

# BĄDŹ GOTOWY I BEZPIECZNY

Przewodnik dla mieszkańców Zielonki na wypadek kryzysu

część III

## WOJNA, WOJNA HYBRYDOWA I CYBERPRZESTĘPCZOŚĆ

Konflikt zbrojny, dezinformacja i cyberataki. Jak ochronić siebie i bliskich?

Miasto Zielonka



Szanowni Państwo,  
Drodzy Mieszkańcy Zielonki

bezpieczeństwo coraz częściej ma dziś także wymiar, którego nie widać na pierwszy rzut oka. Oprócz zagrożeń związanych z pogodą czy infrastrukturą, obserwujemy zmiany w świecie - również w sferze geopolitycznej i informacyjnej. Pojęcia takie jak wojna, działania hybrydowe, cyberataki czy dezinformacja jeszcze niedawno brzmiały jak język analityków. Dziś coraz częściej pojawiają się w codziennych wiadomościach, a ich skutki mogą dotknąć każdego z nas.

Współczesne zagrożenia nie zawsze wyglądają „klasycznie”. Wojna nie musi oznaczać wyłącznie działań zbrojnych w oczywistej formie. Coraz częściej jest to także presja informacyjna, próby destabilizacji, cyberataki na infrastrukturę krytyczną i systemy usług publicznych, a także działania, których celem jest wywołanie chaosu i podważanie zaufania. Równolegle rośnie skala cyberprzestępczości, która dotyka obywateli bez względu na wiek czy doświadczenie, od fałszywych wiadomości i wyłudzeń, po przejęcia kont i kradzieże środków.

Samorząd ma obowiązek przygotowywać miasto na różne scenariusze i wspierać odporność społeczności lokalnej. Oznacza to współpracę ze służbami, rozwijanie procedur, inwestycje w rozwiązania wzmacniające bezpieczeństwo oraz rzetelną komunikację. Równie ważne jest jednak to, co każdy z nas może zrobić sam:

umieć weryfikować informacje, rozpoznawać manipulacje, chronić swoje dane, dokumenty i środki finansowe, a także zachować spokój w sytuacjach, w których łatwo o dezinformację i niepotrzebną panikę. W kryzysie liczy się czas, klarowna informacja i odpowiedzialne decyzje - także te podejmowane w domu, przy telefonie czy komputerze.

Oddajemy w Państwa ręce trzecią część cyklu „Bądź gotowy i bezpieczny”. W tej broszurze odpowiadamy na praktyczne pytania: jak rozpoznać dezinformację i nie stać się jej przekaźnikiem? Jak zabezpieczyć dane i pieniądze? Jak przygotować się na możliwe zakłócenia w funkcjonowaniu usług publicznych i infrastruktury? Jak reagować na komunikaty ostrzegawcze i gdzie szukać wiarygodnych informacji?

Ta publikacja - podobnie jak dwie poprzednie - jest elementem szerszych działań edukacyjnych miasta. Równolegle przygotowujemy szkolenia i działania informacyjne podczas wydarzeń miejskich, dostosowane do różnych grup wiekowych, w tym dzieci, dorosłych oraz seniorów. O kolejnych inicjatywach będziemy informować na stronie internetowej miasta oraz w naszych kanałach komunikacji.

Oby ta wiedza nigdy nie musiała się przydać - ale jeśli ewentualnie przyjdzie moment próby, warto być przygotowanym.

Kamil Michał Iwadowski  
Burmistrz Miasta Zielonka

## Najbliższe działania Miasta Zielonka w zakresie bezpieczeństwa



Dostarczymy mieszkańcom  
**trzy części Przewodnika**  
na czas kryzysu.



Zorganizujemy **szkolenia dla mieszkańców**  
i kadry zarządzającej, np. z pierwszej pomocy.



Zorganizujemy **spotkania z ekspertami**  
od bezpieczeństwa.



Będziemy regularnie  
**publikować treści edukacyjne**  
dotyczące ochrony ludności i obrony cywilnej.

### PAMIĘTAJ

Kryzys niejedno  
ma imię. Dlatego  
warto jest być  
przygotowanym na  
różne scenariusze.

Obowiązkiem każdego  
z nas jest zadbać o  
siebie, swoich bliskich  
i swój majątek.

W taki właśnie sposób  
zbudujemy odporność  
całego państwa.  
Każdy z nas jest za  
nie odpowiedzialny.

# WOJNA HYBRYDOWA



Prowadzenie regularnej wojny - z udziałem wojsk, lotnictwa i czołgów - kosztuje ogromne pieniądze i szybko przyciąga uwagę świata. Dlatego agresor coraz częściej sięga po metody mniej kosztowne i trudniejsze do wykrycia, które pozwalają wywierać presję na inne państwo bez formalnego wypowiedzenia wojny. Tak właśnie działa wojna hybrydowa - łączy różne metody, by osłabiać państwo, siać chaos i podkopywać zaufanie społeczne.

