

WEBINARIUM AKADEMII ODPORNOŚCI

Bezpieczeństwo cyfrowe i dezinformacja

PROWADZĄCY

Zapowiedz dwie części: najpierw oszustwa i bezpieczeństwo kont, potem dezinformacja w lokalnej społeczności. Na końcu, jak zawsze, co z tego da się wpisać do wniosku. Karta pracy do webinarium jest na mms.klaster.org.pl/materialy. Wklej ten adres na czat, zanim zaczniesz.

DO ODCZYTANIA NA POCZĄTKU

Zadanie publiczne Wielka Moc Małych Społeczności, Odporne Śląskie 2026 sfinansowane jest ze środków Narodowego Instytutu Wolności – Centrum Rozwoju Społeczeństwa Obywatelskiego w ramach Rządowego Programu wsparcia organizacji pozarządowych Moc Małych Społeczności.

Wniosek nr 97594, Priorytet 2. Zadanie finansowane ze środków budżetu państwa. Wydarzenia są apartyjne. Nie promujemy partii politycznych ani ich programów, nie prowadzimy agitacji wyborczej.

PROWADZĄCY Przeczytaj na głos, zanim puścisz pierwszy merytoryczny slajd. Obowiązek z § 20 ust. 5 regulaminu. Nagranie zostaje na stronie, więc ten slajd musi być w nagraniu.

260 783

tyle incydentów zarejestrował CERT Polska w 2025 roku

O 152 procent więcej niż rok wcześniej.

Ponad 1 800 zgłoszeń dziennie.

PROWADZĄCY

Źródło: Raport Roczny 2025 CERT Polska i komunikat NASK. Zgłoszeń było 658 320, po weryfikacji zostało 260 783 incydentów, czyli ponad 700 dziennie.

97%

z nich to oszustwa komputerowe

W tym phishing i inne sposoby wyłudzenia danych.

PROWADZĄCY To najważniejsza liczba spotkania. Organizacji nie atakują hakerzy z filmów. Ktoś klika w link z fałszywej wiadomości.

140 mln

prób wejścia na fałszywe strony zablokowano w 2025 roku

Tyle zatrzymała Lista Ostrzeżeń CERT Polska.

PROWADZĄCY Od 2020 roku na listę trafiło ponad pół miliona domen, z tego blisko 250 tysięcy w 2025 roku. Dzięki współpracy z operatorami dostęp do tych stron jest blokowany, dlatego zgłaszanie fałszywych stron ma sens.

Pod kogo podszywają się oszuści

- Banki i firmy kurierskie
- Usługi publiczne, na przykład Profil Zaufany
- Znane osoby w fałszywych reklamach inwestycji
- Wnuczek, policjant albo znajomy proszący o BLIK

PROWADZĄCY

Pierwsze dwa punkty podaje NASK przy Liście Ostrzeżeń. Trzeci to obserwacja CERT Polska: filmy i zdjęcia typu deep fake stały się stałym elementem fałszywych inwestycji. Czwarty to znany schemat oszustw na seniorach.

Co może stracić mała organizacja

- Fanpage, który budowała latami, razem z obserwującymi
- Skrzynkę mailową, a z nią dostęp do innych kont
- Pieniądze ze zbiórki albo z rachunku stowarzyszenia
- Wiarygodność, gdy z jej konta pójdzie fałszywa prośba o wpłatę

PROWADZĄCY Zapytaj na czacie, czy komuś to się już przydarzyło. Kilka takich historii robi więcej niż statystyka.

Cyberprzestępczość

Przestępcy mogą przejąć Twoje dane, podszyć się pod Ciebie w sieci, wziąć w Twoim imieniu pożyczkę lub oszukać Twoich znajomych.

- Dostałeś podejrzaną wiadomość z linkiem lub załącznikiem?
Nie klikaj pochopnie.
- **Sprawdź adresy** nadawców i treść wiadomości. Błędy lub brak polskich znaków mogą sygnalizować oszustwo.
- **Chroń dane** logowania i numery na kartach płatniczych.
- **Regularnie aktualizuj** program antywirusowy i aplikacje na komputerze oraz w telefonie.
- Korzystaj tylko z **legalnego oprogramowania**.
- Nie instaluj aplikacji z niesprawdzonych źródeł.
- **Ustaw silne hasła**, np. używając menedżera haseł.
- Korzystaj z **weryfikacji dwuetapowej** (SMS, e-mail).
- **Rób kopie zapasowe** ważnych plików i dokumentów.
- **Zachowaj ostrożność**, kiedy korzystasz z publicznych sieci Wi-Fi.

