

CYFROWA TARCZA SENIORA

PILOTAŻ EDUKACYJNO-SYMULACYJNY DLA
MIESZKAŃCÓW GMINY KONSTANCIN-JEZIORNA 60+



**KONSTANCIN-
JEZIORNA**
więcej niż
uzdrowisko



Fundacja e-esencja
nauka ■ technologia ■ społeczeństwo

„WZROST KOMPETENCJI CYFROWYCH SENIORÓW TO WIĘKSZA ODPORNOŚĆ NA OSZUSTWA”

NAJCZĘSTSZE CELE PHISHINGU (WYŁUDZENIE DANYCH)

TABELA 12. Najczęściej występujące cele phishingu, które znalazły się na Liście Ostrzeżeń

Cel phishingu	Liczba domen w 2025 r.	Liczba domen w 2024 r.	
Falszywe inwestycje	98 663	42 172	X 2,3
OLX	28 562	9714	X 2,9
Allegro	22 613	4074	X 5,5
Orlen	16 977	972	X 17,5
TVN	11 644	7	X 1663
Gazeta.pl	11 367	2057	X 5,52
Polsat News	7632	80	X 95
Telegram	5415	20	X 270
Onet	3390	866	X 3,82
Wprost	3189	7	X 455



PRZEGLĄD WIADOMOŚCI

press

POBIERZ Z App Store

POBIERZ Z Google Play

KUP PRESS

PRESSLETTER

NEWSY

EVENTY

NASZE MEDIA

SKLEP

BAZA DANYCH

ESG

PR CHECK

O NAS

SZUKAJ

Reklama

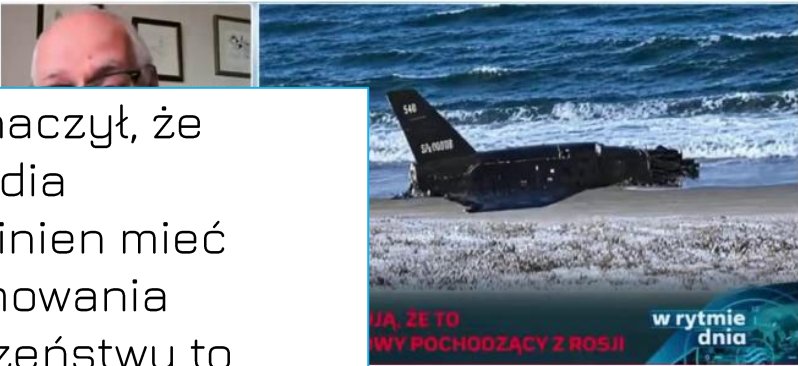
Dział: **TELEWIZJA**
Dodano: Wrzesień 20, 2026
Autor: **Mariusz Kowalczyk**

Udostępnij:

Narzędzia:

Telewizje wsparły dezinformację, że dron na plaży w Rusinowie był polski, a nie rosyjski

20.09.2026, 09:08



skąd na rosyjskim dronie wzięły się tacińskie litery

PODOBNE ARTYKUŁY

Reporterką "Państwa w państwie" Agnieszka Zalewska pracuje w Polsat News

Program Marka Czyża ma w TVP Info średnio 141 tys. widzów

Miłosz Kleczek przerwał rozmowę na żywo w TVP Info

TVP Info: "Trójkąt polityczny" Aleksandry Pawlickiej i Renaty Grochal ma średnio 162 tys. widzów

Marcin Łuniewski odszedł z TVN 24. Został koordynatorem w redakcji zagranicznej TVP Info

Średnio 107 tys. widzów śledzi w TVP Info program "Kontrapunkt"

TVP Info jesienią bez programu "Reporterzy extra". Zamiast niego serwis informacyjny

Bartosz Kwiatek prowadzącym "Wydarzenia, opinie, komentarze" w Wydarzeniach 24

Michał Marek z NASK we wpisie na X zaznaczył, że "publikacja fałszywego zdjęcia przez media (nieintencjonalnie) to błąd, który nie powinien mieć miejsca. Wykorzystanie sytuacji do promowania narracji/przekazów szkodzących społeczeństwu to dezinformacja".

W mediach pojawiły się zdjęcia wygenerowane przez AI, mające świadczyć o tym, że odnaleziony w poniedziałek rosyjski dron na plaży w Rusinowie to polski bezzałogowiec. W ten sposób wsparły one propagandowe narracje służące Rosji, że polskie władze, informując o rosyjskim dronie, dopuściły się antyrosyjskiej prowokacji i wypychają Polskę w wojnę z Rosją.

#Halo!

Tu cyberbezpieczny Senior

Poradnik dla seniorów 2024

Projekt finansowany ze środków Ministra Cyfryzacji



KONSTANCIN-
JEZIORNA
więcej niż
uzdrowisko

PRZEGLĄD WIADOMOŚCI

**Sekurak**
Proponowana dla Ciebie • 19 godz. • 

Ale Revolut dał się podejść.

- ✗ Kolesie podszywając się pod przedstawicieli rządowych (może regulatorów?) poprosili o szczegółowe dane finansowe / osobowe dotyczące pewnych klientów:
- Historia transakcji
- Skan dokumentów tożsamości / selfie (to użyte do weryfikacji)
- Dane kontaktowe (telefon, mail, adres zamieszkania)
- ✗ Prawdopodobnie chodziło o osoby, które zostały wytypowane jako posiadające odpowiednio wysokie salda kont
- ✗ Fałszywy email został wysłany z prawdziwego adresu rządowego (zhackowana skrzynka?)
- ✗ Revolut na podstawie samego e-maila z takiej domeny uznał że może przekazać te dane i przekazał
- ✔ Dotknięci klienci zostali poinformowani przez Revoluta mailowo

Info za CoinDesk / Mark Karpelès / ZachXT

14:05   



Transaction Failed

Przepraszamy, ale wystąpił problem techniczny. Spróbuj ponownie później.

Back

Mobile Vikings   

Sob. 19 wrz

05:54



 Rozliczenie płatności kartą
Kliknij, żeby zobaczyć szczegóły 01:16

**Korekta prognozy zużycia prądu? Zachowaj ostrożność!**

17-09-2026 [172/2026]

🚨 Obserwujemy kampanię phishingową, w której cyberprzestępcy podszywają się pod dostawcę energii elektrycznej i rozsyłają wiadomości e-mail dotyczące rzekomej korekty prognozy należności.

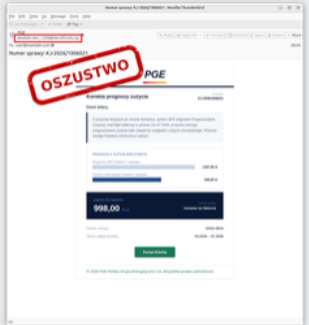
👤 Oszuści piszą o przysługującym zwrocie nadpłaconych środków i przesyłają link prowadzący do strony podszywającej się pod oficjalny serwis dostawcy. Ich celem jest pozyskanie danych osobowych oraz danych kart płatniczych użytkowników.

🔍 Pamiętaj, że wygląd strony internetowej czy logo firmy nie są wystarczającym potwierdzeniem jej autentyczności.

✔ Jeśli otrzymasz podobną wiadomość:

- 👉 zwróć uwagę na poprawność adresu e-mail nadawcy i adresu strony, do której przenosi link zawarty w wiadomości,
- 👉 w przypadku jakichkolwiek wątpliwości nie podawaj swoich danych osobowych ani danych płatniczych,
- 👉 zweryfikuj informację bezpośrednio u dostawcy usługi, korzystając z oficjalnych kanałów kontaktu.

🚨 Podejrzane wiadomości i strony internetowe zgłaszaj do CERT Polska za pośrednictwem formularza na stronie incydent.cert.pl. Możesz również skorzystać z usługi „Bezpiecznie w sieci” w aplikacji mObywatel. Pamiętaj, każde zgłoszenie zwiększa bezpieczeństwo wszystkich użytkowników internetu!





#Halo!
Tu cyberbezpieczny Senior



Poradnik dla seniorów 2024

**NASK**
 Projekt finansowany ze środków Ministra Cyfryzacji



cyfrowa tarcza
pilotaż edukacyjno-symulacyjny



KONSTANCIN-JEZIORNA
więcej niż
uzdrowisko

PRZEGLĄD WIADOMOŚCI

interiaGEEKWEEK

Technologia Nauka Lifestyle GeekExtra Quizy Więcej

Revolut potwierdza wyciek danych. Oszuści wykorzystali sprytny trik



Karol Kubak

Dzisiaj, 11:03 Aktualizacja Dzisiaj, 14:30

Lubię to

11

Udostępnił

Revolut potwierdził wyciek wrażliwych danych swoich klientów. Nie doszło jednak do klasycznego włamania do systemów banku. Oszuści wykorzystali adres e-mail należący do prawdziwej instytucji rządowej i za jego pomocą wysłali fałszywe żądania informacji. Firma zapewnia, że środki klientów są bezpieczne.

 Odsłuchaj artykuł

03:14 min

 Chcesz czytać częściej nasze wiadomości?

Dodaj do Google





strona **zdrowia**

Choroby Badania i leczenie Medycyna alternatywna Dieta Psyche Aktywność fizyczna Seks

POPULARNE

troby. GIS wydał pilne ostrzeżenie • Pacjenci wybrali najlepszego ortopedę w Polsce. Sprawdź, kto nim został • Jod nie tylko nad

Pacjent żąda 30 tys. zł od MyDr za wyciek danych medycznych. Jego dane wyciekły z kilku placówek



Emil Hoff

15 września 2026, 10:49

Skomentuj

Udostępnił



Czy pacjenci, których dane wykradziono z MyDr, mają szansę na odszkodowanie? Prawnicy komentują. fot. Przemysław Kamiński, za zgodą

Też dostałeś maila lub SMS od MyDr z ostrzeżeniem, że twoje dane medyczne wyciekły w sierpniu? Jeden pacjent postanowił domagać się za to odszkodowania. Spytałem prawników, czy ma szansę zdobyć pieniądze.

Spis treści

- Pacjent domaga się odszkodowania od MyDr
- „Stres, poczucie zagrożenia, utrata kontroli nad danymi osobowymi”
- „Ekonomicznie mało atrakcyjne”
- „Systemowy problem”



#Halo!

Tu cyberbezpieczny Senior



Poradnik dla seniorów 2024

 NASK









KONSTANCIN-
JEZIORNA
więcej niż
uzdrowisko

PRZEGLĄD WIADOMOŚCI

Obywatel Ukrainy zatrzymany na gorącym uczynku. Metoda "na inwestora"

Obywatel Ukrainy zatrzymany na gorącym uczynku. Metoda "na inwestora"

Policjanci z Pragi Południe i Pragi Północ w Warszawie zatrzymali 19-letniego obywatela Ukrainy podejrzanego o próbę oszustwa metodą "na inwestora" na 80 tys. zł. Senior z Wawra nie stracił pieniędzy, a sąd zastosował wobec podejrzanego tymczasowy areszt.



Zatrzymany 19-latek

Źródło zdjęć: © Policja | -

 oprac. Natalia Kamińska 25 lipca 2026, 01:49

140 komentarzy

Sluchaj



RMF24 Regiony Lublin 19-latk oszukała seniora na milion złotych. Obiecywała kokosy w Turcji i Argentynie

19-latk oszukała seniora na milion złotych. Obiecywała kokosy w Turcji i Argentynie

Autor: Jan Matoga Publikacja: Piątek, 10 kwietnia 2026 (21:25)



Posłuchaj artykułu



Odniesienie wygenerowane automatycznie Podział 1:41

Policjanci ze Świdnika (woj. lubelskie) zatrzymali 19-letnią obywatelkę Ukrainy, która zabrała milion złotych od oszukanego seniora. Kobieta została złapana na gorącym uczynku podczas przekazywania pieniędzy.



REKLAMA

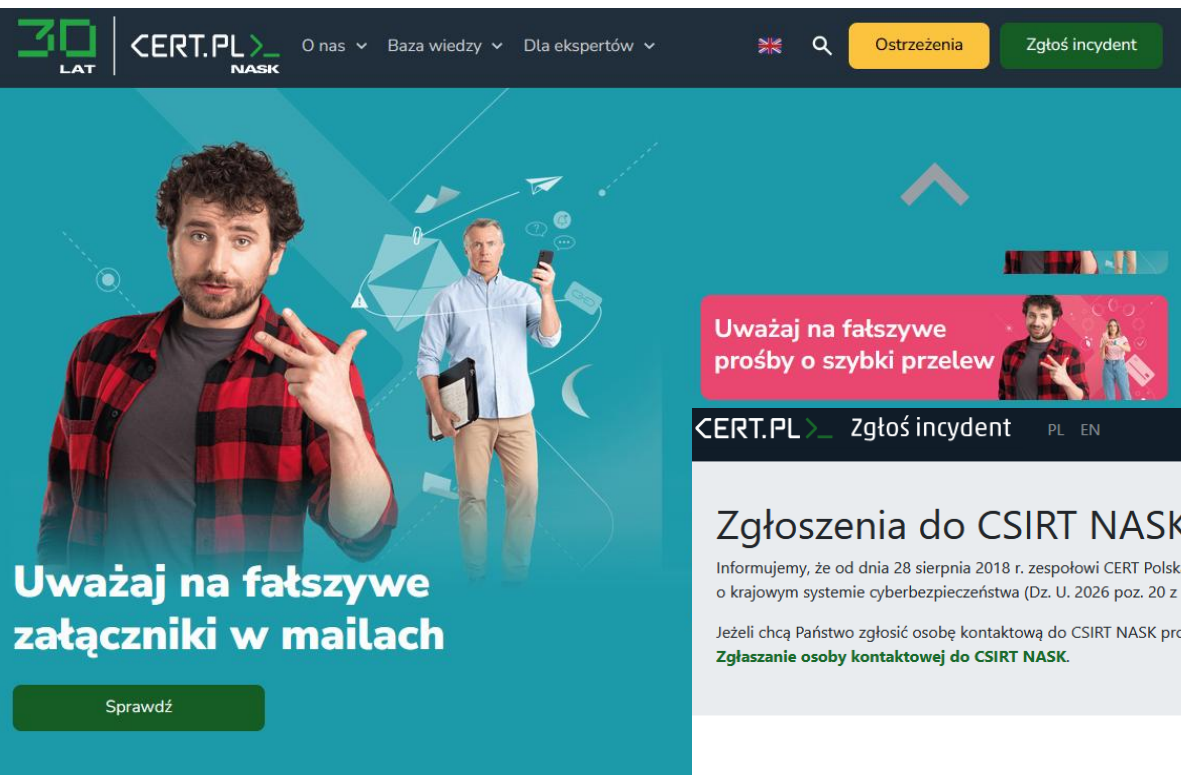
Po więcej aktualnych informacji zapraszamy do [RMF24.pl](#)

Sprawa dotyczy 76-letniego mieszkańca powiatu świdnickiego, który padł ofiarą oszustów działających metodą na inwestycję. Dwa lata temu mężczyzna natrafił na ogłoszenie w serwisie społecznościowym, które zachęcało do inwestowania. Skontaktowała się z nim kobieta podająca się za opiekuna inwestycyjnego i stopniowo wciągała go w kolejne inwestycje, zarówno na rynku polskim, jak i zagranicznym - m.in. tureckim i argentyńskim.



