzacyjne,
- logowanie,
- reset hasła,
- potwierdzenie operacji,
- alerty bezpieczeństwa,
- komunikaty transakcyjne.

Jeżeli Twoja marka używa tego samego nadpisu SMS zarówno do treści marketingowych, jak i transakcyjnych, negatywne reakcje na kampanie promocyjne mogą wpływać na ocenę całego nadawcy. W efekcie problem może dotknąć również wiadomości krytycznych, które odbiorca faktycznie chce i musi otrzymać.

Nasza rekomendacja:

Twórz oddzielne nadpisy dla różnych typów komunikacji, np.:

- osobny nadpis dla komunikacji transakcyjnej i autoryzacyjnej,
- osobny nadpis dla kampanii marketingowych,
- dodatkowe nadpisy dla innych, wyraźnie odrębnych scenariuszy komunikacji.

Takie rozdzielenie **może oznaczać, że dane z różnych typów komunikacji nie będą prezentowane w jednym, wspólnym raporcie nadawcy**. To jednak świadomy kompromis na rzecz bezpieczeństwa, dostarczalności i stabilności komunikacji krytycznej.

Oddzielne nadpisy pomagają ograniczyć ryzyko przenoszenia negatywnej reputacji z kampanii marketingowych na wiadomości transakcyjne.

4. Jak SARE wspiera separację ruchu SMS?

W SARE rozdzielenie komunikacji może działać nie tylko na poziomie samego nadpisu. W zależności od konfiguracji możliwe jest także oddzielenie ruchu marketingowego i transakcyjnego lub autoryzacyjnego na poziomie technicznej obsługi wysyłek.

Może to obejmować m.in.:

- osobne konta,
- osobne ścieżki obsługi ruchu,
- różne priorytety wysyłki,
- oddzielną konfigurację dla komunikacji krytycznej.

Dzięki temu wiadomości autoryzacyjne, takie jak kody logowania czy potwierdzenia operacji, **mogą być obsługiwane niezależnie od masowych kampanii marketingowych** — również w okresach zwiększonego wolumenu wysyłek, np. podczas Black Friday.

Cel:

komunikacja krytyczna nie powinna być obciążona reputacją, tempem ani wolumenem kampanii marketingowych.

5. Linki w SMS-ach: nie mieszaj domen między kanałami

Drugim elementem separacji są linki. Komunikacja marketingowa i transakcyjna nie powinny używać tych samych domen ani tych samych skracaczy.

Jeżeli w SMS-ach marketingowych używana jest domena kampanijna, promocyjna lub trackingowa, **nie powinna ona pojawiać się w SMS-ach autoryzacyjnych**. Filtry analizują nie tylko treść wiadomości, ale także reputację linków. Jeśli domena była wcześniej używana w kampaniach masowych lub często zgłaszanych jako niechciane, może to wpłynąć na ocenę kolejnych wiadomości z tą samą domeną.

Dobre praktyki

- Unikaj popularnych, publicznych skracaczy linków typu bit.ly.
- Korzystaj z własnej domeny lub subdomeny.
- Dla komunikacji autoryzacyjnej stosuj oddzielną domenę.
- Nie używaj tych samych linków w marketingu i transakcjach.
- Dbaj o pełny, wiarygodny adres URL.
- Stosuj HTTPS.
- Nie ukrywaj celu linku.

Skracacz linków w SARE

W systemie SARE możesz korzystać ze skracacza linków działającego w oparciu o oddelegowaną subdomenę klienta. Oznacza to, że link w wiadomości SMS nie opiera się na przypadkowej, publicznej domenie skracacza, ale na domenie powiązanej z Twoją marką.

Dzięki temu komunikacja wygląda **bardziej wiarygodnie dla odbiorcy, a jednocześnie ogranicza ryzyko negatywnych skojarzeń z publicznymi skracaczami wykorzystywanymi często w masowych lub podejrzanych wiadomościach**.

Dla komunikacji marketingowej skracacz SARE może dodatkowo wspierać raportowanie kliknięć i analizę skuteczności kampanii. W przypadku wiadomości autoryzacyjnych lub transakcyjnych rekomendujemy jednak stosowanie osobnej domeny lub subdomeny, aby nie mieszać reputacji ruchu marketingowego z komunikacją krytyczną.

6. Dlaczego SMS-y są oznaczane jako spam?

Klasyfikacja SMS-a jako spam nie zawsze wynika wyłącznie z ręcznej reakcji odbiorcy. Użytkownik może oznaczyć wiadomość jako spam w aplikacji SMS, w systemie operacyjnym, w aplikacji operatora lub narzędziu antyspamowym, ale część wiadomości może być również automatycznie oznaczana jako podejrzana.