## Wojna hybrydowa może obejmować:

- **działania dezinformacyjne** (w mediach społecznościowych, na arenie międzynarodowej)
- **cyberataki** (na system bankowy lub wodociągi)
- **akty sabotażu** (np. podpalenia, podkładanie ładunków wybuchowych, niszczenie światłowodów z internetem na dnie Bałtyku)
- **wykorzystywanie nielegalnej imigracji** (przerzucanie migrantów z Bliskiego Wschodu przez granicę z Białorusią)
- **ataki terrorystyczne**

**Wojna hybrydowa zakłada długotrwałe, rozciągnięte w czasie działania.** Trudno je jednoznacznie udowodnić konkretnemu państwu - i na tym polega ich złowroga siła.

## WAŻNE!



**Przeciwko Polsce toczy się obecnie wojna hybrydowa prowadzona przez wrogie państwa.**

Jej celem jest osłabienie naszego kraju w maksymalny sposób, bez wypowiedzania otwartej wojny.





# DEZINFORMACJA - JAKIE SĄ JEJ CELE?



To **sianie zamętu w kraju, podważanie zaufania do instytucji publicznych, służb, wojska i pogłębianie podziałów społecznych.**

Często jest uruchamiana przy okazji innych wrogich działań (np. aktach sabotażu), aby wzmocnić ich efekt.

## KTO STOI ZA DEZINFORMACJĄ?

- **SŁUŻBY SPECJALNE** wrogich państw.
- **BOTY**, czyli programy internetowe, które są zaprogramowane na wykonywanie określonych zadań w internecie - np. do szerzenia obcej propagandy, obrażania innych użytkowników, pisanie nienawistnych treści. Są groźne, bo rozsiewają dezinformację na szeroką skalę. Robią to w sposób zautomatyzowany.
- **TROLLE**, czyli prawdziwi użytkownicy mediów społecznościowych lub osoby publiczne, które manipulują celowo lub aby wzbudzić zainteresowanie i zaistnieć medialnie.

### WAŻNE!



**Dezinformacja to celowe rozpowszechnianie** fałszywych lub wprowadzających w błąd informacji. Często jest używana w wojnie hybrydowej.

Kryzysy zdarzają się naprawdę...

## **AKCJA DEZINFORMACYJNA PO NARUSZENIU POLSKIEGO NIEBA PRZEZ ROSYJSKIE DRONY (2025)**

Wraz z wielokrotnym i celowym przekroczeniem polskiej przestrzeni powietrznej przez rosyjskie drony we wrześniu 2025 r. w przestrzeni internetowej miała miejsce akcja dezinformacyjna.

### **Jaki cel?**

Rosyjskie i białoruskie służby jeszcze przed incydem z dronami prowadziły wzmożone działania w mediach społecznościowych. Ich celem było zdyskredytowanie działań Wojska Polskiego i służb ("wojsko nie umie bronić polskiego nieba"), a także zrzuć odpowiedzialność za wlot dronów na stronę ukraińską ("Ukraińcy chcą wciągnąć Polskę do wojny"). Chodziło również o wywołanie napięć między Polakami a mieszkającymi w Polsce Ukraińcami.

### **W jaki sposób?**

Treści pojawiały się m. in. na Telegramie i "X" - na kontach o dużych zasięgach, używanych do upowszechniania rosyjskiej dezinformacji. Aktywowano te same konta, które w czasie pandemii COVID-19 były wykorzystywane do szerzenia narracji antyszczepionkowych.

# DEZINFORMACJA - JAK JĄ ROZPOZNAĆ?

## DEZINFORMACJA STOSUJE NAJCZĘŚCIEJ KILKA PROSTYCH TECHNIK:

- **CLICKBAIT** - sensacyjny tytuł lub nagłówek, który ma przyciągnąć uwagę i nakłonić do kliknięcia lub przeczytania.
- **JĘZYK EMOCJONALNY** - styl, który wywołuje silne emocje - strach, gniew, oburzenie.
- **DOWÓD ANEGDOTYCZNY** - podawanie jednej konkretnej historii, aby podważyć jakieś zjawisko poparte danymi statystycznymi czy badaniami naukowymi.
- **BRAK KONTEKSTU** - wybór informacji pasujących do tezy i pominięcie kluczowego kontekstu.
- **PODSZYWANIE SIĘ** - wykorzystanie czyjegoś autorytetu do szerzenia nieprawdy.
- **DEEPFAKE** - wygenerowane przez sztuczną inteligencję (AI) fałszywe wideo.

## PAMIĘTAJ!

**Widzisz treści dezinformujące w internecie?** Zgłoś je do NASK - państwowego instytutu badawczego, który zajmuje się cyberbezpieczeństwem i walką z dezinformacją.