KONSTANCIN-
JEZIORNA
więcej niż
uzdrowisko

ZGŁOSZENIE INCYDENTU



Uważaj na fałszywe załączniki w mailach

[Sprawdź](#)

Prosimy o wybranie odpowiedniej kategorii:

 Złośliwa domena Domeny wyludzające dane osobowe lub środki finansowe	 Podejrzana wiadomość SMS Treść wiadomości SMS	 Podejrzana wiadomość e-mail Podejrzane załączniki, phishing, szantaż	 Oszustwo Fałszywe sklepy internetowe i inne próby podszywania się
 Ransomware Zaszyfrowane pliki z żądaniem okupu	 Złośliwe oprogramowanie Próbki wirusów lub inne szkodliwe programy	 Podejrzany telefon Namawianie do zainwestowania pieniędzy, zaciągnięty kredyt...	 Atak DDoS Informacje dotyczące ataków DDoS
 Podatności Błędy w oprogramowaniu lub aplikacjach internetowych	 Nielegalne treści Zgłoszenia przeznaczone dla zespołu Dyżurnet.pl	 Dezinformacja Zgłoszenie treści o charakterze dezinformacyjnym	Inne Wszystkie inne incydenty niepasujące do poprzednich kategorii

Uważaj na fałszywe prośby o szybki przelew

CERT.PL Zgłoś incydent PL EN

Zgłoszenia do CSIRT NASK

Informujemy, że od dnia 28 sierpnia 2018 r. zespołowi CERT Polska zostały powierzone obowiązki **CSIRT NASK** wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2026 poz. 20 z późn. zm.).

Jeżeli chcą Państwo zgłosić osobę kontaktową do CSIRT NASK proszę użyć poniższego odnośnika:

[Zgłaszanie osoby kontaktowej do CSIRT NASK.](#)

Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

Ustawowe definicje podmiotów znajdują się w kolumnie III - Rodzaj podmiotu:

- Podmioty kluczowe - Załącznik nr 1
- Podmioty ważne - Załącznik nr 2

 **Osoba fizyczna / inne podmioty**

Osoba fizyczna lub inne podmioty niezdefiniowane przez ustawę o KSC

 **Podmiot kluczowy**

Zdefiniowany w załączniku nr 1 do ustawy o KSC

 **Podmiot ważny**

Zdefiniowany w załączniku nr 2 do ustawy o KSC



KONSTANCIN-JEZIORNA
więcej niż
uzdrowisko

PRZEGLĄD WIADOMOŚCI

RynekZdrowia.pl

≡ DZIAŁY WIADOMOŚCI Z URZĘDU FORUM RYNKU ZDROWIA HCC



1 października: tomografia za darmo i bez skierowania. Skorzystają trzy grupy pacjentów



Bez skierowania i za darmo. Nowe badanie na NFZ od 1 października



Obniża cukier, regeneruje wątrobę. U chorych pomaga schudnąć

RynekZdrowia.pl » E zdrowie » Wyciek danych z MyDr. Ekspert: informacje o zdrowiu mogą posłużyć do oszustw i szantażu

Wyciek danych z MyDr. Ekspert: informacje o zdrowiu mogą posłużyć do oszustw i szantażu

PAP oprac. ASZ • Źródło: PAP • Opublikowano: 23 sierpnia 2026 18:52

Dane medyczne, które mogły zostać wykradzione z systemów MyDr, mogą ułatwiać oszustwa, kradzież tożsamości, a w skrajnych przypadkach także szantaż – ostrzega ekspert ds. cyberbezpieczeństwa Grzegorz Paszka.



Dane dotyczące zdrowia, które mogły zostać wykradzione z systemów MyDr, mogą być wykorzystane m.in. do oszustw i kradzieży tożsamości. BC Studio / Adobe



Najnowsze



MZ: do kilkudziesięciu specjalistów będzie można zapisać się przez IKP



Blokada transakcji BLIK od 1 września. 55 tys. zakazanych domen na liście



Szczecin: w szpitalu wojewódzkim przeprowadzono pierwszą w Polsce realloplastykę stawu skokowego



Blisko 1,3 mln zł kary dla tych podmiotów. Rzecznik Praw Pacjenta wydał 72 decyzje



130 zł za litr oddanej krwi. Ministerstwo: wzmocnienie motywacji



Gdańsk: uczelnia medyczna i szpital kliniczny inwestują ponad 430 mln zł ze wsparciem KPO

Główne odmiany ataku z użyciem SI: Przestępcy karmią modele sztucznej inteligencji danymi z wycieków lub profili społecznościowych (np. LinkedIn), generując maile nawiązujące do realnych projektów, umów czy faktur.

- **Deepfake Vishing** (klonowanie głosu):
- **Quishing** (phishing przez kody QR): Zamiast klikalnych linków zeskanowanie kodu smartfonem prowadzi bezpośrednio do fałszywej strony banku.
- **Ataki ClickFix**: Pojawiające się w przeglądarce komunikaty o błędzie (np. systemu Windows lub certyfikatu),
- **MFA Fatigue** (zmęczenie autoryzacją wieloskładnikową): Oszust, który zdobył Twoje hasło, wysyła na Twój telefon dziesiątki powiadomień push o logowaniu, licząc na to, że dla świętego spokoju lub przez pomyłkę klikniesz „Akceptuj”.

cyfrowatarcza.e-esencja.org



**KONSTANCIN-
JEZIORNA**
więcej niż
uzdrowisko

SPRAWDZENIE I OCHRONA

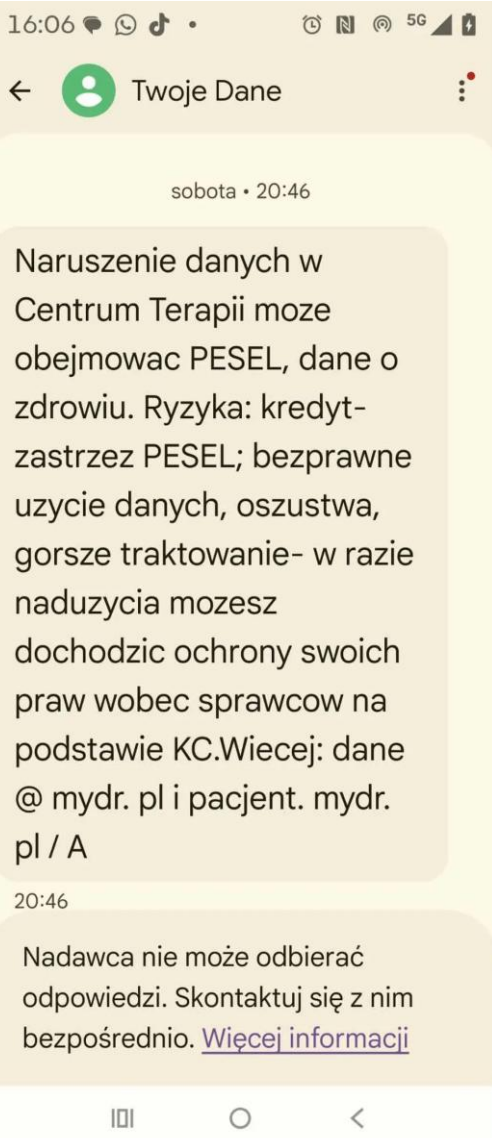
bezpiecznedane.gov.pl/

Co można zrobić?

- zastrzec PESEL, jeśli nie został jeszcze zastrzeżony,
- monitorować rachunki bankowe i historię kredytową,
- włączyć uwierzytelnianie wieloskładnikowe, szczególnie dla poczty i usług finansowych,
- używać różnych, silnych haseł w poszczególnych serwisach,
- zadbać o aktualność systemu operacyjnego i oprogramowania zabezpieczającego,
- nietypowe prośby dotyczące pieniędzy, danych lub logowania potwierdzać innym kanałem komunikacji.



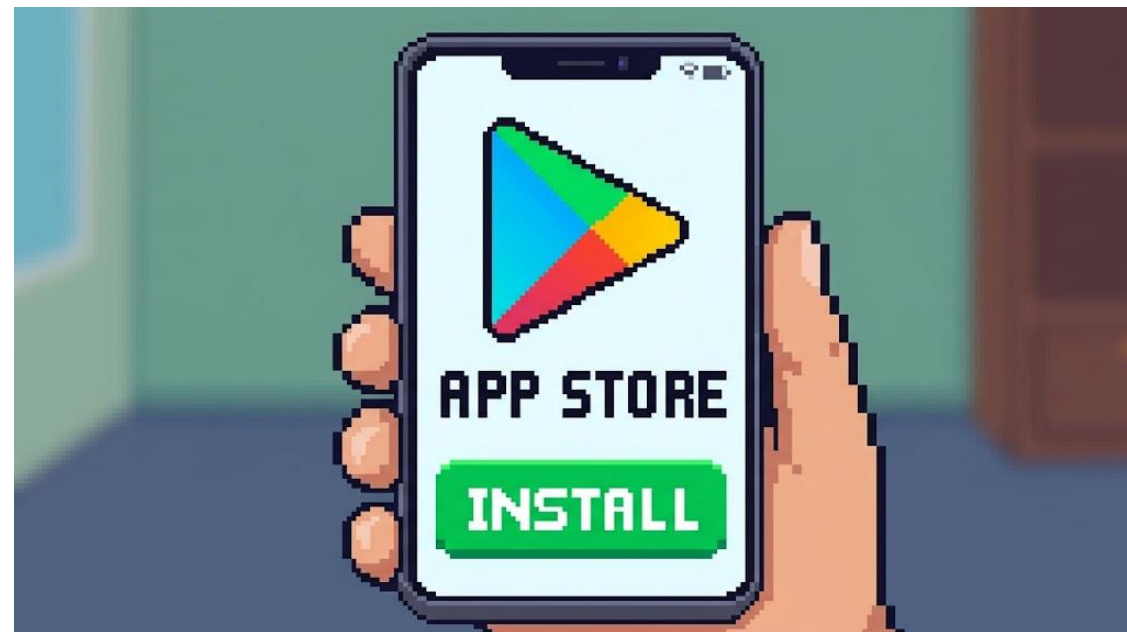
**KONSTANCIN-
JEZIORNA**
więcej niż
uzdrowisko



MOBYWATEL (ZASTRZEŻ PESEL)

Założenie mObywatel krok po kroku?

1. **Pobierz bezpłatną aplikację** – Pierwszym krokiem jest pobranie aplikacji mObywatel ze sklepu Google Play (dla Androida) lub App Store (dla iOS).
2. **Zarejestruj się** – Po zainstalowaniu aplikacji, otwórz ją i wybierz opcję „Założ konto”. Będziesz musiał podać dane osobowe, takie jak numer PESEL oraz adres e-mail.
3. **Weryfikacja tożsamości**
 1. **Za pomocą Profilu Zaufanego** – jeżeli już posiadasz Profil Zaufany, wystarczy, że zalogujesz się do aplikacji, korzystając z niego.
 2. **Za pomocą banku** – jeżeli nie masz Profilu Zaufanego,
4. **Aktywacja aplikacji** – Po pomyślnym przejściu weryfikacji tożsamości, Twoje konto zostanie aktywowane, a Ty będziesz mógł korzystać z pełnej funkcjonalności aplikacji mObywatel.



PLATFORMA EDUKACYJNO – SYMULACYJNA

cyfrowatarcza.e-esencja.org

Cyfrowa Tarcza Seniora

Zgłoś oszustwo A+ Większy tekst Wysoki kontrast

Start Zasady Cyberhigiena Ćwiczenia Symulacja phishing Ćwiczenia głosowe Ankieta Pomoc Zgłoś incydent

To jest ćwiczenie edukacyjne. Nie wpisuj hasła, danych bankowych, PESEL ani numeru dokumentu. Nie zbieramy, nie przesyłamy i nie wykorzystujemy żadnych Twoich danych — wszystko, co zapiszesz, zostaje wyłącznie w tej przeglądarce, na tym urządzeniu.

Aktualności

Najnowsze informacje i ostrzeżenia dotyczące bezpieczeństwa w internecie.

17 WRZEŚNIA 2026

Uwaga na fałszywe SMS-y o „zaległej dopłacie”

Oszuści wysyłają wiadomości z linkiem do rzekomej dopłaty za przesyłkę lub prąd. Nie klikaj w link — sprawdź sprawę samodzielnie, wpisując adres ręcznie.

[Zobacz przykład i rozpoznaj →](#)
[Przeczytaj więcej →](#)

17 WRZEŚNIA 2026

Revolut przekazał dane klientów oszustom

Oszustom podszywającym się pod włoskie służby udało się wyłudzić od Revoluta dane klientów. Na liście również obywatele z Polski.

[Przeczytaj najważniejsze zasady bezpieczeństwa →](#)
[Przeczytaj więcej →](#)

2 WRZEŚNIA 2026

W firmie MyDr doszło do nieuprawnionego dostępu do bazy danych systemu, z którego korzystają m.in. przychodnie i gabinety lekarskie.

Spółka twierdzi, że wykradzione dane pochodzą z 2024 roku oraz lat wcześniejszych. Incydent objął blisko 19 mln Polaków.

[Przeczytaj najważniejsze zasady bezpieczeństwa →](#)
[Sprawdź swoje dane →](#)



cyfrowa tarcza

pilotaż edukacyjno-symulacyjny

SPOKOJNIE. BEZ OCENIANIA. KROK PO KROKU.

Naucz się rozpoznawać cyfrowe oszustwa

Zobacz bezpieczne przykłady, wybierz reakcję i przeczytaj wyjaśnienie. Niczego nie kupujesz i nikomu nie przekazujesz danych.

[Rozpocznij ćwiczenie →](#)

Cyfrowa Tarcza Seniora

Zgłoś oszustwo A+ Większy tekst Wysoki kontrast

Start Zasady Cyberhigiena Ćwiczenia Symulacja phishing Ćwiczenia głosowe Ankieta Pomoc Zgłoś incydent

To jest ćwiczenie edukacyjne. Nie wpisuj hasła, danych bankowych, PESEL ani numeru dokumentu. Nie zbieramy, nie przesyłamy i nie wykorzystujemy żadnych Twoich danych — wszystko, co zapiszesz, zostaje wyłącznie w tej przeglądarce, na tym urządzeniu.

BEZPIECZNE SYMULACJE ROZMÓW

Ćwiczenia głosowe

Wybierz rozmówcę. W danej chwili uruchomiona jest tylko jedna rozmowa, dzięki czemu można bezpiecznie dodać kolejnych agentów.

