

ZAŁĄCZNIK NR 1 DO OPZ

Brief do kampanii społecznej na temat cyberbezpieczeństwa

1. Zadanie

Przygotowanie **strategii mediowej** oraz świadczenie kompleksowej obsługi w zakresie **planowania oraz zakupu czasu antenowego i powierzchni reklamowej w mediach** na potrzeby emisji kampanii społecznej na temat cyberbezpieczeństwa.

2. Kim jesteśmy

NASK to Państwowy Instytut Badawczy, który zajmuje się bezpieczeństwem w sieci. To my, ponad 30 lat temu podłączyliśmy Polskę do Internetu. Teraz, prowadzimy badania naukowe i rozwijamy nowe technologie, które zwiększają poziom cyberbezpieczeństwa. Stale monitorujemy sieć i reagujemy na zgłaszane incydenty. Nasi eksperci angażują się w działalność edukacyjną, szkoleniową i popularyzatorską. Chcemy budować nowoczesne i dobrze funkcjonujące społeczeństwo informacyjne!

3. Dlaczego to robimy

W NASK mamy odwagę mówić głośno o problemach i podejmować tematy, które są trudne i niewygodne. Chcemy przemówić do ludzkiej wyobraźni. Wywołać dyskusję społeczną wokół dwóch istotnych zagrożeń w sieci – oszustw internetowych i uzależnień od mediów społecznościowych, szczególnie wśród młodych.

Nie robimy kampanii wizerunkowej, nie chcemy też sprzedawać kolejnego produktu, dzięki któremu nasze życie będzie wygodniejsze czy bardziej kolorowe. **Mamy niepowtarzalną szansę realnie wpłynąć na społeczeństwo, stworzyć wyjątkowy i ważny przekaz, który zapoczątkuje zmianę postaw i zachowań.** A przede wszystkim pomoże ochronić każdego z nas przed szkodliwymi i często nieodwracalnymi skutkami niebezpieczeństw w sieci.

Chcemy inspirować do podejmowania lepszych decyzji i zmiany złych nawyków. Wierzymy, że odpowiednio dobrane słowa w połączeniu z wyrazistym obrazem mogą zapoczątkować tę zmianę. To inwestycja w lepszą przyszłość naszą i naszych dzieci.

Bezpieczny Internet to nie tylko nasz cel, ale i odpowiedzialność społeczna nas wszystkich.

4. Problem

Nasze obserwacje i analizy dot. cyberprzestrzeni pozwoliły nam określić dwa główne obszary/problemy społeczne związane z bezpieczeństwem w sieci. Skala i rozmiar tych zagrożeń jest niepokojąca, dlatego tak istotne jest prowadzenie wysokozasięgowych akcji komunikacyjnych.

- 1) Pierwszy obszar stanowią **zagrożenia i oszustwa w Internecie**. Przestępcy wykorzystują różne formy manipulacji, aby nakłonić potencjalne ofiary do popełnienia błędów lub przekazania wrażliwych czy tajnych informacji. Bazują na tym samym mechanizmie. Celem jest wykorzystanie ludzkiego błędu lub nieprzemyślanego zachowania i uzyskanie dostępu do informacji lub usług. Najczęściej występujące rodzaje oszustw to: phishing, oszustwa na fałszywe sklepy, kradzieże tożsamości/ podszywanie się, wycieki danych, kradzieże pieniędzy, złośliwe oprogramowanie, fałszywe inwestycje, deepfake.
- 2) Drugim problemem są **zagrożenia i uzależnienia od Internetu i mediów społecznościowych wśród dzieci i młodzieży**. Wyniki badań pokazują, że rodzice nie mają świadomości, ile czasu ich dzieci przebywają w świecie cyfrowym.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NASK

Dlatego tak ważne i potrzebne są kampanie społeczne budujące świadomość celem jest wsparcie rodziców w dbaniu o bezpieczeństwo swoich dzieci w sieci.