[www.zglos-dezinformacje.nask.pl](http://www.zglos-dezinformacje.nask.pl)

## WAŻNE!

**Wiarygodne informacje o tym, co się dzieje w Zielonce znajdziesz:**

- na oficjalnej stronie miasta: [zielonka.pl](http://zielonka.pl)
- na Facebooku: [www.facebook.com/Zielonka.Miasto](https://www.facebook.com/Zielonka.Miasto)
- pod numerem telefonu: (22) 761 39 00

# DEZINFORMACJA - JAK SIĘ CHRONIĆ?



- Sprawdzaj źródła informacji. Krytycznie podchodź do wiadomości podawanych przez anonimowych internautów.
- Zwróć uwagę na to, czy informacja jest sensacyjna i napisana językiem emocjonalnym. Jeśli tak - wzmocnij czujność. To może być dezinformacja.
- Nie podawaj dalej niesprawdzonych informacji.
- Korzystaj z wiarygodnych źródeł informacji (strony rządowe, samorządowe, duże portale, telewizje i rozgłośnie radiowe).
- Sprawdzaj, czy kontrowersyjna lub podejrzana informacja pojawiła się w więcej niż w dwóch źródłach.
- Obserwuj w mediach społecznościowych kanały Policji, wojska, administracji państwowej i samorządowej. To podstawowe źródła informacji w przypadku kryzysu.

## WAŻNE!



**Receptą na dezinformację jest edukacja i weryfikacja informacji**

## PAMIĘTAJ!



W czasie kryzysu nie wierz w doniesienia o upadku państwa i jego kapitulacji. **To może być celowa wroga dezinformacja.**

# ZACHOWAJ CZUJNOŚĆ

## WIDZISZ NIETYPOWE ZACHOWANIE WOKÓŁ SIEBIE? REAGUJ!

Zwróć uwagę na osoby, które:



**oferują przez internet łatwy zarobek** (służby rosyjskie poszukują "jedenorazowych" współpracowników)



**próbują zdobyć informacje wrażliwe**, np. o planach budynków, danych osobowych, kwestiach bezpieczeństwa



**robią zdjęcia lub filmują (np. dronem)** tory kolejowe, węzły logistyczne, jednostki wojskowe, lotniska



**oznaczają skrzynki energetyczne lub telekomunikacyjne albo inne ważne obiekty**, np. taśmą, kredą, farbą

## WAŻNE!

Tego rodzaju nietypowe sytuacje zgłaszaj telefonicznie na Policję (112).

Służby przeanalizują zgłoszenie i podejmą adekwatne działania.

## PAMIĘTAJ!

W czasie poważnego kryzysu - nie wierz w doniesienia o upadku państwa i jego kapitulacji.

**To może być celowa wroga dezinformacja.**









# CYBERATAKI



**Cyberprzestępczość** to domena zarówno oszustów, którzy próbują ukraść pieniądze z konta lub cyfrową tożsamość, jak i obcych służb.

Te ostatnie atakują tzw. infrastrukturę krytyczną - informacyjną, finansową, związaną z energią elektryczną, wodociągami czy ochroną zdrowia. **Ataki mogą być kierowane także przeciwko każdemu z nas.**

Postęp technologiczny i rozwój sztucznej inteligencji (AI) sprawiają, że systemy zabezpieczeń przed cyberatakami są coraz doskonalsze. **W cyberprzestrzeni najsłabszym ogniwem są wciąż ludzie.**

To nasze błędy, pośpiech, nieuwaga czy klikanie w linki niewiadomego pochodzenia sprawiają, że cyberprzestępcom jest łatwiej.

## WAŻNE!



Cyberatak to próba włamania do systemu, sieci komputerowej, zbioru danych lub urządzenia elektronicznego, np. smartfona.

**Celem może być kradzież danych lub pieniędzy, przejęcie kontroli nad urządzeniem lub systemem czy też zakłócenie jego pracy.**

# CYBERATAKI

Cyberataki zdarzają się naprawdę...

## PAP “INFORMUJE” O CZĘŚCIOWEJ MOBILIZACJI DO WOJSKA (2024)

Przed wyborami do europarlamentu na stronach Polskiej Agencji Prasowej pojawiła się depesza, w której Premier polskiego rządu ogłasza częściową mobilizację do wojska i wysłanie żołnierzy do Ukrainy.

Artykuł był całkowicie nieprawdziwy, a został opublikowany wskutek cyberataku. Hakerzy otrzymali dostęp do panelu redakcyjnego, bo włamali się na konto jednego z pracowników. Według rządzących za atakiem stały wschodnie służby. Celem było wywołanie chaosu i podważenie wiarygodności PAP-u, czyli najważniejszej agencji prasowej w Polsce.

Cyberataki zdarzają się naprawdę...

## CYBERATAKI NA GMINNE WODOCIĄGI (2024 - 2025)

W ostatnim czasie polskie służby odnotowały próby włamania do systemów uzdatniania wody i oczyszczalni ścieków, m. in. w Wydminach, Kuźnicy, Tolkmicku, Jabłonnej Lackiej, Sierakowiu.