Próbę wyłudzenia lub oszustwa zgłoś na stronie
incydent.cert.pl lub przez aplikację [mObywatel](https://mObywatel.pl).

Podejrzane SMS-y z linkami prześlij pod numer **8080**.

Cyberprzestępczość według poradnika

Poradnik Bezpieczeństwa MSWiA, wydanie 2025, strona 40

PROWADZĄCY

Lista z poradnika. Zatrzymaj się na weryfikacji dwuetapowej i kopiach zapasowych, bo te dwie rzeczy pozwalają odzyskać konto i dokumenty po włamaniu.

Po czym poznać fałszywą wiadomość

- Link albo załącznik, którego się nie spodziewasz
- Dziwny adres nadawcy
- Błędy i brak polskich znaków
- Pośpiech: zapłać, bo stracisz konto albo przesyłkę
- Prośba o dane logowania albo numer karty

PROWADZĄCY Trzy pierwsze sygnały są wprost w poradniku na stronie 40. Pośpiech to ulubione narzędzie oszustów, dlatego pierwsza rada poradnika brzmi: nie klikaj pochopnie.

SMS: dopłacić 1,50 zł, bo paczka wróci do nadawcy. Co robisz?

- A Klikam link i dopłacam, bo kwota jest mała
- B Przesyłam SMS na 8080 i kasuję wiadomość**
- C Dzwonię pod numer podany w SMS-ie

B. Podejrzany SMS przesyła się na numer 8080, a próbę oszustwa zgłasza na incydent.cert.pl albo w aplikacji mObywatel. Mała kwota to właśnie ten pośpiech, na który liczy oszust.

PROWADZĄCY Zapytaj na czacie, komu przyszedł taki SMS w ostatnim miesiącu. Przy odpowiedzi C dodaj, że numer w wiadomości prowadzi do oszusta, a numer do banku bierze się z własnej karty albo ze strony banku.

Pięć rzeczy do zrobienia w tym tygodniu

- 1 Menedżer haseł i osobne hasło do każdego konta
- 2 Weryfikacja dwuetapowa na mailu, w banku i na fanpage'u
- 3 Kopia zapasowa dokumentów poza jednym komputerem
- 4 Aktualizacje systemu i aplikacji na telefonach zarządu
- 5 Przegląd, kto ma dostęp do fanpage'a i skrzynki

PROWADZĄCY Ostatni punkt: dostęp bywa zostawiony osobom, które dawno odeszły z organizacji. To nic nie kosztuje, a zamyka otwarte drzwi.

Gdy ktoś przejął konto

- 1 Zmień hasło z innego, bezpiecznego urządzenia
- 2 Włącz weryfikację dwuetapową
- 3 Przy danych karty zadzwoń do banku
- 4 Zgłoś incydent na incydent.cert.pl
- 5 Uprzedź obserwujących o możliwych fałszywych wiadomościach

PROWADZĄCY Kolejność ma znaczenie: najpierw odzyskanie kontroli, potem zgłoszenie i ostrzeżenie innych. Ostatni punkt chroni wiarygodność organizacji.



Podejrzany SMS prześlij na 8080.

Próbę oszustwa zgłoś na incydent.cert.pl
albo w aplikacji mObywatel.

PROWADZĄCY W 2025 roku do analizy trafiło w ten sposób przeszło 350 tysięcy SMS-ów, a ponad 80 tysięcy uznano za szkodliwe.
Na podstawie wzorców CERT Polska zablokowano dostarczenie blisko 1,88 miliona złośliwych wiadomości.

Dla organizacji ze stroną internetową

- moje.cert.pl: bezpłatne monitorowanie bezpieczeństwa strony
- wiedza.cert.pl: wiedza CERT Polska dla organizacji
- Kopia zapasowa strony i aktualizacje wtyczek

PROWADZĄCY Z moje.cert.pl korzysta ponad 18 500 użytkowników, serwis monitoruje ponad 20 tysięcy stron. Serwis wiedza.cert.pl NASK uruchomił we wrześniu 2026 roku.