Dane i badania pokazujące skalę problemu

Materiały źródłowe:

- 1) [Raport roczny z działalności CERT Polska 2023](#) – publikacja podsumowująca działalność zespołu ds. reagowania na incydenty komputerowe, zawiera analizy i statystyki dotyczące cyberzagrożeń, incydentów oraz działań prewencyjnych prowadzonych w ciągu roku.
Główne wnioski:
 - Rok do roku CERT Polska rejestruje coraz większą liczbę incydentów. W 2023 roku wpłynęło ponad 371 tys. zgłoszeń. W stosunku do roku ubiegłego odnotowano ponad stu procentowy przyrost.
 - Najpopularniejszym typem incydentów zarejestrowanych w 2023 r. były, tak jak niezmiennie od wielu lat, strony phishingowe. Zarejestrowano 41 tys. tego typu incydenty, co stanowi aż 51 proc. wszystkich obsługiwanych incydentów. To wzrost o ponad 61 pkt. proc. w porównaniu do roku ubiegłego. Najpopularniejszymi kampaniami phishingowymi były m.in. wykorzystujące wizerunek serwisu aukcyjnego Allegro – 11 161 przypadków, serwisu społecznościowego Facebook – 5 308 przypadków i serwisu sprzedażowego OLX – 4 753 przypadki.
 - Innym popularnym typem incydentów były oszustwa komputerowe. Zarejestrowano ich ponad 34 tys., co stanowi ponad 42 proc. wszystkich zarejestrowanych incydentów. Są to m.in. fałszywe sklepy internetowe oraz popularne w ubiegłym roku oszustwa finansowe, w których przestępcy podszywają się pod koncerny paliwowo-energetyczne, firmy oraz instytucje.
- 2) Badanie „[Nastolatki 3.0](#)” zrealizowane przez Thinkstat, zespół badania opinii działający w NASK. Główne wnioski:
 - Nastolatki korzystają z internetu średnio 5 godzin i 36 minut w dni powszednie. W weekendy to aż 6 godzin i 16 minut. Z roku na rok ten czas się wydłuża, w poprzedniej edycji badania, które jest realizowane co dwa lata, średni czas bycia online wynosił 4 godziny 50 minut dziennie.
 - Większość nastolatków deklaruje, że rodzice nie ustalają z nimi żadnych zasad korzystania z internetu, a jednocześnie niemal 60% rodziców deklaruje, że takie zasady ustala. Ta wysoka rozbieżność danych może wskazywać na niską świadomość rodziców dotyczącą tego, co ich dzieci oglądają, słuchają, czytają w sieci.

5. Cele kampanii

W ramach zadania oczekujemy pomysłu na kampanie społeczne we wskazanych już wyżej dwóch obszarach. Ich głównym celem jest zwiększenie świadomości na temat bezpiecznego korzystania z Internetu, umiejętności rozpoznawania zagrożeń oraz właściwej reakcji na nie.

Każda z kampanii ma dodatkowo określony swój cel szczegółowy oraz charakter.

1) Noga 1 – kampania o zagrożeniach i oszustwach internetowych

Ta kampania powinna być efektywna i skuteczna. W prosty i zrozumiały sposób powinna poruszać problem zagrożeń związanych z oszustwami w sieci, do których można zaliczyć m.in. wyłudzenie danych, kradzież tożsamości czy pieniędzy i dezinformację (bazującą na socjotechnice i inżynierii społecznej).



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NASK

Celem komunikacji jest:

- budować świadomość w zakresie podstawowych zasad bezpiecznego korzystania z narzędzi internetowych,
- uczyć w zakresie umiejętności rozpoznawania cyberzagrożeń,
- dostarczać informacji o skutecznych metodach obrony przed atakami w internecie – wskazówki, jak reagować i chronić się przed zagrożeniami,
- zachęcać użytkowników do zgłaszania podejrzanych aktywności lub incydentów do odpowiednich organów zajmujących się cyberbezpieczeństwem.

2) Noga 2 – kampania o uzależnieniach od Internetu i mediów społecznościowych

Ta kampania powinna być wyrazista i mocna, może być kontrowersyjna. Kampania powinna bazować na emocjach, w nieoczywisty i zaskakujący sposób podejmować problem zagrożeń związanych z uzależnieniem od Internetu i mediów społecznościowych wśród dzieci i młodzieży.

Celem komunikacji jest:

- zwiększanie świadomości wśród rodziców i opiekunów na temat zagrożeń jakie niesie ze sobą regularne korzystanie z mediów społecznościowych,
- zwiększenie świadomości wśród rodziców i opiekunów na temat tego, że media społecznościowe uzależniają.