**Za cyberatakami stały grupy hakerskie powiązane z Federacją Rosyjską.** Ich celem jest testowanie zabezpieczeń. Tego typu ataki mogą w przyszłości być wykorzystane do zakłócenia dostaw wody lub paraliżu przepompowni ścieków.



# CYBERATAK - PHISHING



- **widzisz wiadomość z banku lub firmy kurierskiej**, która wywiera presję czasu i prosi o pilne działanie (np. przełanie pieniędzy, potwierdzenie danych, kliknięcie w link)
- **dostajesz wiadomość z informacją o wygranej** w konkursie lub od nieznanego nadawcy
- **widzisz sensacyjny post**, który wymaga od Ciebie potwierdzenia wieku (np. poprzez podanie numeru PESEL)
- **wiadomość zawiera błędy językowe** (treść może być generowana automatycznie)

## PAMIĘTAJ!



**Cyberatak to również bróń pospolitych oszustów internetowych.**

Jedną z najczęściej wybieranych przez nich metod jest phishing. Polega na podszywaniu się pod zaufane podmioty (banki, instytucje) lub firmy i wyłudzeniu poufnych informacji, np. danych osobowych, PIN-u, numeru BLIK lub numeru karty płatniczej.

## WAŻNE!



Jesteśmy atakowani przez te kanały, których na co dzień używamy, np. e-mail, SMS, rozmowy telefoniczne, reklamy w portalach, media społecznościowe.

**Oszuści liczą na naszą rutynę i obniżenie czujności.**  
**W 2023 roku w Polsce phishing stanowił aż 64% incydentów zgłoszonych do NASK.**

# CYBERATAK - PHISHING



Cyberataki zdarzają się naprawdę...



## JAK MOŻE WYGLĄDAĆ PHISHING KROK PO KROKU

- **Dostajesz sms lub e-mail** od "banku", "urzędu", "firmy kurierskiej".
- Wrzeczywistości to oszust, który **podszyswa się pod instytucję lub firmę**.
- Wiadomość zawiera link, który prowadzi **na fałszywą stronę**.
- Strona wymaga **podania danych osobowych** lub do logowania albo też - przesłania określonej kwoty.
- Gdy wpiszesz dane, oszust je przejmuje, **gdy zrobisz przelew - tracisz pieniądze**.

## PAMIĘTAJ!



W walce z phishingiem **Twoim sprzymierzeńcem jest czas**. Jeśli jakaś instytucja lub firma wymaga od Ciebie szybkiej reakcji (np. podania poufnych danych lub dopłaty do usługi), nie rób niczego pochopnie. Uważnie przeanalizuj treść wiadomości.





# CYBERATAK - PHISHING

Cyberataki zdarzają się naprawdę...

## JAK MOŻE WYGLĄDAĆ PHISHING KROK PO KROKU

- **Dzwoni do Ciebie "bank"** (lub "policja"). Na wyświetlaczu w telefonie widzisz nazwę swojego banku. W rzeczywistości to oszust.
- Podczas rozmowy **twierdzi, że Twoje pieniądze są zagrożone** lub ktoś wziął kredyt na Twoje dane.
- **Oszust twierdzi, że chce Ci pomóc** - odzyskać środki lub też uchronić je przed kradzieżą. Próbuje wzbudzić Twoje zaufanie.
- **Chce zdobyć Twoje dane**, dlatego próbuje przeprowadzić ich "weryfikację". Może wykorzystać je do wzięcia kredytu w Twoim imieniu.
- Może też namówić Cię do konkretnego działania - np. **do przelewu zagrożonych środków na "techniczny" rachunek bankowy** lub zainstalowania aplikacji, która w efekcie wykradnie pieniądze.

## PAMIĘTAJ!

Pracownik banku nie może prosić Cię o: podanie pełnych danych osobowych (PESEL, numer dowodu) czy loginu i hasła, zrobienie przelewu pieniędzy, podanie kodu SMS autoryzującego operację finansową, instalowanie aplikacji.

**Masz wątpliwość, z kim rozmawiasz? Rozłącz się i zadzwoń na infolinię Twojego banku, aby wyjaśnić sprawę.**

# CYBERATAK - PHISHING

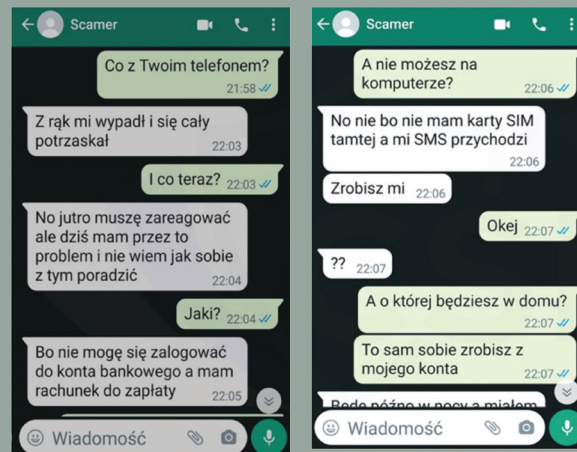
Cyberataki zdarzają się naprawdę...