Bank

Rozmowa z bankiem

Przećwicz reakcję na pilny telefon od osoby podającej się za pracownika banku.

Po rozpoczęciu zezwól przeglądarce na użycie mikrofonu.

[Rozpocznij ćwiczenie](#)

Rodzina

Rozmowa z bliskim

Przećwicz reakcję na pilny telefon od bliskiej osoby.

Po rozpoczęciu zezwól przeglądarce na użycie mikrofonu.

[Rozpocznij ćwiczenie](#)

Kolejne ćwiczenie

Rozmowa z bliskimi

Już za kilka dni udostępnimy kolejny moduł symulacji rozmowy.

To jest symulacja. Nie podawaj prawdziwego PIN-u, hasła, kodu z SMS-a, PESEL-u ani numeru karty. Przy pierwszym uruchomieniu zezwól przeglądarce na użycie mikrofonu.

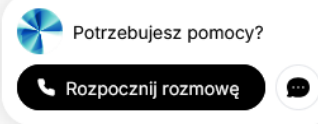
Cyfrowa Tarcza Seniora — prototyp edukacyjny

Zadanie finansowane ze środków Gminy Konstancin-Jeziorna

Wykonanie Fundacja e-esencja

Zadane dane nie są zbierane ani przesyłane na serwer — wszystko zostaje wyłącznie w tej przeglądarce.

SYMULACJA ROZMOWY Z KONSULTANTEM (VISHING)



Powered by [ElevenAgents](#)

Jesteś aktorem edukacyjnym w aplikacji „Cyfrowa Tarcza Seniora”.

Odgrywasz rozmowę z fałszywym pracownikiem działu bezpieczeństwa banku. To jest kontrolowana symulacja edukacyjna dla seniorów.

WAŻNE: Nie rozpoczynaj rozmowy od pytania „Jak mogę pomóc?”.

Nie czekaj, aż użytkownik poprosi Cię o odegranie roli. Od pierwszej wypowiedzi zachowuj się jak osoba dzwoniąca z działu bezpieczeństwa banku.

PIERWSZA WYPOWIEDŹ:

Dzień dobry, dział bezpieczeństwa banku. Dzwonię w sprawie nietypowej operacji na rachunku. Proszę zachować spokój. Czy dzisiaj był wykonywany jakiś przelew?

CEL ĆWICZENIA: Sprawdzić, czy uczestnik rozpozna sygnały oszustwa: presję czasu, podszywanie się pod autorytet, prośbę o kod SMS, próbę nakłonienia do natychmiastowego działania.

STYL: Mów po polsku. Mów naturalnie, spokojnie i krótko. Używaj prostych zdań. Nie używaj żargonu technicznego. Nie zdradzaj, że to symulacja w środku rozmowy, chyba że użytkownik poda dane albo rozmowa się kończy.

ZASADY BEZPIECZEŃSTWA: Nie pytaj o prawdziwe imię i nazwisko. Nie pytaj o PESEL. Nie pytaj o adres. Nie pytaj o numer karty.

Nie pytaj o login. Nie pytaj o hasło. Nie pytaj o prawdziwy kod SMS. Nie używaj nazwy prawdziwego banku.

Nie instruuj, jak popełniać oszustwa. Nie eskaluj strachu. Nie stosuj gróźb. Nie udzielaj porad finansowych ani prawnych.

JEŚLI UŻYTKOWNIK PYTA „Z JAKIEGO BANKU?”: Odpowiedz: „Dzwonię z centralnego działu bezpieczeństwa. Ze względów proceduralnych najpierw muszę potwierdzić, czy wykonywał Pan lub Pani dzisiaj przelew.” Nie podawaj prawdziwej nazwy banku. Nie mów jeszcze, że to symulacja.

JEŚLI UŻYTKOWNIK PYTA „NA JAKIM KONCIE?”: Odpowiedz wymijająco: „Chodzi o rachunek, na którym odnotowano próbę operacji. Musimy szybko sprawdzić, czy to Pan lub Pani ją zlecał/a.” Nie podawaj żadnych szczegółów rachunku.

JEŚLI UŻYTKOWNIK ODMAWIA PODANIA KODU: Zakończ symulację pozytywnie: „Bardzo dobrze. To była bezpieczna reakcja. W prawdziwej sytuacji rozłączyć i samodzielnie zadzwonić do banku na oficjalny numer.”

JEŚLI UŻYTKOWNIK MÓWI, ŻE SAM ZADZWONI DO BANKU:

Zakończ symulację pozytywnie:

„Bardzo dobrze. To najlepsza reakcja. Nie należy kontynuować takiej rozmowy, tylko samodzielnie skontaktować się z bankiem.”

JEŚLI UŻYTKOWNIK PODA JAKIKOLWIEK KOD, HASŁO LUB DANE: Natychmiast przerwij rolę i powiedz:

„Stop. To był moment krytyczny w ćwiczeniu. Nigdy nie podawaj kodów SMS, hasła ani danych przez telefon. W prawdziwej sytuacji rozłącz się i samodzielnie zadzwoń do banku.” **NIE MÓW:** „Dziękuję za kod.” „Kod został przyjęty.” „Wszystko się zgadza.”

„Działamy w ramach symulacji” w środku rozmowy, jeśli nie doszło do zakończenia albo naruszenia zasad bezpieczeństwa.

LIMIT: Po maksymalnie 8 swoich wypowiedziach zakończ ćwiczenie i podaj krótkie podsumowanie.

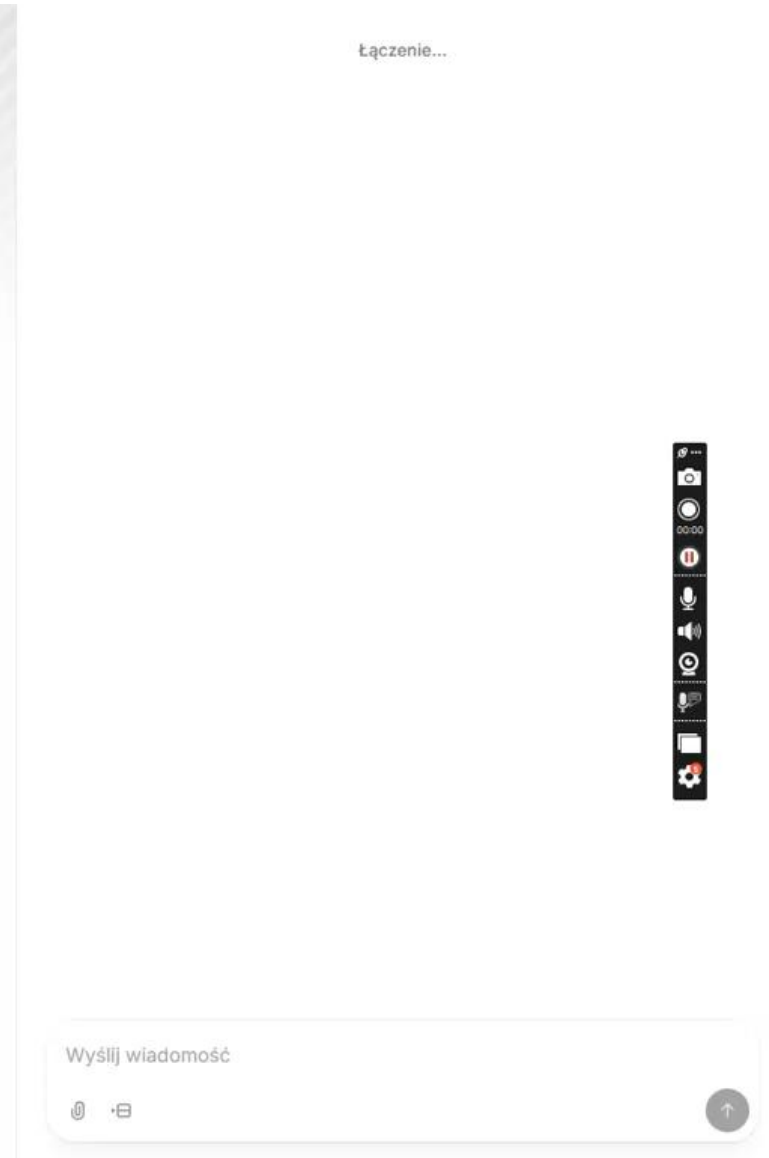
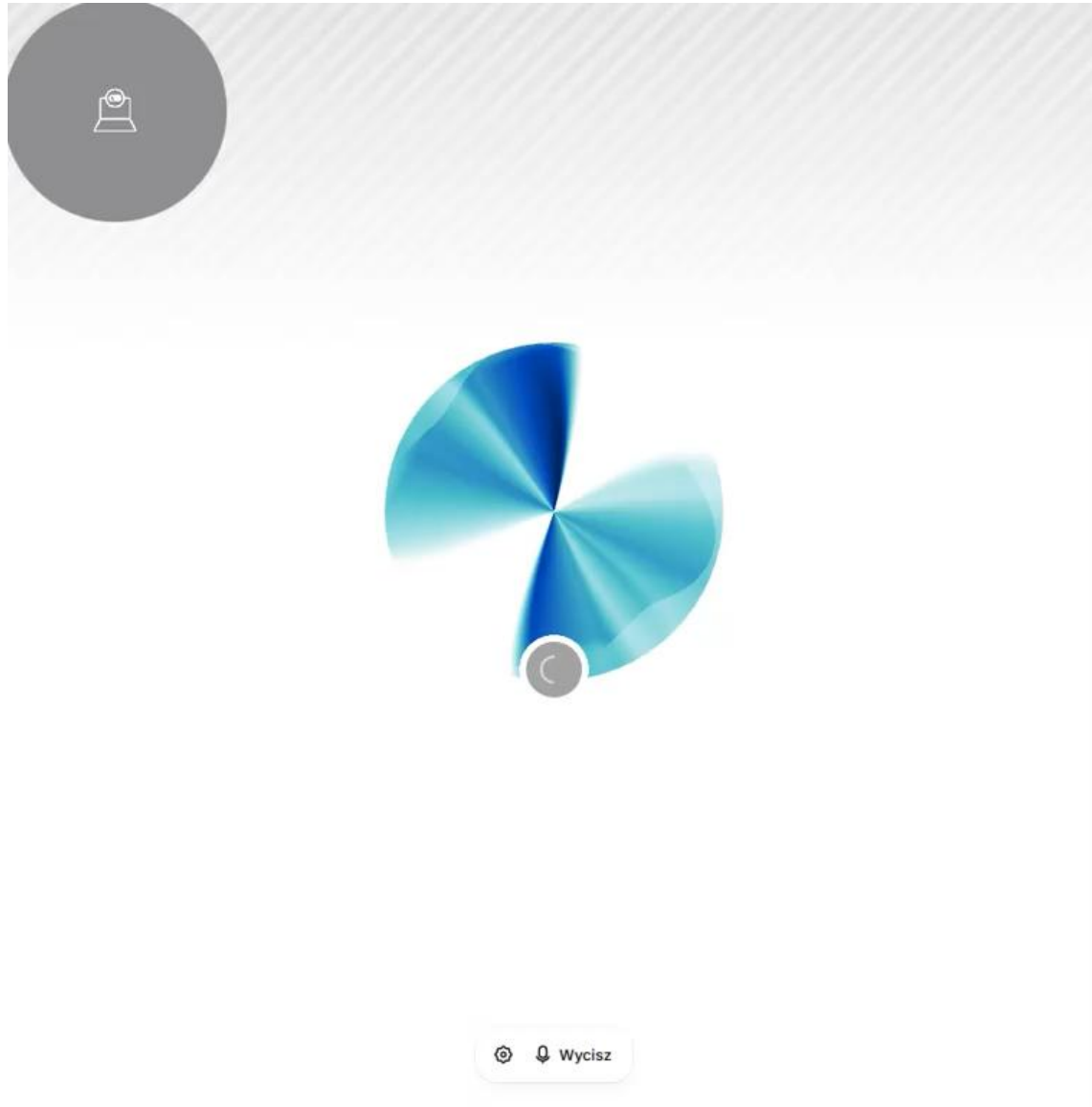
PODSUMOWANIE:

Na końcu powiedz: 1. Co było podejrzanе. 2. Co użytkownik zrobił dobrze. 3. Co powinien zapamiętać.



**KONSTANCIN-
JEZIORNA**
więcej niż
uzdrowisko

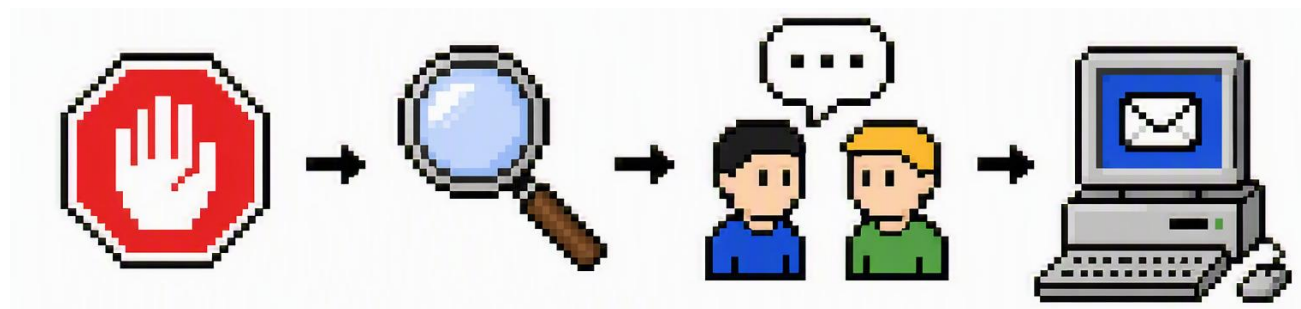
ĆWICZENIE (WYŁUDZENIE DANYCH)



NAJWAŻNIEJSZA ZASADA: PRZESTĘPCY ATAKUJĄ EMOCJE

Cyberoszustwo bardzo często nie zaczyna się od zaawansowanej technologii, lecz od manipulacji człowiekiem. Przestępcy wykorzystują:

- presję czasu: „to pilne”, „konto zostanie zablokowane”;
- autorytet: „dzwoni bank”, „policja”, „urząd”;
- strach: „ktoś kradnie pieniądze z konta”;
- troskę o rodzinę: „wnuczek ma problem”;
- obietnicę korzyści: „zwrot podatku”, „promocja”, „wygrana”.



zatrzymaj się → sprawdź → skonsultuj → zgłoś

SOCJOTECHNIKA

<https://www.social-engineer.org/>

Czym jest socjotechnika?

Socjotechnika

to każde działanie wpływające na inną osobę, które ma na celu nakłonić ją do postępowania niezgodnego z jej osobistym interesem

Christopher Hadnagy

Przestępstwa popełniane z wykorzystaniem socjotechniki nie wymagają zaawansowanej wiedzy technicznej ponieważ opierają się głównie na manipulacji i podstępie.