Telefony, aplikacje wiadomości i systemy antyspamowe mogą analizować m.in.:

- treść SMS-a,
- linki,
- reputację nadawcy,
- historię wcześniejszych wysyłek,
- tempo kampanii,
- podobieństwo do wzorców spamu i smishingu.

Czasem użytkownik oznacza wiadomość jako spam, bo faktycznie jest niechciana. Czasem dlatego, że nie rozpoznaje nadawcy. A czasem dlatego, że nie spodziewał się SMS-a od danej marki.

Niezależnie od źródła oznaczenia — ręcznego lub automatycznego — każda negatywna klasyfikacja może wpływać na reputację nadawcy i skuteczność kolejnych wysyłek.

7. Budowanie dobrego ruchu: edukuj odbiorców

Reputacja nadawcy nie buduje się wyłącznie po stronie systemów technicznych. **Wpływają na nią również reakcje odbiorców.**

Jeżeli prowadzisz ważne kampanie SMS — zwłaszcza do własnych pracowników, partnerów, klientów lub użytkowników aplikacji — warto wcześniej poinformować ich innym kanałem, że mogą otrzymać wiadomość SMS.

Może to być:

- komunikat e-mailowy,
- powiadomienie w aplikacji,
- informacja w panelu klienta,
- komunikat wewnętrzny,
- informacja w procesie obsługi klienta.

Celem jest przygotowanie odbiorcy na wiadomość i zwiększenie jej rozpoznawalności.

Przykład komunikatu

*W najbliższych dniach możesz otrzymać od nas wiadomość SMS dotyczącą [**cel komunikacji**]. Wiadomość zostanie wysłana z nadawcy [**nazwa nadawcy**]. Jeżeli korzystasz z aplikacji, która klasyfikuje SMS-y, możesz oznaczyć tę wiadomość jako zaufaną, aby w przyszłości łatwiej otrzymywać ważne komunikaty.*

Nie chodzi o sztuczne „oszukiwanie" filtrów, ale o budowanie naturalnego, pozytywnego kontekstu komunikacji. Jeżeli odbiorca wie, że SMS jest oczekiwany i pochodzi od właściwej marki, rzadziej oznaczy go jako spam.

8. Higiena treści: drobne błędy, duże znaczenie

Treść SMS-a powinna być prosta, naturalna i technicznie poprawna. W przypadku filtrów antyspamowych znaczenie mają nawet drobne szczegóły.

Unikaj

- nadmiaru wielkich liter,
- wielu wykrzykników,
- agresywnych zwrotów typu „kliknij teraz", „wygraj", „odbierz natychmiast",
- niejasnych skrótów,
- przypadkowych znaków specjalnych,
- zbitek tekstu, które mogą zostać rozpoznane jako link.

Szczególnie ważne są kropki i ciągi znaków. Jeżeli w treści pojawi się zbitka typu:

Sprawdź szczegóły.Twój kod

Wtedy telefon lub aplikacja może błędnie zinterpretować fragment jako element linku albo podejrzany ciąg znaków.

Lepsza wersja:

> Sprawdź szczegóły. Twój kod

W wiadomościach autoryzacyjnych najlepiej sprawdzają się proste treści z kodem, bez zbędnych dodatków. Sam numer kodu, krótki kontekst i informacja, aby nikomu go nie udostępniać, są zwykle lepsze niż rozbudowany komunikat.

Przykład:

> Twój kod logowania do [nazwa]: 482913. Nie udostępniaj go nikomu.

9. Kody autoryzacyjne: prostota działa na korzyść

Wiadomości z kodami jednorazowymi **powinny być maksymalnie przewidywalne**. Dla użytkownika to komunikacja techniczna, a nie marketingowa. Nie warto dodawać do niej treści promocyjnych, linków sprzedażowych ani elementów zachęcających do kliknięcia.

Dobra wiadomość OTP powinna zawierać:

- nazwę marki lub usługi,
- kod,
- krótki cel wiadomości,
- ostrzeżenie, aby nie udostępniać kodu,
- brak elementów marketingowych,
- brak przypadkowych linków.

Nie rekomendujemy łączenia kodu autoryzacyjnego z komunikatem sprzedażowym. To dwa różne typy komunikacji, które powinny mieć osobne nadpisy, osobne domeny i osobną logikę wysyłki.

10. Co zrobić, gdy nadawca został oznaczony jako spam?

Jeżeli problem już wystąpił, pierwszym krokiem powinna być diagnoza. Warto sprawdzić:

- którego nadawcy dotyczy problem,
- czy problem występuje przy SMS-ach marketingowych, transakcyjnych czy obu,
- u których operatorów pojawia się klasyfikacja spamowa,
- na jakich systemach i aplikacjach występuje problem,
- czy wiadomości zawierają linki,
- czy marketing i autoryzacja korzystają z tego samego nadawcy lub domeny,
- czy baza zawiera nieaktywne lub błędne numery,
- czy kampanie były wysyłane nagle, masowo i bez stopniowania wolumenu.