6. Grupy docelowe

1) Noga 1 – kampania o zagrożeniach i oszustwach internetowych

- Grupa ogólna all – ogół społeczeństwa polskiego – przekaz dot. wszystkich najpopularniejszych cyberzagrożeń, które mogą być kierowane do każdego, bez względu na płeć, wiek, zachowanie itp. (z uwzględnieniem all 15+ , osób o niższych kompetencjach cyfrowych lub wykluczonych cyfrowo, a będących potencjalnymi ofiarami zagrożeń oraz osób starszych (kobiety i mężczyźni w wieku 60+).

3) Noga 2 – kampania o uzależnieniach od Internetu i mediów społecznościowych

- Grupa ogólna all – ogół społeczeństwa polskiego (z uwzględnieniem rodziców i opiekunów (dzieci od lat 7 do 18) – przekaz dot. zagrożeń, które dotyczą dzieci i młodzieży.

7. Kluczowe przekazy

1) Noga 1 – kampania o zagrożeniach i oszustwach internetowych

- Główny przekaz kampanii to: komunikacja dotycząca zagrożeń masowych, skierowana do osób starszych i wykluczonych (+ ogół społeczeństwa).
- Take-out konsumencki: korzystanie z internetu może wiązać się z zagrożeniami, jednak wiem, jak się chronić i postępować w sytuacji zagrożenia, bo większa świadomość i wiedza nt. działań oszustów to większe nasze bezpieczeństwo w sieci.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NASK

2) Noga 2 – kampania o uzależnieniach od Internetu i mediów społecznościowych

- Główny przekaz kampanii to komunikacja związana z bezpieczeństwem dzieci w sieci, kierowana głównie do rodziców i opiekunów.
- Take out konsumencki: Social media uzależniają, nie pozwól swojemu dziecku zrobić sobie krzywdę.

8. Pożądany efekt działań (oczekiwane korzyści)

Wzrost świadomości na temat cyberzagrożeń oraz zasad jak się chronić.

1) Noga 1 – kampania o zagrożeniach i oszustwach internetowych

Zmiana postaw i zachowań w kierunku bardziej bezpiecznego korzystania z internetu (m.in. zwiększenie używania silnych haseł, unikanie klikania w podejrzane linki, czy regularne aktualizacje oprogramowania).

2) Noga 2 – kampania o uzależnieniach od Internetu i mediów społecznościowych

Większa świadomość rodziców i znajomość narzędzi, jak wspierać dzieci i młodzież (podopiecznych), aby potrafiły świadomie poruszać się w internecie i wystrzegać cyberzagrożeń, zmniejszenie czasu spędzanego przez dzieci w internecie.

9. Wskaźniki efektywności kampanii (cele mediowe)

- 1) Dotarcie z kampanią radiowo-telewizyjną do grupy docelowej „all”, ogół społeczeństwa, min. 26 mln osób.
- 2) Liczba wejść na landing page kampanii: 7 mln.

10. Planowane media

1) Noga 1 – kampania o zagrożeniach i oszustwach internetowych

Telewizja, Radio, OOH/DOOH, Internet, prasa, inne

2) Noga 2 – kampania o uzależnieniach od Internetu i mediów społecznościowych

Telewizja, Radio, OOH/DOOH, ambient, internet, inne

11. Terminy kampanii

- 1) Rozpoczęcie realizacji zamówienia – po podpisaniu umowy (początek IV kwartału 2024).
- 2) Prace strategiczno-koncepcyjne, w tym: planowanie strategii medialnej oraz media planów, produkcja materiałów reklamowych przez Wykonawcę (agencję kreatywną wybraną w odrębnym przetargu) – start: IV kwartał 2024, bieżąca współpraca na przestrzeni całego 2025 roku.
- 3) Emisja kampanii – start: I kwartał 2025, kontynuacja do końca 2025 roku na zgodnie ze strategią i zaakceptowanymi media planami.
- 4) Kontynuacja kampanii w latach 2026-2027. Możliwość skorzystania przez Zamawiającego z zamówienia, o którym mowa w pkt XI SOPZ tj. Zamówienie polegające na powtórzeniu podobnych usług.

12. Dodatkowe informacje

- 1) Nadawcą komunikacji, podmiotem odpowiedzialnym za realizację kampanii jest Instytut, który działa na rzecz bezpieczeństwa w sieci. Niska świadomość marki NASK wymusza poszukiwanie innowacyjnych rozwiązań (nie chcemy zginąć w tle telekomów i FMCG), zależy nam na autorskim podejściu Wykonawcy w tworzeniu media mixu. Do rozważenia – skupienie na mniejszej ilości mediów, ale z większą częstotliwością/intensywnością.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



NASK