## JAK MOŻE WYGLĄDAĆ PHISHING KROK PO KROKU

- Dostajesz SMS lub wiadomość na komunikatorze od obcego numeru. Oszust podaje się za Twojego bliskiego.
- Informuje Cię o utracie telefonu i - jeśli pisze SMS-a - często prosi o przeniesienie rozmowy na komunikator WhatsApp.
- W następnym kroku **prosi o wykonanie pilnego przelewu**.
- Rozmowa jest prowadzona w taki sposób, aby wywołać u Ciebie **silne emocje i presję czasu**.

## PAMIĘTAJ!

Jeśli dostajesz wiadomość z obcego numeru, od kogoś, kto podaje się za Twojego bliskiego i prosi o pieniądze, **nie rób nic, nie klikaj w linki i nie rób żadnych przelewów**. Skontaktuj się z bliskim w inny sposób - np. dzwoniąc pod stary numer i zweryfikuj prośbę.





# CYBERATAKI - JAK SIĘ ICH USTRZEC?



- Nie klikaj w linki i załączniki **niewiadomego pochodzenia**.
- **Sprawdź dokąd prowadzi link**, w który chcesz kliknąć (po najechaniu na niego myszką w prawym rogu przeglądarki wyświetla się prawdziwy adres strony).
- **Uważnie sprawdzaj adres nadawcy**. Oszuści tworzą adresy e-mail nieznacznie różniące się od tych, które znasz albo też ustawiają nazwę wiarygodnego nadawcy (np. Ministerstwa Finansów), które wyświetla się przed prawdziwym podejrzanym adresem mejlowym.
- Korzystaj tylko z **legalnego oprogramowania**.
- **Aktualizuj aplikacje na komputerze i telefonie**. Producenci oprogramowania w kolejnych aktualizacjach wprowadzają ulepszenia zabezpieczeń.
- **Ustaw silne hasła - używaj menedżera haseł** lub stwórz długie hasło samodzielnie, które będzie zawierało znaki specjalne, małe i wielkie litery oraz liczby.
- **Nie stosuj jednego hasła** do kilku kont.
- Przy logowaniu **korzystaj z weryfikacji dwuetapowej** (np. hasło + SMS).
- **Rób kopie zapasowe** ważnych plików.
- Korzystasz z **publicznej sieci wi-fi**? Nie loguj się do banków.

## PAMIĘTAJ!



**Szef poprosił Cię przez e-mail o pilne wykonanie dużego przelewu? Bank wymaga podania danych, których zazwyczaj nie wymaga?**

Zweryfikuj to.  
Sięgnij po telefon, zadzwoń i upewnij się, czy nie jest to próba oszustwa.

Pamiętaj, żeby używać innego kanału komunikacji niż tego, z którego pochodzi wiadomość.

# BEZPIECZNE DANE

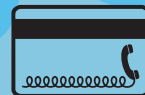
**PADŁEŚ OFIARĄ PHISHINGU,  
A TWOJE DANE OSOBOWE LUB  
DO LOGOWANIA WYCIĘKŁY?  
SPRAWDŹ, CO POWINIENEŚ  
ZROBIĆ.**

## PAMIĘTAJ!

**W każdej chwili możesz sprawdzić,  
czy Twoje dane są bezpieczne.**  
Wejdź na [bezpiecznedane.gov.pl](https://bezpiecznedane.gov.pl)  
i sprawdź, czy Twój PESEL, numer  
telefonu lub adres mejlowy nie  
zostały udostępnione w sieci.  
To rządowa strona. Żeby z niej  
skorzystać i sprawdzić swoje dane,  
musisz się zalogować - np. poprzez  
aplikację mObywatel, Profil Zaufany  
lub bankowość elektroniczną.



**Zmień dane logowania**  
na najważniejszych stronach



**Skontaktuj się z bankiem**  
i powiedz o wycieku danych



**Zastrzeż PESEL przez mObywatela**  
- uniemożliwisz przestępcy wzięcie  
kredytu na swoje dane



**Zgłoś próbę oszustwa**  
na stronie [incydent.cert.pl](https://incydent.cert.pl)  
lub przez mObywatela



**Podjęrżane SMS-y z linkami  
prześlij pod numer 8080**





# JAK PRZYGOTOWAĆ SIĘ FINANSOWO NA KRYZYS?

W każdej sytuacji **warto regularnie odkładać** nawet drobne sumy pieniędzy na tzw. czarną godzinę. Z biegiem czasu możemy zbudować poduszkę finansową, która **pozwole nam lepiej poradzić sobie w przypadku większych i mniejszych kryzysów**, np.:

- niespodziewanych wydatków,
- utraty pracy,
- problemów zdrowotnych,
- przeprowadzki,
- ewakuacji na wypadek konfliktu.