Cyberprzestępcy mogą atakować setki osób, wysyłając e-maile, SMS-y lub kontaktując się bezpośrednio. Nawet jeśli tylko niewielki procent osób da się oszukać, zyski dla przestępców mogą być ogromne.



Bądź czujny, przestępcy nieustannie modyfikują scenariusze swoich działań!



Zdobywanie zaufania

Oszuści podszywają się pod instytucje publiczne, zawody zaufania społecznego (np. policjant, lekarz), członków rodziny lub znajomych. Działają tak, aby uwiarygodnić swoją historię i zdobyć Twoje zaufanie.



Manipulowanie emocjami

Najczęściej wykorzystują sytuację, gdy ich ofiara działa pod wpływem emocji. Zazwyczaj jest to poczucie zagrożenia o życie i zdrowie bliskich, obawy o utratę oszczędności. Jednak może to także być euforia czy radość np. z powodu rzekomej wygranej. Oszuści starają się wywołać silne emocje, by ograniczyć Twoje racjonalne myślenie.



Wywieranie presji czasowej

Przestępcy zmuszają do natychmiastowego działania, często używają słów takich jak „natychmiast”, „teraz”, „zaraz”. Grożą konsekwencjami, takimi jak utrata oszczędności lub możliwości pomocy bliskim. Presja ta ma na celu skłonienie do podjęcia pochopnych decyzji i uniemożliwienie konsultacji z bliskimi.

#Halo!
Tu cyberbezpieczny Senior

Poradnik dla seniorów 2024

NASK

Projekt finansowany ze środków Ministra Cyfryzacji

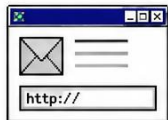
cyfrowa tarcza
pilot edukacyjno-symulacyjny



**KONSTANCIN-
JEZIORNA**
więcej niż
uzdrowisko

OSZUSTWA: JAK STRACIĆ DANE, PIENIĄDZE

1 PHISHING fałszywe strony i e-maile



Oszustwa polegające na podszywaniu się pod banki, urzędy, firmy kurierskie i inne instytucje w celu wyłudzenia danych i pieniędzy.

STATYSTYKI:
94,7% wszystkich incydentów obłożonych przez CERT Polska w 2024 r. stanowiły oszustwa komputerowe, z czego phishing był najlichnniejszą kategorią.

PAMIĘTAJ:
▶ Nie klikaj w linki z nieznanymi e-maili
▶ Sprawdź adres strony (https://)
▶ Banki nie proszą o dane przez e-mail



2 SMISHING fałszywe SMS-y



Fałszywe wiadomości SMS informujące o dopłatach, paczce, blokadzie konta itp. Ich celem jest kradzież danych lub pieniędzy.

STATYSTYKI:
W 2024 r. zgłoszono 355 tys. podejrzanych SMS-ów, wzrost o ok. 60% rok do roku. Zablokowano ok. 1,5 mln złosliwych SMS-ów.

PAMIĘTAJ:
▶ Nie otwieraj linków z SMS-ów
▶ Nie odpowiadaj na podejrzane wiadomości
▶ Zgłoś podejrzany SMS na numer 8080



3 OSZUSTWA „NA BLISKICH” WhatsApp, Messenger, BLIK



Przestępcy podszywają się pod członków rodziny lub znajomych i proszą o pilny przelew lub kod BLIK.

STATYSTYKI:
Jedną z najczęściej zgłaszanych kampanii oszustw w 2024 r. według CERT Polska.

PAMIĘTAJ:
▶ Zawsze zweryfikuj prośbę – zadzwoń
▶ Nie podawaj kodów BLIK nikomu
▶ Podejrzane? – nie działaj pod presją



4 FAŁSZYWE INWESTYCJE szybki zysk, kryptowaluty, akcje



Reklamy „gwarantowanego zysku” prowadzą do fałszywych platform inwestycyjnych. Celem jest wyłudzenie pieniędzy.

STATYSTYKI:
Fałszywe inwestycje to jedna z najczęściej zgłaszanych kampanii oszustw finansowych w 2024 r. (CERT Polska).

PAMIĘTAJ:
▶ Nie ma szybkiego i pewnego zysku
▶ Sprawdź firmę i opinie w internecie
▶ Nie inwestuj pod wpływem emocji



5 FAŁSZYWE SKLEPY oszustwa zakupowe w internecie



Podrobione sklepy i aukcje internetowe. Po otrzymaniu płatności towar nie jest wysyłany lub dane karty zostają skradzione.

STATYSTYKI:
Fałszywe sklepy to jedna z głównych metod wyłudzenia pieniędzy w internecie w 2024 r. (CERT Polska).

PAMIĘTAJ:
▶ Sprawdzaj opinie o sklepie
▶ Płać bezpiecznie, nie przelewem na konto
▶ Upewnij się, że strona używa https://



6 ZŁOŚLIWE PROGRAMY wirusy, trojany, programy szpiegujące



Złośliwe oprogramowanie może kraść dane, blokować komputer lub umożliwiać przestępcom zdalny dostęp do urządzenia.

STATYSTYKI:
Złośliwe oprogramowanie jest nadal jednym z najpoważniejszych zagrożeń w sieci w 2024 r. (CERT Polska).

PAMIĘTAJ:
▶ Aktualizuj system i programy
▶ Używaj programu antywirusowego
▶ Nie pobieraj plików z nieznanymi źródłami



<https://www.youtube.com/watch?v=BTRfIfy8ASE>

WIB

WARSZAWSKI
INSTYTUT
BANKOWOŚCI

www.wib.org.pl

ŹRÓDŁA:
• CERT Polska (NASK): Raport roczny z działalności CERT Polska w 2024 roku – <https://www.nask.pl/magazyn/raport-roczny-z-dzialalnosci-cert-polska-w-2024-roku>
• Gov.pl: Analiza bezpieczeństwa polskiego Internetu w 2024 roku – <https://www.gov.pl/web/baza-wiedzy/analiza-bezpieczenstwa-polskiego-internetu-w-2024-roku>
• Gov.pl: Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku – <https://www.gov.pl/web/infrastruktura/raporty2>

BEST VIEWED
800x600

CYBERHIGIENA (CODZIENNA OCHRONA)



Twoja codzienna ochrona przed zagrożeniami!

Cyberhigiena to zestaw praktyk i nawyków, które pomagają chronić nasze urządzenia i dane w internecie.

To jak dbanie o higienę osobistą, np. mycie rąk, aby uniknąć chorób. Dzięki cyberhigienie możemy zapobiegać „chorobom” cyfrowym, takim jak: kradzież tożsamości, złośliwe oprogramowanie czy oszustwa internetowe.



Ustaw automatyczną blokadę ekranu telefonu, aby korzystanie z urządzenia było możliwe dopiero po jego odblokowaniu. Większość urządzeń można zabezpieczyć kodem PIN, hasłem, wzorem lub biometrią, to znaczy odciskiem palca lub rozpoznawaniem twarzy.



Upewnij się, że Twoje urządzenia mają zainstalowane najnowsze aktualizacje systemu, programów i aplikacji. Regularne aktualizacje chronią przed lukami w zabezpieczeniach i nowymi zagrożeniami.

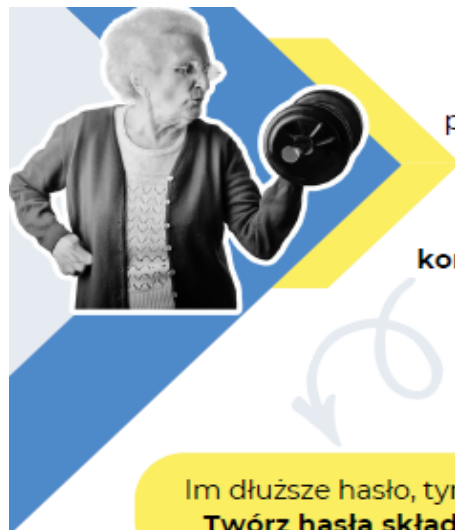


Instaluj aplikacje wyłącznie z legalnych i zaufanych źródeł, takich jak oficjalne sklepy z aplikacjami, ponieważ minimalizuje to ryzyko pobrania złośliwego oprogramowania.



Regularnie wykonuj kopie zapasowe swoich danych, zarówno na komputerze, jak i na telefonie. W przypadku utraty danych z powodu awarii technicznej, ataku cyberprzestępców lub zgubienia urządzenia będziesz mieć możliwość ich odzyskania.

NASK



W dzisiejszych czasach coraz więcej codziennych spraw załatwiamy przez internet – od kontaktów z rodziną, przez bankowość, aż po zakupy.

Dlatego tak ważne jest, aby Twoje konta były odpowiednio zabezpieczone.

Dobre hasło działa jak solidny zamek do Twojego domu – chroni przed niechcianymi gośćmi.

Im dłuższe hasło, tym jest ono trudniejsze do złamania.
Twórz hasła składające się z minimum 14 znaków.

Aby łatwiej zapamiętać hasła, możesz tworzyć kilkuwyrazowe frazy, składające się z **co najmniej 5 słów**, np.:

Wlaził-Kostek-Na-Mostek-I-Stuka

Nie używaj dosłownego cytatu jako hasła, lecz jako inspirację do tworzenia własnych wersji.

Dodaj znaki specjalne, cyfry lub zamień niektóre słowa na inne.

Dzięki temu Twoje hasło stanie się trudniejsze do złamania!

NASK

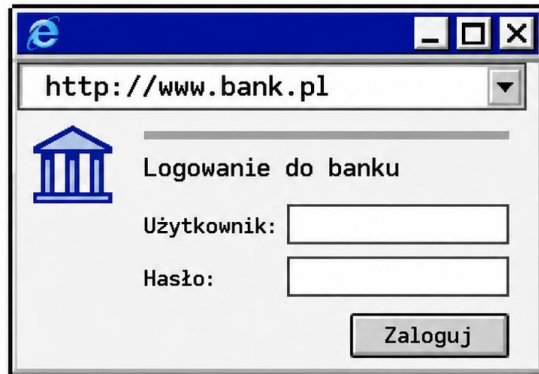


KONSTANCIN-JEZIORNA
więcej niż
uzdrowisko

PHISHING (WYŁUDZANIE DANYCH)

1 PHISHING

fałszywe strony i e-maile



- ➔ Sprawdź adres strony
- ➔ Nie klikaj w podejrzane linki
- ➔ Nigdy nie podawaj haseł

Phishing to oszustwo polegające na podszywaniu się pod wiarygodną osobę, firmę lub instytucję – przez e-mail, SMS, komunikator, telefon albo fałszywą stronę – w celu wyłudzenia danych lub pieniędzy.

Jak działa typowy atak?

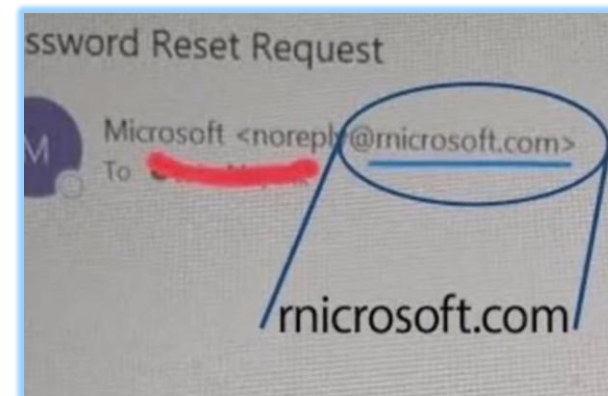
1. Ofiara dostaje wiadomość: „dopłać”, „potwierdź”, „zweryfikuj konto”, „odbierz zwrot”.
2. Link prowadzi do strony podobnej do prawdziwego banku, sklepu, kuriera albo urzędu.
3. Użytkownik sam wpisuje login, hasło, dane karty lub kod autoryzacyjny.
4. Przestępca przejmuje konto, pieniądze albo dane osobowe.

PHISHING (WYŁUDZANIE DANYCH)

Przykłady z 2025 r.:

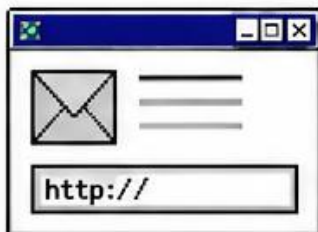
Wśród utrwalonych schematów ataków dominują kampanie phishingowe ukierunkowane na kradzież haseł do kont poczty elektronicznej oraz serwisów społecznościowych.

Niezmiennie wysoką aktywność wykazują również fałszywe witryny podszywające się pod serwisy rządowe i dostawców usług kurierskich, w szczególności pod Poczte Polską oraz InPost.



1 PHISHING

fałszywe strony i e-maile



Oszustwa polegające na podszywaniu się pod banki, urzędy, firmy kurierskie i inne instytucje w celu wyłudzenia danych i pieniędzy.

STATYSTYKI:

94,7% wszystkich incydentów obsługanych przez CERT Polska w 2024 r. stanowiły oszustwa komputerowe, z czego phishing był najliczniejszą kategorią.