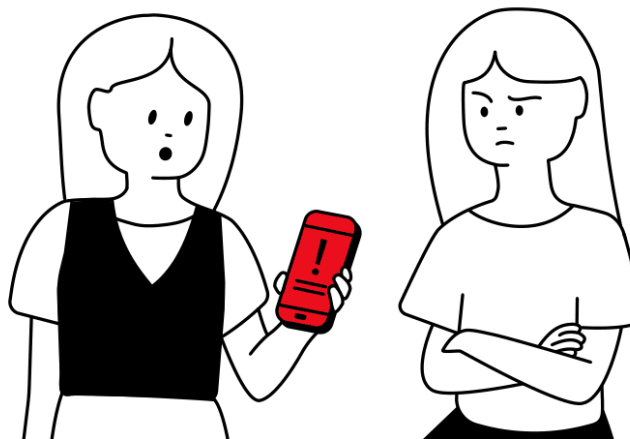
Dezinformacja to celowe rozpowszechnianie fałszywych lub zmanipulowanych treści.

PROWADZĄCY Słowo celowe jest tu ważne. Sąsiad, który podaje dalej plotkę, zwykle nie działa celowo, i z nim rozmawia się inaczej niż z kontem, które zalewa lokalną grupę tymi samymi wpisami.

Sprawdzaj w pewnych źródłach

Poradnik Bezpieczeństwa MSWiA, wydanie 2025, strona 39

Wszystkie informacje sprawdzaj w pewnych, publicznych źródłach informacji, takich jak Polskie Radio, Telewizja Polska, rządowe strony internetowe i służby państwowe.



PROWADZĄCY Przeczytaj zdanie z poradnika na głos. Wśród pewnych źródeł poradnik wymienia Polskie Radio, Telewizję Polską, rządowe strony internetowe i służby państwowe.

Czego nie robić w kryzysie

PORADNIK MSWiA, STRONY 38 I 39

- Nie udostępniaj zdjęć i filmów z miejsca zdarzenia
- Nie rozpowszechniaj niesprawdzonych informacji
- Nie wierz w doniesienia o upadku państwa i kapitulacji
- Nie publikuj zdjęć wojska, mostów ani stacji kolejowych

PROWADZĄCY Zdjęcia z miejsca zdarzenia i przerobione komunikaty łatwo rozchodzą się w lokalnych grupach. Organizacja może być miejscem, gdzie ludzie wiedzą, czego nie podawać dalej.

Jak nie powielać

- 1 Zatrzymaj się, zanim klikniesz Udostępnij
- 2 Sprawdź, kto to napisał i kiedy
- 3 Poszukaj tej samej informacji w dwóch innych źródłach
- 4 Jeśli nie wiesz, nie podawaj dalej

PROWADZĄCY Cztery kroki, które mieszczą się na lodówce. Dobry materiał na ulotkę w mikroprojekcie.

Jak przeciwdziałać w gminie

NIE DZIAŁA

**Kłótnia pod postem
i wyzywanie od trolli.**

DZIAŁA

**Krótki, spokojny wpis
z konkretem i źródłem,
podpisany przez osobę,
której ludzie ufają.**

PROWADZĄCY W małej miejscowości sołtys, strażak z OSP albo nauczycielka mają często więcej zaufania niż odległa instytucja.

Spokojne sprostowanie w trzech zdaniach



Co wiemy

Tylko to, co wiemy na pewno.



Skąd wiemy

Z podaniem źródła, na przykład urzędu gminy.



Co robić teraz

Jedno konkretne zdanie, co ludzie mają zrobić.

PROWADZĄCY

Przykład: Woda w wodociągu jest zdatna do picia. Tak podał dziś urząd gminy na swojej stronie.
Jeśli coś się zmieni, gmina wyda komunikat. Pisanie takich wpisów to gotowy temat warsztatu.