## WAŻNE!

Jeśli chcesz sprawdzić, ile musisz odkładać, żeby zrealizować określony cel albo też jak wygląda przyrost odsetek przy oszczędzaniu długoterminowym, **skorzystaj z kalkulatora oszczędzania** na stronie Urzędu Ochrony Konkurencji i Konsumentów: [uokik.gov.pl/twoje-finanse](https://uokik.gov.pl/twoje-finanse).



# JAK PRZYGOTOWAĆ SIĘ FINANSOWO NA KRYZYS?

Na wypadek konfliktu lub sytuacji kryzysowej **warto mieć w domu:**



**gotówkę w różnych nominałach**



**złotą biżuterię** - pozwoli płacić za niezbędne towary lub usługi



**"twardą" walutę** (np. dolar amerykański, euro) - w czasie wojny lokalny pieniądź traci na wartości

## WAŻNE!

Pamiętaj, że oprócz zabezpieczenia środków na przetrwanie w pierwszym okresie wojny, musisz zadbać o odtworzenie swojego majątku po kryzysie.

**Dlatego w czasie ewakuacji zabierz ze sobą wszystkie dokumenty**, które udowodnią Twoje prawo własności do domu lub mieszkania (zob. -> II część Poradnika dla mieszkańców Zielonki)

## PAMIĘTAJ!

W Poradniku edukujemy i dzielimy się jedynie dobrymi praktykami. Nie jest to jednak profesjonalne doradztwo w zakresie finansów ani rekomendacja inwestycyjna w rozumieniu przepisów prawa. **Każdy z nas sam podejmuje decyzje finansowe i bierze za nie pełną odpowiedzialność.**



# KONFLIKT ZBROJNY

**Za obronę kraju nie odpowiada tylko wojsko.** Przed nieprzyjacielem broni się całe państwo - instytucje publiczne, służby ratownicze, porządkowe, medyczne, przedsiębiorstwa, organizacje pozarządowe, a także my wszyscy - obywatele. **Każdy ma ważną rolę do spełnienia - niekoniecznie na froncie.**

W czasie pokoju w Polsce funkcjonuje system ochrony ludności. Po wybuchu wojny przekształca się w obronę cywilną. Armia walczy z najazdem wrogich wojsk, a obrona cywilna - ze skutkami działań wojennych.

**Naszym zadaniem jest wzięcie odpowiedzialności za nas samych i za nasze najbliższe otoczenie.** W ten sposób ograniczamy skutki kryzysu i skuteczniej bronimy się przed nieprzyjacielem.

Celem państwa jest, aby - mimo wojny - nadal funkcjonowało. Aby dzieci się uczyły, piekarnie piekły chleb, a seniorzy otrzymywali emerytury.

## WAŻNE!

**Z art. 85 Konstytucji RP wynika wprost, że obowiązkiem obywatela polskiego jest obrona Ojczyzny.**





# ATAK Z POWIETRZA



- W czasie ataku lotniczego lub dronowego ukryj się. **Wybierz najbliższe miejsce schronienia.**
- Zawsze **lepiej być wewnątrz budynku** niż na zewnątrz - ze względu na uderzenia odłamków.
- Schroń się **w piwnicy, garażu podziemnym, na stacji metra.**
- Schronienie powinno być **bez okien**, mieć grube ściany i strop, a także - wyjście awaryjne.
- Jeśli w pomieszczeniu są okna, odejdź od nich jak najdalej - **rozpryskujące szkło jest bardzo niebezpieczne.**
- Chowasz się w domu? **Stosuj zasadę dwóch ścian.** Niech od ulicy oddzielają Cię dwie ściany. Często najbezpieczniejszymi miejscami są łazienka lub korytarz.
- Jeśli przebywasz **na dworze, połóż się na ziemi** - najlepiej w rowie lub zagłębieniu. Chroń głowę.
- **Najlepszą ochronę zapewniają schrony.** Ich liczba w Polsce jest jednak ograniczona.





Kryzysy zdarzają się naprawdę...



## WIELOKROTNE NARUSZENIE POLSKIEJ PRZESTRZENI POWIETRZNEJ (2025)

We wrześniu 2025 roku polska przestrzeń powietrzna została wielokrotnie naruszona przez rosyjskie drony. Atak był celowy - **chciano przetestować reakcje państwa polskiego i NATO**. Jeden z dronów został zestrzelony przez wojsko. Wskutek obrony ucierpiał dom jednorodzinny w Wyrykach na Lubelszczyźnie.

Kryzysy zdarzają się naprawdę...



## EKSPLOZJA W PRZEWODOWIE (2022)

W listopadzie 2022 r. na Lubelszczyźnie, tuż przy granicy, **doszło do eksplozji rakiety przeciwlotniczej**. Zginęło dwóch obywateli Polski.

Do wypadku doszło w dniu zmasowanych ataków Rosji na Ukrainę - ukraiński pocisk obrony przeciwlotniczej zabłąkał się na terytorium Polski.