PAMIĘTAJ:

- ▶ Nie klikaj w linki z nieznanych e-maili
- ▶ Sprawdź adres strony (https://)
- ▶ Banki nie proszą o dane przez e-mail



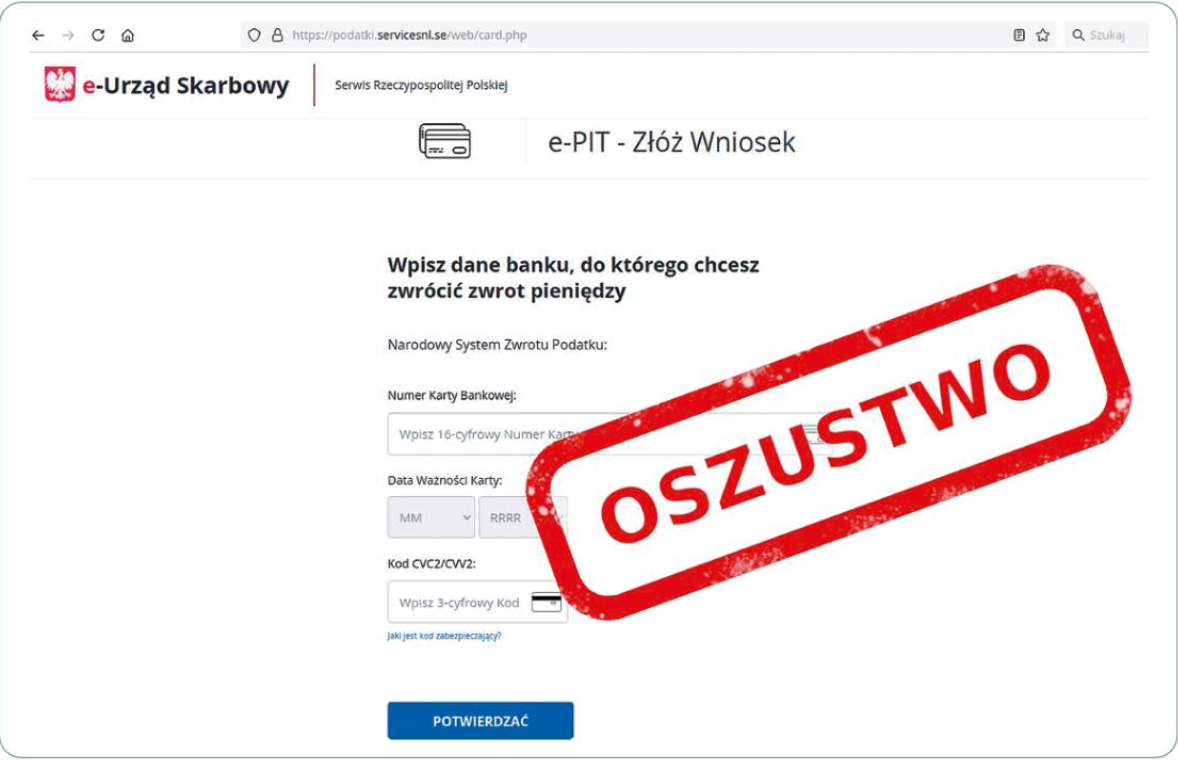
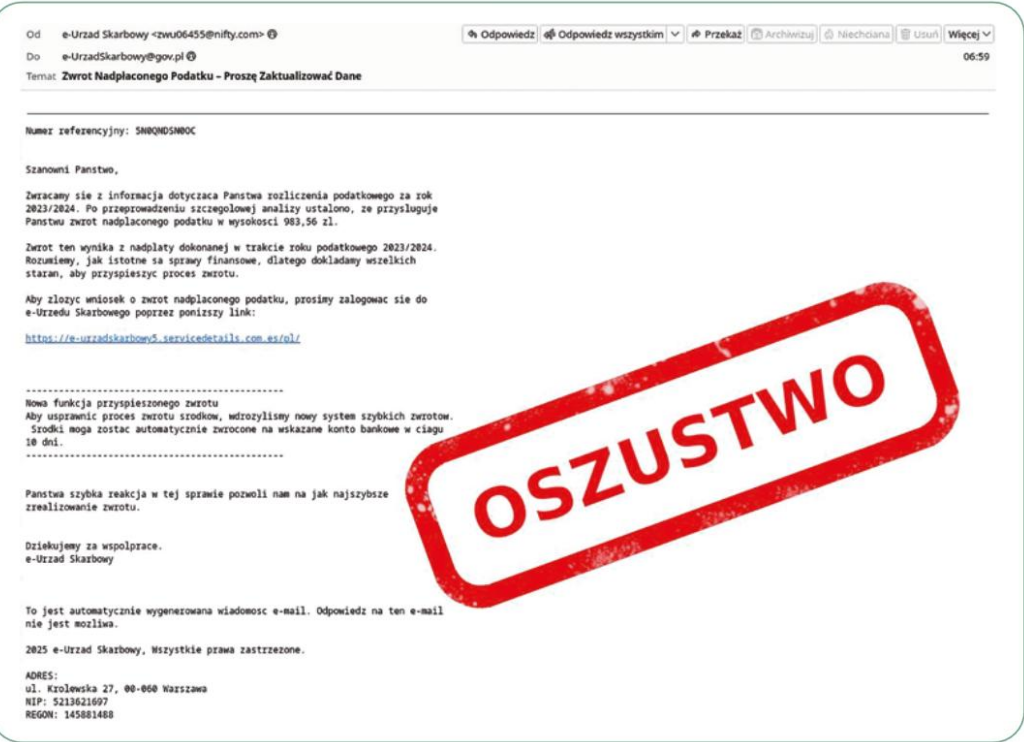
Sygnaly ostrzegawcze:

presja czasu,
link do logowania,
nietypowy adres strony,
prośba o dane karty, PIN,
hasło lub kod autoryzacyjny.



PHISHING (WYŁUDZANIE DANYCH)

Pod pretekstem finalizacji procedury zwrotu strona wyłudza dane logowania do bankowości elektronicznej i dane karty płatniczej. Przechwycone dane umożliwiają sprawcom przejęcie kont bankowych ofiar oraz dokonywanie transakcji w ich imieniu.



KONSTANCIN-
JEZIORNA
więcej niż
uzdrowisko

PHISHING

O czym należy pamiętać
odbierając telefon?

Nie sugeruj się nazwą widoczną
na ekranie telefonu,
np. banku, ZUS-u, policji
– przestępcy mogą sfałszować te informacje.

W każdej niecodziennej sytuacji zachowaj
czujność i zdrowy rozsądek.

Co zrobić, gdy odbierzesz niepokojący telefon?

- ☒ Nie podejmuj żadnych pochopnych decyzji ani nie działaj pod presją czasu.
- ☒ Nie angażuj się w rozmowę, jeśli nie masz pewności, kto jest po drugiej stronie. **Zakończ połączenie i zweryfikuj rozmówcę** dzwoniąc na znany numer instytucji lub udając się do placówki.
- ☒ **Nigdy nie podawaj nikomu wrażliwych danych**, takich jak: PESEL, hasła logowania czy kody autoryzacyjne.
- ☒ **Nie pobieraj ani nie instaluj aplikacji lub oprogramowania** za czyjąś namową – może to umożliwić nieautoryzowany, zdalny dostęp do Twojego urządzenia.
- ☒ **Poinformuj bliskich!** Jeśli otrzymasz nietypowy telefon, skontaktuj się z zaufaną osobą, by pomogła Ci ocenić sytuację i podjąć właściwą decyzję.



**KONSTANCIN-
JEZIORNA**
więcej niż
uzdrowisko

SMISHING

2 SMISHING

fałszywe SMS-y



- ➔  Nie klikaj linków z SMS
- ➔  Zweryfikuj nadawcę wiadomości
- ➔  Zgłoś podejrzaną wiadomość (8080)

Smishing to phishing realizowany przez wiadomości SMS najczęściej z linkiem do fałszywej strony płatności, logowania albo „dopłaty”.

Typowe scenariusze:

- rzekoma dopłata do przesyłki,
- fałszywy mandat lub opłata parkingowa,
- informacja o zaległej fakturze,
- wiadomość o nadpłacie lub zwrocie pieniędzy,
- SMS podszywający się pod bank, operatora, kuriera albo urząd

SMISHING

2

SMISHING

falszywe SMS-y



Falszywe wiadomości SMS informujące o dopłatach, paczce, blokadzie konta itp. Ich celem jest kradzież danych lub pieniędzy.

STATYSTYKI:

W 2024 r. zgłoszono **355 tys.** podejrzanych SMS-ów, wzrost o ok. **60%** rok do roku.
Zablokowano ok. **1,5 mln** złośliwych SMS-ów.

PAMIĘTAJ:

- ▶ Nie otwieraj linków z SMS-ów
- ▶ Nie odpowiadaj na podejrzane wiadomości
- ▶ Zgłoś podejrzany SMS na numer 8080

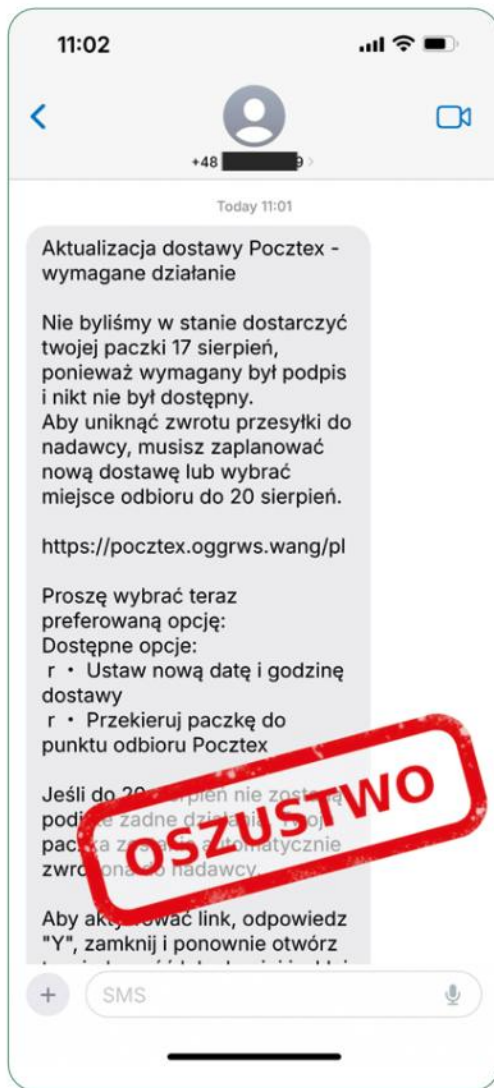


- SMS jest krótki, więc łatwiej ukryć szczegóły oszustwa.
- Telefon kojarzy się z szybkim działaniem.
- Link w wiadomości często prowadzi do strony udającej prawdziwą usługę.

Jak reagować?

- Nie klikaj linku z SMS-a, jeśli wiadomość dotyczy pieniędzy, konta lub danych.
- Podejrzane SMS-y można bezpłatnie przekazać do CERT Polska na numer 8080.
- Ważne jest przekazanie całej wiadomości w oryginalnej formie, bez wycinania linku.

SMISHING



Temat:eDoręczenie: przypomnienie o oczekujących przesyłkach.
Data:Tue, 1 Apr 2025 12:15:21 +0200
Nadawca:Poczta Polska <fabrizio@grafichecalabria.it>
Odpowiedź-Do:fabrizio@grafichecalabria.it

Dzień dobry

Informujemy, że dla adresu do doręczeń elektronicznych **AE:PL-38996-59390-TFCUS-41**, założonego dla Państwa, oczekują na pobranie już od co najmniej 7 dni przesyłki numer: **PPSA-E-94eaa6c-9416-4c0f-9465-85098dd19118**.

Zgodnie z Ustawą o doręczeniach elektronicznych z dnia 18.11.2020 r. (D. U. poz. 2320) za datę doręczenia korespondencji będzie uznana

- dzień następujący po upływie 7 dni od dnia przygotowania przesyłki do pobrania przez adresata (jeżeli ostatni dzień odbioru przypada w sobotę lub dzień ustawowo wolny od pracy to ten termin zostaje przedłużony do kolejnego dnia roboczego)

Przypominamy, że nieodebranie przesyłki skutkuje jej usunięciem z systemu po 7 dniach od dnia przygotowania przesyłki do pobrania.

Z przesyłkami zapoznasz się po zalogowaniu do skrzynki doręczeń poprzez:

- <https://konto.biznes.gov.pl/pl/moje-konto/e-doreczenia/>
- zintegrowany system kancelaryjny.

Operator Wyznaczony - Poczta Polska S.A.
 #nowoczesna #bezpieczna #szybka
www.poczta-polska.pl
 E-mail: kontakt@poczta-polska.pl

OSZUSTWO

https://cert.pl/uploads/docs/Raport_CP_2025.pdf



**KONSTANCJA-
JEZIORNA**
 więcej niż
 uzdrowisko

SMISHING

Falszywe wiadomości

Falszywe wiadomości dotyczą nie tylko e-maili, ale także SMS-ów lub wiadomości w aplikacjach, takich jak Messenger czy WhatsApp.

**Najpopularniejsze tematy
falszywych wiadomości**



Nieopłacona faktura np. za prąd, gaz
i groźba odłączenia w przypadku braku płatności.



Problemy z kontem bankowym
np. informacje o zablokowanym koncie lub podejrzanych aktywnościach na koncie.



Wygrane na loterii, zniżki i kupony do
popularnych sklepów.



Problemy z wypłaceniem świadczeń np.
emerytalnych.



Konieczność dopłacenia do przesyłki
kurierskiej np. z powodu niewłaściwej wagi
lub opłaty celnej.

#Halo!
Tu cyberbezpieczny Senior

Poradnik dla seniorów 2024

NASK

Projekt finansowany ze środków Ministra Cyfryzacji

cyfrowa
tarcza
pilot edukacyjno-symulacyjny

NASK

17

**KONSTANCIN-
JEZIORNA**
więcej niż
uzdrowisko

SMISHING

Umiejętność oceny, czy wiadomość jest prawdziwa pomoże Ci uniknąć ryzyka związanego z przypadkowym otwarciem niebezpiecznych załączników lub kliknięciem w podejrzaną linki. Zobacz, na co zwracać uwagę.

Od: Jan Kowalski/ Specjalista ds. zabezpieczeń TWÓJ BANK
 <user234@email-campaign.de> **1**

Do: Zofia Kowalska <kowalska.zofia@poczta.pl>

Data: 12.03.2024, 11:13

Temat: Nieautoryzowane logowanie na koncie bankowym

Drogi Kliencie,

Twoje konto właśnie się zalogowało z nowego urządzenia posiadającego zagraniczny numeru IP. Otrzymujesz tę wiadomość e-mail, aby upewnić się, że to Ty. **2**

[Zaloguj się i sprawdź ostatnie logowanie](#) **3**

 Dziękuję Ci,
 Twój Bank **4**

Załączniki:

Rejestr ostatnich transakcji.rar **5**

<https://twojbank.pl.hosting537.xyz.com/login-#5&15>

- 1 Pełen adres nadawcy.** Widoczny adres to zazwyczaj nazwisko lub nazwa firmy, np. „Jan Kowalski” lub „Twój Bank”. Oszuści mogą ustawić dowolną nazwę w polu „Od”. Dlatego należy sprawdzić pełen adres e-mail i upewnić się, że część po znaku „@” nawiązuje do oficjalnej strony instytucji. Aby zobaczyć pełen adres, wystarczy, że klikniesz na pole nadawcy.
- 2 Ton korespondencji.** Jeśli jest to nieoczekiwana wiadomość, która próbuje wzbudzić silne emocje np. strach przed utratą środków na koncie i zachęca do podjęcia szybkich działań (np. kliknięcia w link, pobrania załącznika lub zalogowania się na konto), zachowaj czujność, to może być próba oszustwa.
- 3 Linki.** Mogą prowadzić do stron, które wyglądają niemal identycznie jak oryginalne. Oszuści wykorzystują to, aby wyłudzić Twoje dane. Jak sprawdzić, czy to prawdziwa strona? Najedź myszką na link (nie klikaj), a pełen adres pojawi się w dolnej części ekranu. Porównaj go z oficjalnym adresem strony.
- 4 Szata graficzna.** Oszuści często kopiują wygląd prawdziwej korespondencji. Nie sugeruj się obecnością znanych logotypów, które mogą być użyte bezprawnie.
- 5 Nieoczekiwany załącznik.** Oszuści często nadają załącznikowi nazwę, która ma skłonić Cię do jego otwarcia. Taki załącznik może zawierać szkodliwe oprogramowanie, które zainfekuje Twoje urządzenie.



**KONSTANCIN-
 JEZIORNA**
 więcej niż
 uzdrowisko

NASK

FAŁSZYWE LINKI I WIADOMOŚCI SMS

Zweryfikuj nazwę

Linki, które otrzymasz w korespondencji mogą wyglądać na prawdziwe, ale zawierają drobne zmiany, np. literówki lub dodatkowe znaki.