Dopiero po takiej analizie można dobrać działania naprawcze.

Rekomendowane działania

- Rozdzielenie nadpisów dla marketingu i autoryzacji.
- Wydzielenie osobnych domen dla różnych typów komunikacji.
- Poprawa treści.
- Ograniczenie linków.
- Wdrożenie throttlingu, czyli rozłożenia wysyłki w czasie.
- Higiena bazy numerów.
- Dodanie łatwej rezygnacji z komunikacji marketingowej.
- Edukacja odbiorców innymi kanałami.
- Testy dostarczalności.
- Analiza raportów i reakcji odbiorców.

System SARE wspiera realizację komunikacji SMS i RCS, raportowanie wysyłek oraz analizę danych, co pozwala lepiej monitorować skuteczność kampanii i optymalizować kolejne działania.

11. Zgłoszenie do zewnętrznych baz reputacyjnych, np. Hiya

W przypadku błędnych oznaczeń jako spam **warto rozważyć zgłoszenie problemu bezpośrednio do dostawcy klasyfikacji lub reputacji**, np. Hiya.

Takie zgłoszenie powinno zostać wysłane przez właściciela marki, ponieważ to on najlepiej może potwierdzić charakter swojej komunikacji, wskazać przykłady wiadomości oraz wyjaśnić, że są to komunikaty oczekiwane przez odbiorców — np. autoryzacyjne, transakcyjne lub informacyjne.

Hiya udostępnia formularz kontaktowy, przez który można zgłosić nieprawidłowe oznaczenie nadawcy lub wiadomości jako spam.

W zgłoszeniu warto opisać:

- kim jest nadawca,
- jakiego nadpisu lub numeru dotyczy problem,
- jaki charakter ma komunikacja,
- czy są to wiadomości krytyczne, transakcyjne lub autoryzacyjne,
- kiedy problem wystąpił,
- przykładową treść wiadomości,
- skalę problemu,
- informację, że odbiorcy oczekują tej komunikacji.

Z doświadczenia rynkowego wynika, że zgłoszenie wykonane bezpośrednio przez właściciela marki może być skuteczniejsze niż zgłoszenie wykonane przez pośrednika, np. przez SARE. **Dostawca technologii może pomóc przygotować argumentację i dane, ale to Twoja marka jako nadawca najlepiej potwierdza charakter własnej komunikacji**.

12. SMS-y binarne jako opcja dla aplikacji mobilnej

W wybranych scenariuszach, szczególnie przy autoryzacji w aplikacji mobilnej, można rozważyć wdrożenie SMS-ów binarnych. To rozwiązanie techniczne, które umożliwia automatyczne przekazanie kodu do aplikacji i ogranicza konieczność ręcznego przepisywania go przez użytkownika.

W tym poradniku traktujemy SMS-y binarne informacyjnie — jako możliwą ścieżkę dla firm, które posiadają własną aplikację mobilną i prowadzą procesy autoryzacyjne.

Nie jest to rozwiązanie dla każdej organizacji ani zamiennik higieny reputacji nadawcy. Może być jednak kierunkiem wartym analizy tam, gdzie kluczowe jest szybkie i wygodne przekazanie kodu do aplikacji. Koszt pojedynczego SMS-a binarnego może być taki sam jak koszt standardowego SMS-a, natomiast samo **wdrożenie wymaga dodatkowej analizy technicznej po stronie aplikacji i procesu bezpieczeństwa**.

13. A może RCS?

RCS może być alternatywą lub uzupełnieniem komunikacji SMS. To kanał oparty na innej technologii niż SMS, dlatego bezpośrednie reguły blokady SMS nie przenoszą się automatycznie na RCS.

Nadawcy RCS przechodzą proces weryfikacji, a wiadomości mogą zawierać elementy multimedialne, przyciski akcji i bardziej rozbudowaną identyfikację marki.

Nie oznacza to jednak, że RCS jest całkowicie wolny od ryzyka. Odbiorcy nadal mogą oznaczać konwersacje jako spam, a reputacja marki pozostaje ważna. RCS daje jednak większą kontrolę nad

prezentacją nadawcy i może zwiększać zaufanie odbiorców, zwłaszcza w komunikacji, w której ważne są czytelność, branding i interakcja.

W systemie SARE moduł RCS umożliwia realizację kampanii do numerów GSM posiadających aktywną obsługę RCS, a wiadomości mogą przyjmować bogatsze formaty, takie jak karuzele, odnośniki czy video.