# ZAGROŻENIE ATAKIEM CBRN

## BRONŃ CBRN

to broń masowego rażenia substancjami:

- C** chemicznymi
- B** biologicznymi
- R** radiologicznymi
- N** jądrowymi

## PAMIĘTAJ!

W przypadku skażenia promieniotwórczego bądź gotowy na pobyt w uszczelnionym budynku. **Poziom napromieniowania w miejscu wybuchu jądrowego znacząco spada już po kilku dniach.**

# ZAGROŻENIE ATAKIEM CBRN



**Jak najszybciej opuść skażony obszar**, w aucie zamknij okna, wyłącz klimatyzację i wentylację.



**Chroń drogi oddechowe i skórę.**



**W budynku - zamknij i uszczelnij okna, drzwi, kominki i piece.** Wyłącz wentylatory i klimatyzację.



**Aby ochronić się przed promieniowaniem**, ukryj się w piwnicy lub w miejscu z grubymi ścianami.



**Po wyjściu z zagrożonej strefy** zdejmij skażone ubranie, i włóż do plastikowego worka i zamknij.



**Umyj ręce i twarz mydłem**, weź prysznic lub przetrzyj ciało mokrymi chusteczkami.



**Zalóż czyste ubranie.**



**Nie jedz i nie pij** niczego, co mogło być narażone na promieniowanie.



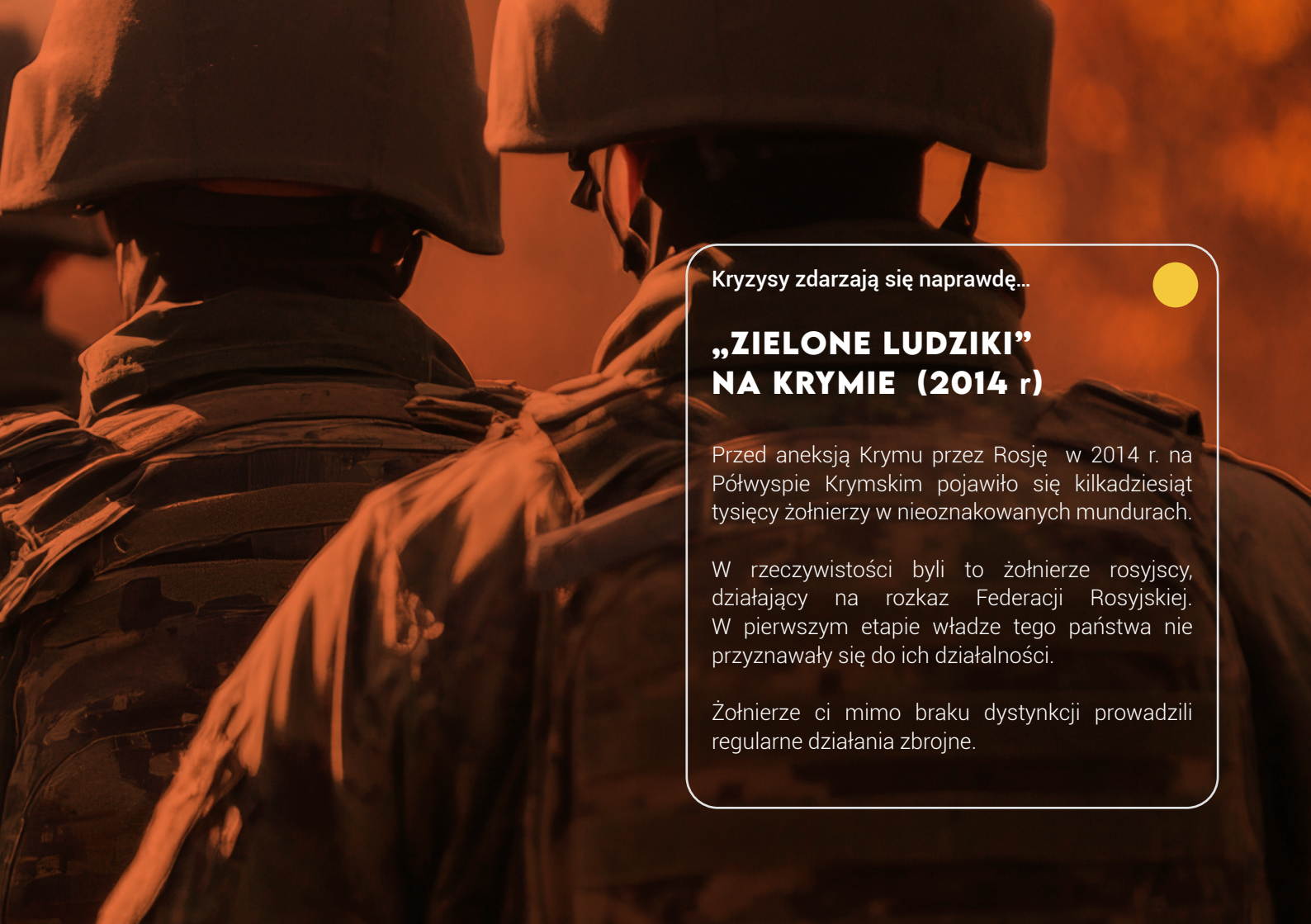


# OBCY ŻOŁNIERZE W POLSCE



Jeśli w Twojej okolicy pojawią się **niezidentyfikowani żołnierze**, zachowaj szczególną ostrożność.