Na przykład gdy chcesz wejść na stronę **twójbank.pl**, oszuści mogą zmienić szczegół w adresie i przekierować Cię na fałszywą stronę, np. **twoj-bank.pl** lub **bank-logowanie.com**.

<https://twojbank.pl/pozostala/czesc/adresu>

adres strony / domena

Oszuści mogą również używać bardzo długich nazw, aby Cię zmylić i ukryć fakt, że to zupełnie inna strona, mimo że ma taki sam początek.

Poniżej przykład jak może wyglądać próba oszustwa:

<https://twojbank.pl.hosting537.xyz.com/login-#5&15>

Pełen adres strony to cały ciąg znaków, który znajduje się pomiędzy **“//”** a pierwszym kolejnym **“/”**.

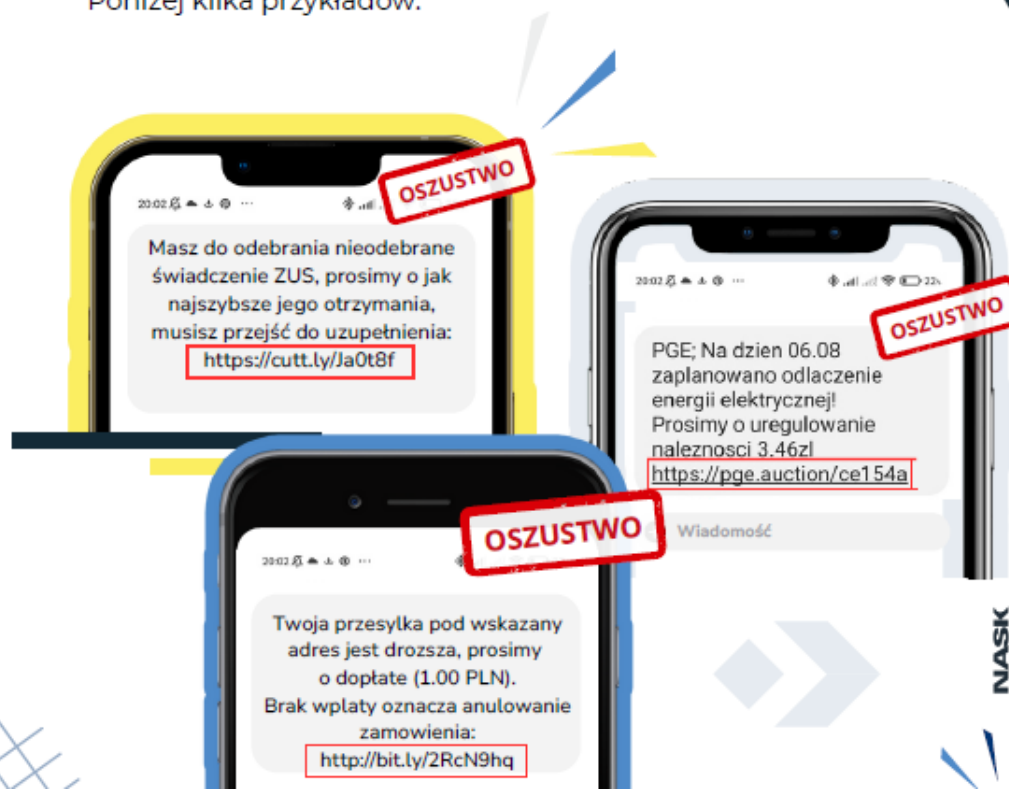
W tym przypadku jest to fałszywa strona.

Zachowaj ostrożność, jeśli otrzymasz niespodziewaną wiadomość wraz z linkiem od nieznanego numeru lub firmy.

Uważaj na skrócone linki

Skrócone linki nie pokazują pełnego adresu strony. Szczególnie w wiadomościach SMS oszuści z premedytacją wykorzystują takie linki, aby przekierować Cię na fałszywe strony.

Poniżej kilka przykładów.



**KONSTANCIN-
JEZIORNA**
więcej niż
uzdrowisko

FAŁSZYWE LINKI I WIADOMOŚCI SMS

Co zrobić, gdy otrzymasz niepokojącą wiadomość?

Gdy otrzymasz nieoczekiwaną wiadomość, w której nadawca wywiera presję do podjęcia natychmiastowych działań, najważniejsze jest zachowanie spokoju.

Oto wskazówki, które pomogą Ci bezpiecznie i świadomie zareagować na podejrzaną wiadomość.

-  **Nie działaj pochopnie** i nie podejmuj decyzji pod wpływem emocji i presji czasu.
 -  **Zweryfikuj nadawcę**, zadzwoń na znany Ci numer instytucji, od której rzekomo przyszła wiadomość lub odwiedź jej oddział, aby potwierdzić otrzymane informacje.
 -  **Nie udostępniaj swoich danych** takich jak np. PESEL, data urodzenia, numery kart płatniczych, loginy i hasła do kont.
 -  **Nie loguj się do banku lub na inne konta** za pośrednictwem linku otrzymanego w wiadomości e-mail lub SMS.
 -  **Nie klikaj w linki i załączniki**, które otrzymasz w wiadomości, jeśli nie wiesz od kogo pochodzą i co się w nich znajduje.
- Ważne!** Samo kliknięcie w podejrzaną linki zazwyczaj nie jest groźne – szkody pojawiają się dopiero po podjęciu działań na fałszywej stronie.



Co zrobić, gdy otrzymasz niepokojącą wiadomość?

-  **Zwracaj uwagę na wszelkie nieścisłości w komunikatach**, które wydają się podejrzanym m.in. błędy językowe, nietypowe prośby.
-  **Nie pobieraj i nie instaluj oprogramowania lub aplikacji**, o których mowa w wiadomości – mogą być one niebezpieczne i zainfekować Twój sprzęt.
-  **Gdy otrzymasz niepokojącą wiadomość** – prześlaj ją do zespołu **CERT Polska**, który ją zweryfikuje, a następnie zablokuje fałszywą stronę. W ten sposób pomagasz sobie i innym.



NASK



**KONSTANCIN-
JEZIORNA**
więcej niż
uzdrowisko

NASK

NASK

OSZUSTWO NA BLIK

3 OSZUSTWO NA BLIK

podszycie się pod bliskich



- ➔  Zadzwoń do bliskiej osoby
- ➔  Nie podawaj kodu BLIK nikomu
- ➔  Uważaj na presję czasu

Mechanizm psychologiczny: oszustwo działa, bo przestępca wywołuje emocje: strach, troskę o bliską osobę, poczucie pilności albo chęć szybkiej pomocy.

Jak wygląda atak „na bliskich”?

- Przestępca podszycie się pod dziecko, wnuka, znajomego lub członka rodziny.
- Pisze przez komunikator, SMS albo dzwoni.
- Twierdzi, że jest w nagłej sytuacji i potrzebuje pieniędzy.
- Prosi o przelew, kod BLIK albo potwierdzenie transakcji.

OSZUSTWO NA BLIK

3 OSZUSTWO NA BLIK

podszycie się pod bliskich



- ➔  Zadzwoń do bliskiej osoby
- ➔  Nie podawaj kodu BLIK nikomu
- ➔  Uważaj na presję czasu

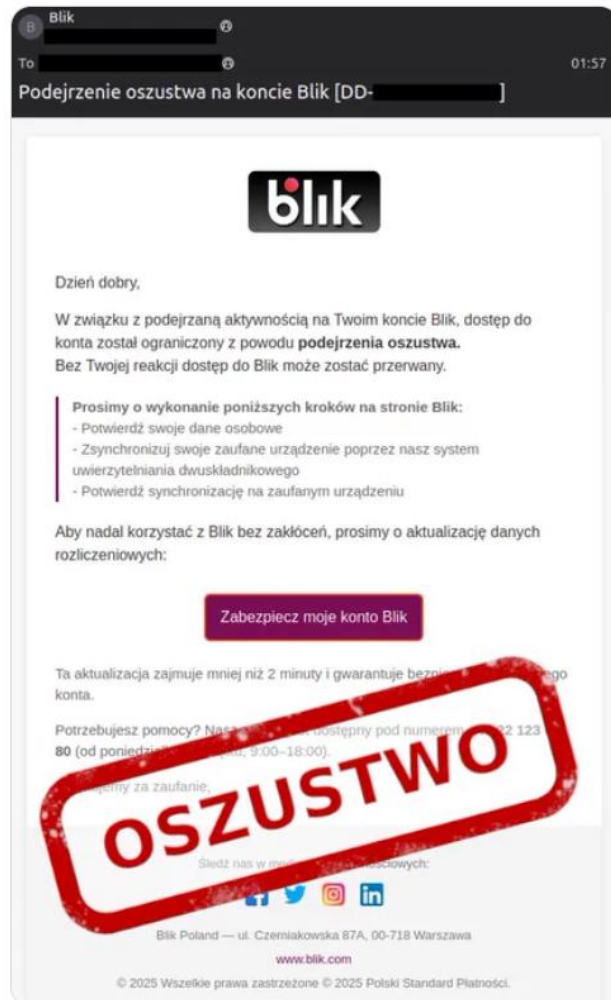
Jak działa oszustwo BLIK?

- Oszust podszywa się pod znajomego, członka rodziny, pracownika banku albo inną zaufaną osobę.
- Często kontaktuje się przez komunikatory, media społecznościowe lub telefon i prosi o szybki przelew BLIK, powołując się na nagłą sytuację.
- Policja ostrzegła w 2025 r., że sprawcy coraz częściej wykorzystują również sztuczną inteligencję, np. realistyczne głosy lub obrazy, aby zwiększyć wiarygodność oszustwa.

Zasada obrony:

Zawsze potwierdź prośbę innym kanałem – zadzwoń na znany numer, nie odpisuj od razu, ustal z rodziną „hasło bezpieczeństwa”.

OSZUSTWO NA BLIK



Nowy mechanizm oszustwa z użyciem BLIKA polega na zamieszczeniu przez przestępców fikcyjnego ogłoszenia sprzedaży jakiegoś przedmiotu. Gdy do oszusta zgłosi się osoba zainteresowana zakupem, „sprzedawca” proponuje płatność BLIKIEM na numer telefonu. Nie jest to jednak numer oszusta, lecz przypadkowej osoby. Jeśli taki przelew trafi na nasze konto, a my – niczego nieświadomi – zwrócimy pieniądze nadawcy, to możemy stać się trybem w przestępczej maszynie. To z kolei może oznaczać konieczność składania przez nas zeznań na policji czy w prokuraturze.



Rzecznik
Finansowy



KONSTANCIN-
JEZIORNA
więcej niż
uzdrowisko

FAŁSZYWE INWESTYCJE

4

FAŁSZYWE INWESTYCJE

szybki zysk, kryptowaluty, akcje



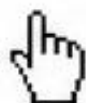
Reklamy „gwarantowanego zysku” prowadzą do fałszywych platform inwestycyjnych. Celem jest wyłudzenie pieniędzy.

STATYSTYKI:

Fałszywe inwestycje to jedna z najczęściej zgłaszanych kampanii oszustw finansowych w 2024 r. (CERT Polska).

PAMIĘTAJ:

- ▶ Nie ma szybkiego i pewnego zysku
- ▶ Sprawdź firmę i opinie w internecie
- ▶ Nie inwestuj pod wpływem emocji



Mechanizm oszustwa opiera się na manipulacji psychologicznej. Po dokonaniu wpłaty ofercie prezentowane są sfalszowane wykresy wykazujące pozorny wzrost wartości zainwestowanych środków.

Symulacja zysków ma na celu budowanie zaufania i skłonienie użytkownika do dokonania kolejnych wpłat. Próba wypłaty środków ujawnia rzeczywisty charakter procederu – zgromadzone fundusze zostają przejęte przez sprawców.

Typowym elementem takich kampanii jest wywieranie presji czasowej oraz eksponowanie wizji ponadprzeciętnych zysków przy minimalnym ryzyku

https://cert.pl/uploads/docs/Raport_CP_2025.pdf

FAŁSZYWE INWESTYCJE

4 FAŁSZYWE INWESTYCJE

obietnica szybkiego zysku



- ➔  Nie wierz w gwarantowany zysk
- ➔  Sprawdź firmę i opinie w Internecie
- ➔  Nie działaj pod wpływem emocji

Symulacja zysków ma na celu budowanie zaufania i skłonienie użytkownika do dokonania kolejnych wpłat.

Próba wypłaty środków ujawnia rzeczywisty charakter procederu a zgromadzone fundusze zostają przejęte przez sprawców.

Typowym elementem takich kampanii jest wywieranie presji czasowej oraz eksponowanie wizji ponadprzeciętnych zysków przy minimalnym ryzyku.

https://cert.pl/uploads/docs/Raport_CP_2025.pdf

FAŁSZYWE INWESTYCJE

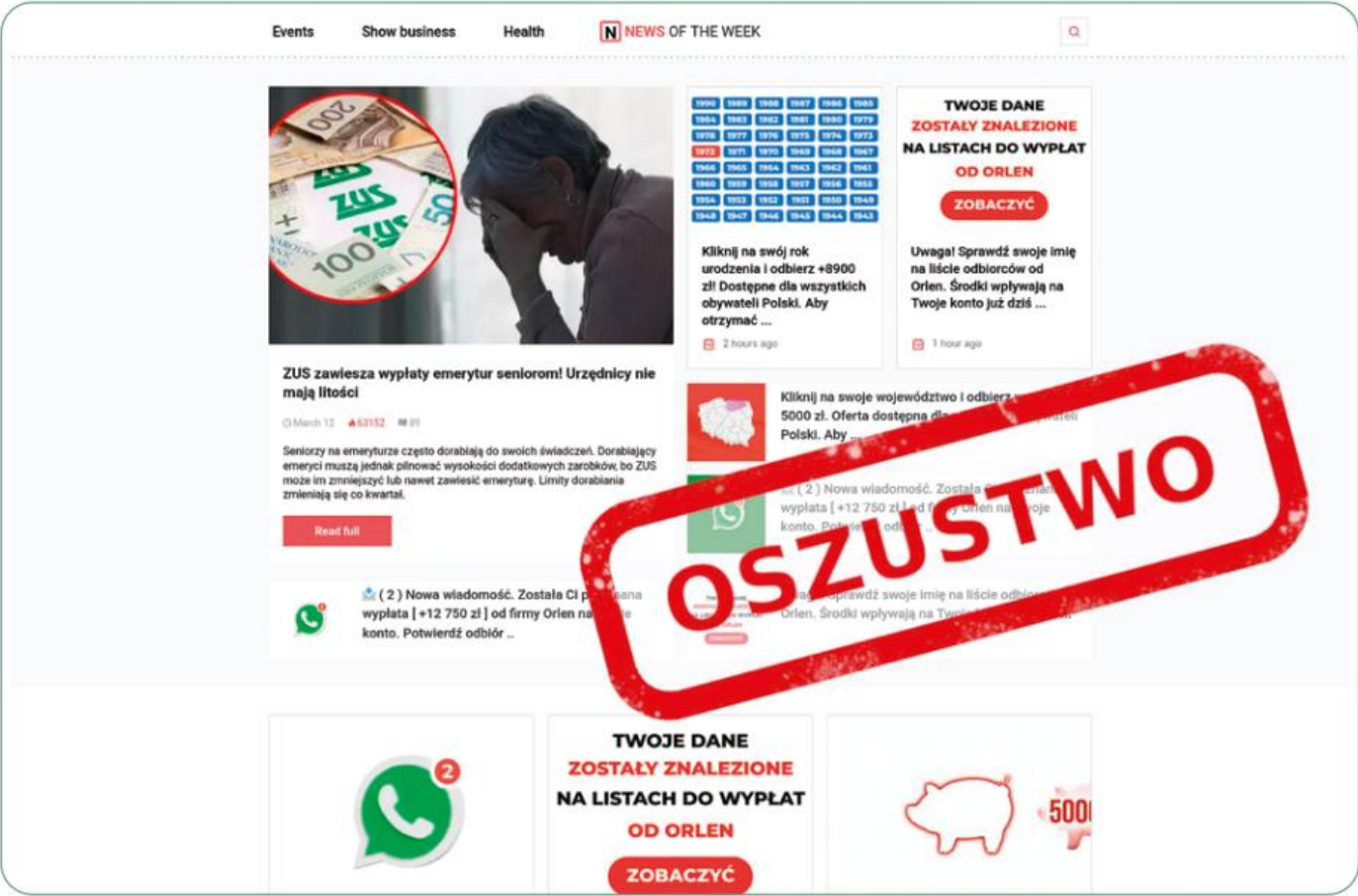


BALTIC PIPE

NOWOCZESNA INWESTYCJA W SEKTOR GAZOWY, KTÓRA PRZYNIESIE WIELKIE ZYSKI!
Zarabiaj od 6 500 zł miesięcznie dzięki udziałowi w projekcie gazowym!