Gdzie sprawdzać

- Rządowe strony internetowe i strona urzędu gminy
- Alerty RCB i aplikacja Regionalnego Systemu Ostrzegania
- Komunikaty służb, w tym straży pożarnej i policji
- Polskie Radio i Telewizja Polska, które wskazuje poradnik

PROWADZĄCY Poradnik na stronie 53 opisuje RSO jako bezpłatną aplikację, która informuje o zagrożeniach. Alert RCB przychodzi SMS-em sam, bez zapisów.

Pięć obszarów, lista zamknięta

§ 6 UST. 3 REGULAMINU



Pierwsza pomoc i AED

pierwsza pomoc i obsługa
automatycznego
defibrylatora zewnętrznego



Kłęski i blackout

kłęski żywiołowe oraz długotrwała
przerwa w dostawie prądu



Bezpieczeństwo cyfrowe

bezpieczeństwo cyfrowe,
dezinformacja i oszustwa



Sieci sąsiedzkie

sieci sąsiedzkie i wolontariat spontaniczny



Służby i OSP

współpraca ze służbami
oraz z jednostkami
ochotniczych straży pożarnych

PROWADZĄCY

Bezpieczeństwo cyfrowe, dezinformacja i oszustwa to trzeci obszar. Zwróć uwagę na słowo oszustwa: warsztat dla seniorów o fałszywych telefonach mieści się w kompetencjach.

Kryterium 1: o co zapyta ekspert

KARTA OCENY MERYTORYCZNEJ, ZAŁĄCZNIK NR 3

- Czy odbiorcy są określani i wiadomo, dlaczego właśnie oni?
- Czy uczestnicy realnie ćwiczą umiejętność, a nie tylko o niej słuchają?

PROWADZĄCY Dwa pytania z kryterium pierwszego. Pierwsze dotyczy odbiorców: warsztat dla seniorów trzeba uzasadnić. Drugie dotyczy ćwiczeń: w tym obszarze łatwo o wykład, a uczestnicy mogą na przykład ustawić weryfikację dwuetapową na własnym telefonie.

Co z tego robi mikroprojekt

- Spotkania dla seniorów o fałszywym wnuczku, banku i kurierze
- Godzina z telefonem: razem ustawiamy weryfikację dwuetapową
- Ulotka z czterema krokami przed udostępnieniem
- Szkolenie zarządów lokalnych organizacji z bezpieczeństwa kont
- Grupa osób, które wiedzą, gdzie sprawdzić informację w kryzysie

PROWADZĄCY Wszystkie mają policzalny rezultat: liczba osób, liczba telefonów z ustawionym zabezpieczeniem, liczba rozdanych ulotek.

Zadanie na dziś

- 1 Wypisz, kto ma dostęp do fanpage'a i maila organizacji
- 2 Usuń dostęp osobom, które już nie działają
- 3 Włącz weryfikację dwuetapową na skrzynce organizacji
- 4 Zapytaj trzy starsze osoby o podejrzone telefony

PROWADZĄCY Czwarty punkt to gotowa mini diagnoza. Jeżeli dwie z trzech osób powiedzą tak, masz argument do wniosku.



Czas na pytania z czatu.

Piszcie w okienku czatu, odpowiadamy po kolei.

PROWADZĄCY Według programu pytania trwają od 18:00 do 18:45. Przeczytaj pytanie na głos, zanim odpowiesz, bo nagranie nie pokazuje czatu. Pytania o konkretny wniosek odsyłaj na mentoring albo na infolinię.

Co dalej?

- Nagranie i slajdy: mms.klaster.org.pl/materialy
- Następne webinarium: piątek 25 września, sieci sąsiedzkie
- Asystent AI: przycisk na każdej stronie konkursu
- Mentoring indywidualny: zapytaj na infolinii albo mailem
- Infolinia 539 644 192, pon-pt 10:00 do 16:00

PROWADZĄCY Przypomnij numer 8080 i adres incydent.cert.pl jeszcze raz, to dwie rzeczy do wyniesienia z tego spotkania.

Nabór trwa do 6 października

WNIOSEK mms.klaster.org.pl/wniosek
NABÓR DO 6 października 2026, godz. 23:59
INFOLINIA 539 644 192, pon–pt 10:00 do 16:00
MAIL mms@klaster.org.pl



PROWADZĄCY Następne webinarium w piątek: sieci sąsiedzkie i wolontariat spontaniczny. Przypomnij o 6 października.