- Jeśli widzisz ich na swojej drodze, **zmień kierunek**.
- **Nie nagrywaj żołnierzy, nie rób im zdjęć**, ani nie przyglądaj się sprzętowi wojskowemu. Możesz być wzięty za szpiega.
- Podczas rozmowy z nimi **nie trzymaj rąk w kieszeni**.
- Jeśli obcy żołnierz prosi o dokumenty, daj mu je. **Współpracuj z nim i nie kłóć się**.
- **Noś odzież w neutralnych kolorach**. Zrezygnuj z ubrań moro lub z emblematami. Możesz być uznany za żołnierza.



Kryzysy zdarzają się naprawdę...

## **„ZIELONE LUDZIKI” NA KRYMIE (2014 r)**

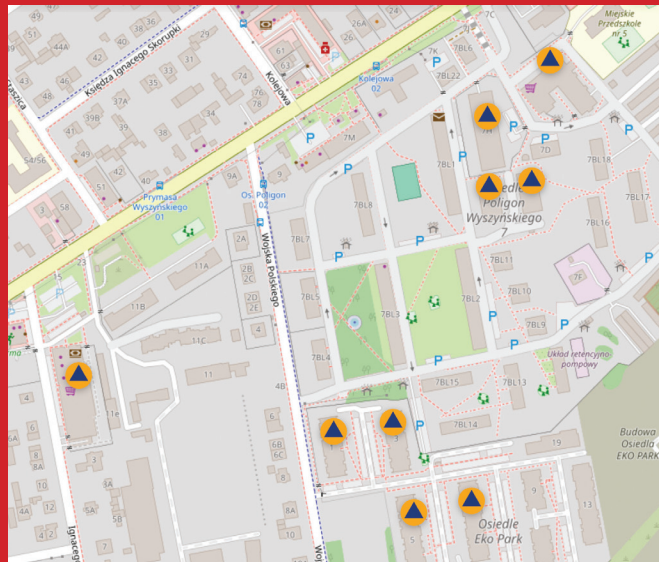
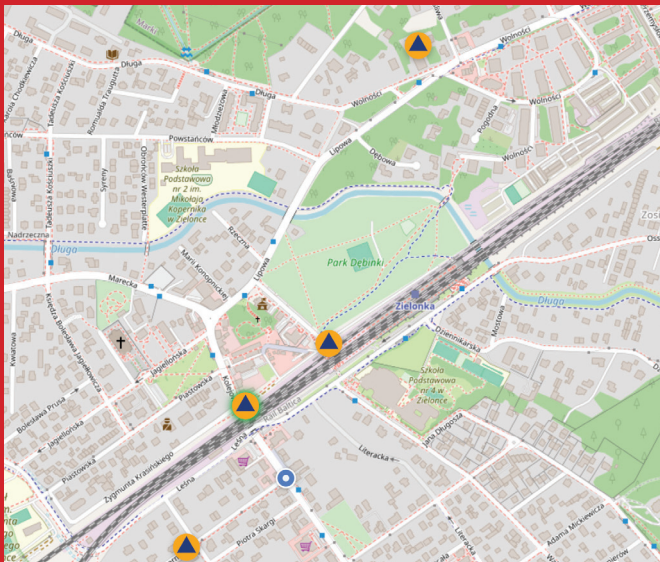
Przed aneksją Krymu przez Rosję w 2014 r. na Półwyspie Krymskim pojawiło się kilkadziesiąt tysięcy żołnierzy w nieoznakowanych mundurach.

W rzeczywistości byli to żołnierze rosyjscy, działający na rozkaz Federacji Rosyjskiej. W pierwszym etapie władze tego państwa nie przyznawały się do ich działalności.

Żołnierze ci mimo braku dystynkcji prowadzili regularne działania zbrojne.



# PUNKTY SCHRONIENIA



Najbliższe punkty schronienia w Zielonce możesz sprawdzić w nowej rządowej aplikacji

[gdziesieukryc.pl](https://gdziesieukryc.pl)



# RODZINNY PUNKT ZBORNY



W razie rozdzielenia i utraty kontaktu spotykamy się w:

adres miejsca spotkania

adres miejsca spotkania

adres miejsca spotkania



adres miejsca spotkania

adres miejsca spotkania

adres miejsca spotkania





**Ochrona ludności  
i obrona cywilna**

**SFINANSOWANO ZE ŚRODKÓW PROGRAMU  
OCHRONY LUDNOŚCI I OBRONY CYWILNEJ  
NA LATA 2025-2026**



Ministerstwo Spraw  
Wewnętrznych i Administracji



**Ochrona ludności  
i obrona cywilna**