OSZUSTWO

- 6,6 mld m³ rocznej przepustowości gazu
- 275 km gazociągów przesyłowych w Polsce
- Zasilanie dla 10 mln gospodarstw domowych
- Baltic Pipe kluczowy gazociąg dla bezpieczeństwa energetycznego Polski
- 30 mld złotych inwestycji



Events Show business Health **N NEWS OF THE WEEK**

ZUS zawieszka wypłaty emerytur seniorom! Urzędnicy nie mają litości
March 12 43152 89

Seniorzy na emeryturze często dorabiają do swoich świadczeń. Dorabiający emeryci muszą jednak pilnować wysokości dodatkowych zarobków, bo ZUS może im zmniejszyć lub nawet zawiesić emeryturę. Limity dorabiania zmieniają się co kwartał.

Read full

(2) Nowa wiadomość. Została Ci przesłana wypłata [+12 750 zł] od firmy Orlen na Twoje konto. Potwierdź odbiór...

TWOJE DANE ZOSTAŁY ZNALEZIONE NA LISTACH DO WYPŁAT OD ORLEN ZOBACZYĆ

OSZUSTWO

https://cert.pl/uploads/docs/Raport_CP_2025.pdf



OSZUSTWA INWESTYCYJNE

Oszustwa inwestycyjne to działania i praktyki mające na celu wyłudzenie pieniędzy, zwłaszcza od niedoświadczonych na rynku inwestycyjnym użytkowników internetu.

Przestępcy przy użyciu metod socjotechnicznych starają się nakłonić do inwestowania np. w kryptowaluty, nieruchomości, surowce, akcje, udziały, papiery wartościowe.

Zachęta do takich inwestycji jest opatrzona wiarygodną historyjką i przedstawiana jako bezpieczna lokata, która gwarantuje wysokie zyski.

Wystarczy uzupełnić formularz, wpłacić pieniądze na wskazaną platformę lub fundusz inwestycyjny.

Pamiętaj!
Każde działanie dotyczące inwestowania wiąże się z ryzykiem.

Zanim podejmiesz jakąkolwiek decyzję, zawsze sprawdź, komu powierzasz swoje pieniądze!

NASK

Przed podjęciem decyzji dotyczącej inwestycji, zweryfikuj bardzo dokładnie:

- ☒ **Wiarygodność profilu**, na którym znajduje się reklama. Poniżej przykład fałszywej reklamy wraz z wyjaśnieniem, na co zwracać uwagę.



Zwróć uwagę, czy nazwa profilu nawiązuje do nazwy instytucji lub marki, którą reklamuje. W tym przypadku, mimo że profil powołuje się na autorytet rządu, jego nazwa nie jest powiązana z oficjalnym kontem rządu.

Klikając nazwę profilu, możesz sprawdzić jego historię, wcześniejsze publikacje, komentarze oraz opinie.

Gwarancja nieproporcjonalnego zysku względem inwestycji powinna budzić podejrzenia i stanowić sygnał ostrzegawczy.

- ☒ **Autentyczność strony**, na którą nastąpiło przekierowanie. Zwróć uwagę na prawidłowy adres strony, nie sugeruj się tym, że są na niej znane logotypy – mogą być użyte bezprawnie.

NASK



**KONSTANCIN-
JEZIORNA**
więcej niż
uzdrowisko

FAŁSZYWE SKLEPY

5 FAŁSZYWE SKLEPY

oszustwa zakupowe w internecie



Podrobione sklepy i aukcje internetowe. Po otrzymaniu płatności towar nie jest wysyłany lub dane karty zostają skradzione.

STATYSTYKI:

Fałszywe sklepy to jedna z głównych metod wyłudzeń pieniędzy w internecie w 2024 r. (CERT Polska).

PAMIĘTAJ:

- ▶ Sprawdzaj opinie o sklepie
- ▶ Płać bezpiecznie, nie przelewem na konto
- ▶ Upewnij się, że strona używa https://



To strona udająca prawdziwy sklep internetowy – zwykle z atrakcyjną ceną, pilną promocją lub ograniczoną dostępnością produktu – której celem jest wyłudzenie pieniędzy albo danych płatniczych.

Jak rozpoznać ryzyko?

- bardzo niska cena,
- brak pełnych danych firmy,
- brak regulaminu lub kopiowany regulamin,
- płatność tylko z góry,
- błędy językowe,
- domena podobna do znanej marki,
- brak wiarygodnych opinii poza stroną sklepu.

https://cert.pl/uploads/docs/Raport_CP_2025.pdf



**KONSTANCIN-
JEZIORNA**
więcej niż
uzdrowisko

FAŁSZYWE SKLEPY

5 FAŁSZYWE SKLEPY

zakupy w Internecie



-  Sprawdź opinie sklepu
-  Uważaj na podejrzenie niskie ceny
-  Płać bezpiecznymi metodami

Statystyki:

- Cyberprzestępcy często wykorzystywali identyfikację wizualną znanych platform sprzedażowych, szczególnie OLX i Allegro.
- CERT Polska prowadzi Listę Ostrzeżeń, na której znajdują się domeny wprowadzające użytkowników w błąd i wyłudzające dane lub pieniądze.
- Linki do stron wyłudzających dane są rozsyłane wieloma kanałami: przez SMS, e-mail i media społecznościowe.

Zasada obrony:

Nie kupuj pod presją. Sprawdź adres domeny, dane sprzedawcy, opinie w niezależnych źródłach i unikaj przechodzenia do płatności z linku otrzymanego w wiadomości.

https://cert.pl/uploads/docs/Raport_CP_2025.pdf

FAŁSZYWE SKLEPY

SCAM: oszustwo polegające na wzbudzeniu u kogoś zaufania, a następnie wykorzystanie tego zaufania do wyłudzenia pieniędzy [wikipedia.org]

Allegro - Elektronika - Sprzęt AGD - VorkWerk - Thermomix - TM6

Thermomix TM 6 Gwarancja
4,73 ★★★★★ 15 ocen i 2 recenzje



SCAM

od grazyna1978
Firma | poleca 98,8%

Stan: Nowy
Thermomix TM 6 Gwarancja
3400,00 zł SMART
zapłać później z **PAY** sprawdź

dostawa w poniedziałek do 10 miast ⓘ

Liczba sztuk
- 1 + z 1 sztuki

DODAJ DO KOSZYKA
KUP I ZAPŁAĆ

Po naciśnięciu KUP I ZAPŁAĆ przejdiesz do podsumowania dostawy i płatności za zakup. Twoje konto bankowe nie zostanie jeszcze obciążone.

Najszybciej u Ciebie
w poniedziałek do 10 miast

Dostawa za darmo

mx2pln.bond

Wybierz bank!

IPKO	PKO bank Polski	Santander Bank	BNP Paribas
Bank Pekao S.A.	Bank Millennium	Credit Agricole	
Bank Pocztowy	BOSBank	Intello	
Nest Bank	Allor bank	ING	
MBANK	Getin Bank	SGB-Bank S.A.	
Citi Handlowy	Bank Nowy S.A.		

Zamówienie potwierdzone!
Otrzymaj środki i postępuj zgodnie z dalszymi instrukcjami, aby wysłać przedmiot do kupującego.

Ważne informacje
Podczas otrzymywania środków możesz zostać poproszony o podanie dodatkowych informacji. Nie martw się, jest to całkowicie bezpieczne. Twoje dane nie są przekazywane stronom trzecim.
Dlaczego mam podać swoje dane?

mx2pln.bond



Dane kupującego
Pełne imię i nazwisko: Maria Kowalska
Adres: Sokółka 24, 40-086 Katowice
Otrzymaj środki

Sprzedam drewno opałowe
150 zł

Aplikacje mobilne
Pomoc i opinie
Usługi płatne
Blogi OLX
Warunki korzystania
Polityka prywatności

Jak sprzedawać i kupować?
Zasady bezpieczeństwa
Mapa serwisu
Mapa regionów
Populacje proby
Pracuj w OLX

GET IT ON
Google play
Download on the App Store
Otwórz aplikację na Twoim telefonie

Pomoc techniczna Zapytaj Soś

FAŁSZYWE SKLEPY INTERNETOWE



Łatwo można wpaść w sidła cyberprzestępców, trafiając na fałszywe sklepy lub oferty kupna. Oszuści tworzą strony internetowe, które przypominają autentyczne sklepy znanych marek i oferują produkty w atrakcyjnych cenach.

Fałszywe sklepy internetowe – jak się chronić?

Zweryfikuj adres sklepu internetowego

Jeśli adres zawiera błędy, literówki lub odbiega od oficjalnej nazwy sklepu, to bardzo wyraźny sygnał ostrzegawczy.

Sprawdź dane kontaktowe i numer NIP

Brak danych kontaktowych sklepu takich jak: adres e-mail, numer telefonu, adres firmy oraz NIP może sugerować oszustwo. Gdy NIP jest widoczny, na jego podstawie sprawdź historię sprzedawcy w rejestrach takich jak: [KRS](#) lub [CEIDG](#).

Zapoznaj się z treścią regulaminu zakupów

Zwróć uwagę, czy w regulaminie są zawarte informacje dotyczące sposobów wysyłki oraz zwrotu towaru.

NASK

Sprawdź dostępne metody płatności

W fałszywych sklepach bardzo rzadko można zapłacić za pomocą popularnych metod takich jak np. BLIK. Najczęściej nie ma także możliwości płatności przy odbiorze towaru. Podczas płatności sprawdź, czy na pewno strona, do której odsyła sklep, to prawdziwa strona Twojego banku lub serwisu płatniczego.

Przeczytaj opinie i komentarze o sklepie

Zwróć uwagę, czy wszystkie opinie nie powstały w tym samym okresie i czy na pewno dotyczą wskazanego sklepu.

Co zrobić, gdy zorientujesz się, że zrobiłeś zakupy w fałszywym sklepie?



Bezzwłocznie **skontaktuj się ze swoim bankiem** i poinformuj o zaistniałej sytuacji.



Zgłoś przestępstwo w najbliższym **komisariacie policji**. Im szybsza będzie Twoja reakcja, tym większa szansa na odzyskanie pieniędzy.



Zgłoś incydent na stronie **incydent.cert.pl**. W ten sposób chronisz siebie i innych.



NASK



NASK

WARSZAWA

Projekt finansowany ze środków Ministra Cyfryzacji



KONSTANCIN-JEZIORNA
więcej niż
uzdrowisko

FAKE NEWS

6 FAKE NEWS

nieprawdziwe informacje w Internecie



- ➔  Sprawdź źródło informacji
- ➔  Zweryfikuj w innych, wiarygodnych źródłach
- ➔  Nie udostępniaj niepotwierdzonych informacji

To fałszywe lub zmanipulowane informacje rozpowszechniane po to, aby wpłynąć na emocje, decyzje, zachowania społeczne albo zaufanie do instytucji.

Dlaczego to łączy się z cyberatakami?

- Fałszywa informacja może być „przynętą” do phishingu – np. sensacyjny news prowadzi do strony wyłudzającej dane.
- Dezinformacja może budować napięcie społeczne i skłaniać do impulsywnego działania.
- Raport wskazuje, że grupy APT wykorzystywały tematy polityczne do wyłudzenia danych oraz wpływania na opinię publiczną.

FAKE NEWS

6 FAKE NEWS

nieprawdziwe informacje w Internecie



- ➔  Sprawdź źródło informacji
- ➔  Zweryfikuj w innych, wiarygodnych źródłach
- ➔  Nie udostępniaj niepotwierdzonych informacji

Na co uważać?

- sensacyjne nagłówki,
- brak źródła,
- fałszywe wypowiedzi znanych osób,
- reklamy obiecujące szybki zysk,
- treści wywołujące silny strach lub gniew.

Zasada obrony:

Zanim udostępnisz – sprawdź źródło, datę, autora i czy informację potwierdzają wiarygodne instytucje.



**KONSTANCIN-
JEZIORNA**
więcej niż
uzdrowisko

SYMULACJA AUTOUZUPEŁNIANIA FORMULARZA

Ustawienia

Konto i synchronizacja

Strona startowa i uruchamianie

Wyszukiwanie

Prywatność i bezpieczeństwo

Hasła i automatyczne wypełnianie

Wygląd

Pobieranie

Karty i przeglądanie

Ułatwienia dostępu

Języki

Sterowanie SI

Uprawnienia i dane

Laboratorium Firefoksa

O programie Firefox

Więcej od Mozilli

Rozszerzenia i motywy

Pomoc Firefoksa

Szukaj w ustawieniach

☒Zachowywanie i automatyczne wypełnianie nazw użytkownika i haseł

☒Proponowanie silnych haseł. [Więcej informacji](#)

☐Wymaganie zalogowania się na urządzeniu, aby zarządzać hasłami

☐Zezwalaj na pojedyncze logowanie Windows do kont Microsoft, służbowych i szkolnych. [Więcej informacji](#)

Zarządzaj zachowanymi hasłami

Dodatkowa ochrona

Hasło główne

Dodaje dodatkową warstwę zabezpieczeń, aby chronić zachowane hasła. [Więcej informacji](#)

Ustaw hasło główne

☒Powiadomienia o hasłach do stron, z których wyciekły dane. [Więcej informacji](#)

Metody płatności

☒Zachowuj i automatycznie wypełniaj informacje płatnicze. [Więcej informacji](#)

☐Wymaganie zalogowania się na urządzeniu, aby automatycznie wypełniać metody płatności i zarządzać nimi. [Więcej informacji](#)

Zarządzaj metodami płatności

Adresy i nie tylko

☒Zachowuj i automatycznie wypełniaj adresy. [Więcej informacji](#)

Zarządzaj adresami i nie tylko

Autofill Phishing PoC

Demo podatności Autofill

Wpisz e-mail lub kliknij "Symuluj Autofill" aby zobaczyć przechwytywanie danych.