14. Checklista przed wysyłką SMS

Przed uruchomieniem kampanii sprawdź:

- ☐ Czy komunikacja marketingowa i transakcyjna są rozdzielone?
- ☐ Czy używasz osobnych nadpisów dla różnych typów komunikacji?
- ☐ Czy wiadomości autoryzacyjne nie korzystają z tych samych domen co marketing?
- ☐ Czy linki są wiarygodne i prowadzą do domeny powiązanej z marką?
- ☐ Czy unikasz publicznych skracaczy linków typu bit.ly?
- ☐ Czy treść SMS-a jest prosta, jasna i pozbawiona agresywnych zwrotów?
- ☐ Czy nie używasz nadmiaru wielkich liter, wykrzykników i znaków specjalnych?
- ☐ Czy po kropkach i znakach interpunkcyjnych zachowane są spacje?
- ☐ Czy wiadomości OTP nie zawierają treści marketingowych?
- ☐ Czy baza numerów jest aktualna i zgodna z udzielonymi zgodami?
- ☐ Czy duża wysyłka jest rozłożona w czasie?
- ☐ Czy odbiorcy wiedzą, że mogą otrzymać SMS od Twojej marki?
- ☐ Czy monitorujesz raporty i reakcje odbiorców?
- ☐ Czy masz plan działania na wypadek oznaczenia nadawcy jako spam?

15. Najważniejsze zasady w skrócie

- ➔ Rozdzielaj treści marketingowe, autoryzacyjne i transakcyjne.
- ➔ Używaj osobnych nadpisów dla różnych typów komunikacji.
- ➔ Nie stosuj tych samych domen w marketingu i wiadomościach transakcyjnych.
- ➔ Unikaj popularnych skracaczy linków.
- ➔ Korzystaj z własnej domeny lub subdomeny.
- ➔ Pisz prosto, naturalnie i bez agresywnych zwrotów.
- ➔ Nie dodawaj treści promocyjnych do kodów autoryzacyjnych.
- ➔ Dbaj o higienę bazy numerów.
- ➔ Rozkładaj duże wysyłki w czasie.
- ➔ Edukuj odbiorców innymi kanałami.

- ➔ Monitoruj raporty i reakcje użytkowników.
- ➔ W razie problemów zgłaszaj błędne oznaczenia do właściwych dostawców reputacji.
- ➔ Dla aplikacji mobilnych rozważ dodatkowe rozwiązania wspierające autoryzację.
- ➔ Przy bardziej angażujących scenariuszach rozważ RCS.

16. Podsumowanie

SMS nie jest już prostym kanałem masowej wysyłki. To element ekosystemu bezpieczeństwa, w którym znaczenie mają reputacja, zaufanie, jakość treści i techniczna separacja ruchu.

Odpowiedzialna komunikacja SMS powinna łączyć skuteczność marketingową z zasadami bezpieczeństwa. Separacja ruchu, higiena treści, wiarygodne domeny, rozpoznawalny nadawca i stałe monitorowanie reakcji odbiorców pomagają ograniczać ryzyko błędnej klasyfikacji jako spam.

W SARE wspieramy naszych Partnerów w projektowaniu komunikacji, która nie tylko dociera do odbiorców, ale także buduje zaufanie: przez odpowiednią konfigurację nadawców, pracę na wiarygodnych domenach, raportowanie, segmentację i dobór właściwego kanału — SMS, RCS lub komunikacji omnichannel.

Źródła i dodatkowe materiały

CERT Polska: Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej
https://cert.pl/posts/2023/09/uznke/

NASK: Groźne SMS-y będą blokowane — jak działa blokowanie na podstawie wzorców tworzonych przez CERT Polska
https://www.nask.pl/aktualnosci/grozne-sms-y-beda-blokowane-jak-czy-nasza-prywatnosc-zostanie-naruszona-o-tym-takze-na-secure-2024

Ministerstwo Cyfryzacji: Nowe zabezpieczenia przed niechcianymi SMS-ami
https://www.gov.pl/web/cyfryzacja/nowe-zabezpieczenia-przed-niechcianymi-smsami

CERT Polska / CSIRT NASK: zgłaszanie podejrzanych SMS-ów na numer 8080
https://www.gov.pl/web/baza-wiedzy/dostales-niepokojacy-sms-albo-email-zglos-go-do-cert-polska-csirt-nask

UKE: Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej
https://www.uke.gov.pl/akt/ustawa-o-zwalczaniu-naduzyc-w-komunikacji-elektronicznej%2C500.html

Hiya: formularz zgłoszeniowy
https://hiyahelp.zendesk.com/hc/en-us/requests/new?ticket_form_id=824667

Naszym priorytetem jest bezpieczna komunikacja cyfrowa.

Potrzebujesz więcej informacji?

Skontaktuj się z nami!

kontakt@sare.pl | sare.pl

Wydawca:

Digitree Group SA
Raciborska 35A
44-200 Rybnik