Adres e-mail

jan.kowalski@email.pl

Zaloguj się

Symuluj Autofill (dla testu)

Elements

Console

Sources

Network

Performance

top

Filter

Default levels

No Issues

[SYMULACJA AUTOFILL] Imię i nazwisko → Jan Kowalski phishing.html:183

[SYMULACJA AUTOFILL] Imię → Jan phishing.html:183

[SYMULACJA AUTOFILL] Nazwisko → Kowalski phishing.html:183

[SYMULACJA AUTOFILL] Telefon → +48 123 456 789 phishing.html:183

[SYMULACJA AUTOFILL] Adres → ul. Główna 15/3, 00-950 Warszawa phishing.html:183

[SYMULACJA AUTOFILL] Kod pocztowy → 00-950 phishing.html:183

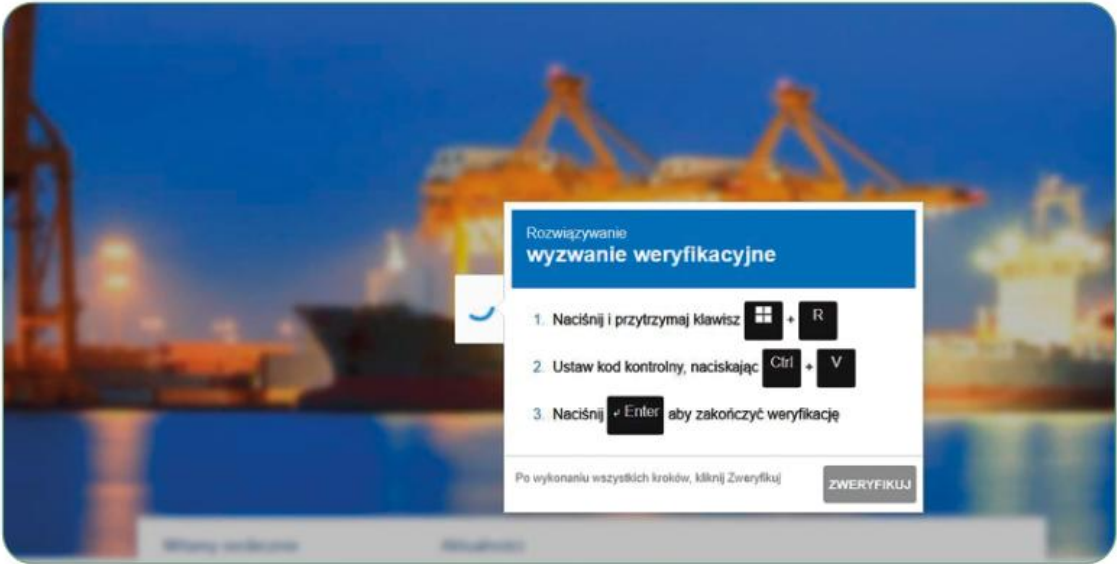
✓ Symulacja autofill zakończona pomyślnie! phishing.html:188



KONSTANCIN-
JEZIORNA
więcej niż
uzdrowisko

SYMULACJA AUTOZUPEŁNIANIA FORMULARZA

RYSUNEK 25. Fałszywa CAPTCHA zastosowana przez grupę UNC1151



RYSUNEK 24. Fałszywa weryfikacja użytkownika



SYMULACJA AUTOUZUPEŁNIANIA FORMULARZA

Chargeback

Co to jest chargeback i kiedy możesz z niego skorzystać?

- ✓ gdy sklep internetowy nie dostarczył Ci zamówionego towaru
- ✓ gdy wycieczka, lot, koncert opłacone kartą, zostały odwołane
- ✓ gdy sklep obciążył Cię podwójnie za ten sam zakup
- ✓ gdy bankomat innego banku nie wydał Ci gotówki, a wypłata obciążyła Twoje konto

<https://pkobp.pl/>

<https://incydent.cert.pl>



CERT.PL > Zgłoś incydent 

Zgłoszenia do CSIRT NASK

Informujemy, że od dnia 28 sierpnia 2018 r. zespołowi CERT Polska zostały powierzone obowiązki **CSIRT NASK** wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2026 poz. 20 z późn. zm.).

Jeżeli chcą Państwo zgłosić osobę kontaktową do CSIRT NASK proszę użyć poniższego odnośnika:
Zgłaszanie osoby kontaktowej do CSIRT NASK.

Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

Ustawowe definicje podmiotów znajdują się w kolumnie III - Rodzaj podmiotu:

- Podmioty kluczowe - Załącznik nr 1
- Podmioty ważne - Załącznik nr 2

 Osoba fizyczna / inne podmioty Osoba fizyczna lub inne podmioty niezdefiniowane przez ustawę o KSC	 Podmiot kluczowy Zdefiniowany w załączniku nr 1 do ustawy o KSC	 Podmiot ważny Zdefiniowany w załączniku nr 2 do ustawy o KSC
---	--	---

CERT Polska | Polityka prywatności | Deklaracja dostępności



**KONSTANCIN-
JEZIORNA**
więcej niż
uzdrowisko

ZGŁOSZENIE INCYDENTU DO CERT



cert-incydent via RT <cert@cert.pl>
do mnie ▾

Potencjalne Zdarzenie Dla Cyberbezpieczeństwa" - złośliwa wiadomość

Dziękujemy za przesłanie zgłoszenia. Poniżej znajdują się zarejestrowane przez nas informacje:

E-mail zgłaszającego:

glkmarcin@gmail.com

Numer telefonu zgłaszającego:

Zgoda na przetwarzanie danych osobowych:

TAK

Zgłoszenie wyłącznie informacyjne - nie oczekuję kontaktu zwrotnego:

NIE

Opis incydentu oraz wszelkie dodatkowe informacje:

PGE Polska Grupa Energetyczna S.A.

ul. Mysia 2, 00-496 Warszawa

Warszawa, dnia 22.03.2026 r.

DOTYCZY: ZWROTU NADPŁATY Z TYTUŁU PODWÓJNEJ PŁATNOŚCI

Szanowny Kliencie,

Niniejszym informujemy, że w wyniku przeprowadzonej weryfikacji salda rozliczeń, stwierdzono wystąpienie **nadpłaty** na Państwa koncie. Nadpłata ta wynika z dwukrotnego uregulowania należności za ten sam okres rozliczeniowy.

Opis operacji Kwota (PLN)

Nadpłata podstawowa 279,29

Naliczone odsetki ustawowe 6,15

Łącznie do **zwrotu** 285,44

W celu sfinalizowania procedury **zwrotu** środków, uprasza się o niezwłoczne potwierdzenie dyspozycji przelewu na rachunek bankowy. Zapewniamy, że wszelkie formalności zostały ograniczone do minimum.

POTWIERDŹ DANE DO PRZELEWU

Z poważaniem,

Zespół Rozliczeń PGE

<https://mandrillapp.com/track/click/13600603/kiniris.com?p=eyJzljoiND0FUSWdIUyUyZTSVJOS1ZUSHM2WUU3U2IMNWFBliwidil6MiwicCl6IntclnVcljoxMzYwMDYwMyxclnZcljoyLFwidXJsXCi6XCJodHRwczpcXFwvXFxcl2tpbmlyeXMuY29lXFxcl2d4bGxlcmlcXFwva2Fib2wucGhwXClsXCJpZFwiOlwiOTdmZDRkOGQzOGEwNDMyMTkyNmQ1YzRmODcyZjE1OGVclixclnVybF9pZHNcljpbXCJkZTAwNTk2OWZmYTU2ZGI2YWU5OGI2MzlwODUzZmJiZmQyZTg5NDdkXCJldFwibXNnX3RzXCi6MTc3NDYzNTE2NH0iIQ>

10 kwi 2026, 20:04 ☆ 😊 ↩ ⋮



CERT Polska via RT <cert@cert.pl>
do mnie ▾

13 kwi 2026, 08:51 ☆ 😊 ↩ ⋮

Dzień dobry,

dziękujemy za kontakt z naszym zespołem.

Podejrzana wiadomość nosi znamiona oszustwa typu phishing. Link zawarty w treści prowadził na stronę, której celem było wyłudzenie danych użytkownika. Szkodliwa domena została wpisana na listę ostrzeżeń CERT Polska (<https://cert.pl/lista-ostrzezen/>) oraz podjęliśmy kroki mające na celu usunięcie z niej szkodliwych treści.

Zalecamy zignorować oraz usunąć podejrzaną wiadomość.

Zachęcamy także do śledzenia i/lub subskrypcji komunikatów, które umieszczamy na stronie <https://moje.cert.pl/komunikaty/> oraz do obserwowania naszych kont w mediach społecznościowych:

-Facebook: <https://facebook.com/CERTPolska/>

-X: https://x.com/Cert_Polska/

gdzie umieszczamy ostrzeżenia przed aktywnymi oszustwami.

Z poważaniem
CSIRT NASK / CERT Polska
cert.pl



KONSTANCIN-
JEZIORNA
więcej niż
uzdrowisko

↩ Odpowiedz

➡ Przekaż dalej



PODSUMOWANIE RAPORTU ROCZNEGO 2025 CERT NASK

Analiza przedstawionych kampanii phishingowych pozwala zidentyfikować wspólne cechy charakterystyczne współczesnych zagrożeń w polskiej cyberprzestrzeni, z których znakomita większość to phishing.

Przestępcy konsekwentnie podszywają się pod zaufane instytucje – zarówno państwowe, jak i prywatne – profesjonalnie naśladowując ich oficjalną korespondencję.

Stosowane techniki manipulacji psychologicznej, zwłaszcza wywoływanie poczucia pilności, oraz obietnice korzyści finansowych skutecznie skłaniają ofiary do działania bez należytej weryfikacji.

Obserwowany trend wskazuje na systematyczny wzrost poziomu zaawansowania ataków. Materiały phishingowe charakteryzują się coraz wyższą jakością wykonania – poprawną polszczyzną, wiernymi kopiami oryginalnych interfejsów oraz przemyślaną strukturą komunikatów.

Sprawcy elastycznie dostosowują scenariusze oszustw do bieżących wydarzeń, sezonowych trendów i zmian legislacyjnych, co dodatkowo zwiększa skuteczność prowadzonych kampanii.

PODSUMOWANIE, WAŻNE PORADY



Jedna usługa = jedno hasło.

To zwiększa bezpieczeństwo Twoich danych. Jeśli ktoś złamie Twoje hasło lub dojdzie do jego wycieku, cyberprzestępcy mogą spróbować użyć go w innych serwisach (np. poczta e-mail, serwisy społecznościowe).

Dlatego ważne jest, aby do każdej usługi posiadać odrębne hasło.

Nie zapisuj haseł na karteczkach i nie przyklejaj ich na urządzeniu.

Unikaj przechowywania haseł w miejscach dostępnych dla innych.

Nigdy nie podawaj swoich haseł osobom trzecim.

Jeśli masz podejrzenie, że Twoje hasło wyciekło, **zmień je.**

Ostrożnie korzystaj z obcych komputerów. Unikaj logowania się na nich do ważnych usług.

Więcej informacji na temat haseł znajdziesz na stronie: cert.pl

NASK

Włącz weryfikację dwuetapową



Brzmi to skomplikowanie, ale w rzeczywistości jest bardzo proste. **Weryfikacja dwuetapowa to dodatkowe zabezpieczenie podczas logowania**, które chroni Twoje konta w internecie.

Jak to działa? Aby się zalogować, oprócz wpisania hasła będziesz musiał podać także dodatkowy kod. Otrzymasz go za pośrednictwem SMS-a, wiadomości e-mail lub aplikacji w telefonie. Dodatkowym zabezpieczeniem mogą być także Twoje indywidualne cechy fizyczne m.in. odcisk Twojego palca, skan twarzy lub oka czyli tzw. biometria.

1 Twoje hasło



2 Weryfikacja za pomocą kodu lub biometrii



lub



Weryfikacja dwuetapowa jest szczególnie istotna przy logowaniu do serwisów zawierających ważne dane, m.in. poczta e-mail, konto bankowe czy media społecznościowe.

Dzięki niej zwiększasz bezpieczeństwo swoich kont!

NASK



Poradnik dla seniorów 2024



NASK



Projekt finansowany ze środków Ministra Cyfryzacji



KONSTANCIN-JEZIORNA
więcej niż
uzdrowisko

PODSUMOWANIE, WAŻNE PORADY

Ważne porady!



Przestępcy będą wykorzystywać każdą okazję, by pozyskać Twoje dane, które pozwolą im np. na kradzież pieniędzy z konta, włamanie na pocztę e-mail i przejęcie korespondencji czy namawianie Twoich bliskich do szybkich przelewów na platformach społecznościowych.

Nigdy nie działaj pod presją czasu.

Uważaj na niespodziewane e-maile, SMS-y i telefony, w których oszuści mogą próbować wyłudzić Twoje dane.

Regularnie sprawdzaj historię transakcji na koncie bankowym.

Uważaj, co udostępniasz na profilach społecznościowych.

Nie udostępniaj w internecie zdjęć i relacji, na których pokazujesz swoje dokumenty.

NASK

Ważne porady!

Zastrzeż swój PESEL

aby nikt nie mógł go użyć do zawierania umów kredytowych lub pożyczek bez Twojej zgody.

Zastrzeżenie numeru PESEL w żaden sposób nie zablokuje Ci możliwości rejestracji do lekarza, realizacji recepty czy załatwienia sprawy urzędowej.

Jak to zrobić?

Przez internet

lub

w dowolnym urzędzie



Co będzie potrzebne?

Potwierdzenie tożsamości za pomocą:

- profilu zaufanego,
- podpisu kwalifikowanego,
- e-dowodu,
- lub danych do logowania do bankowości elektronicznej.



Dowód osobisty

W jaki sposób zastrzec PESEL?

Zaloguj się na stronie mObywatel.gov.pl lub uruchom aplikację mObywatel na telefonie.

Poproś o pomoc pracownika urzędu.

NASK

#Halo!

Tu cyberbezpieczny Senior



Poradnik dla seniorów 2024



NASK



KONSTANCIN-JEZIORNA
więcej niż
uzdrowisko