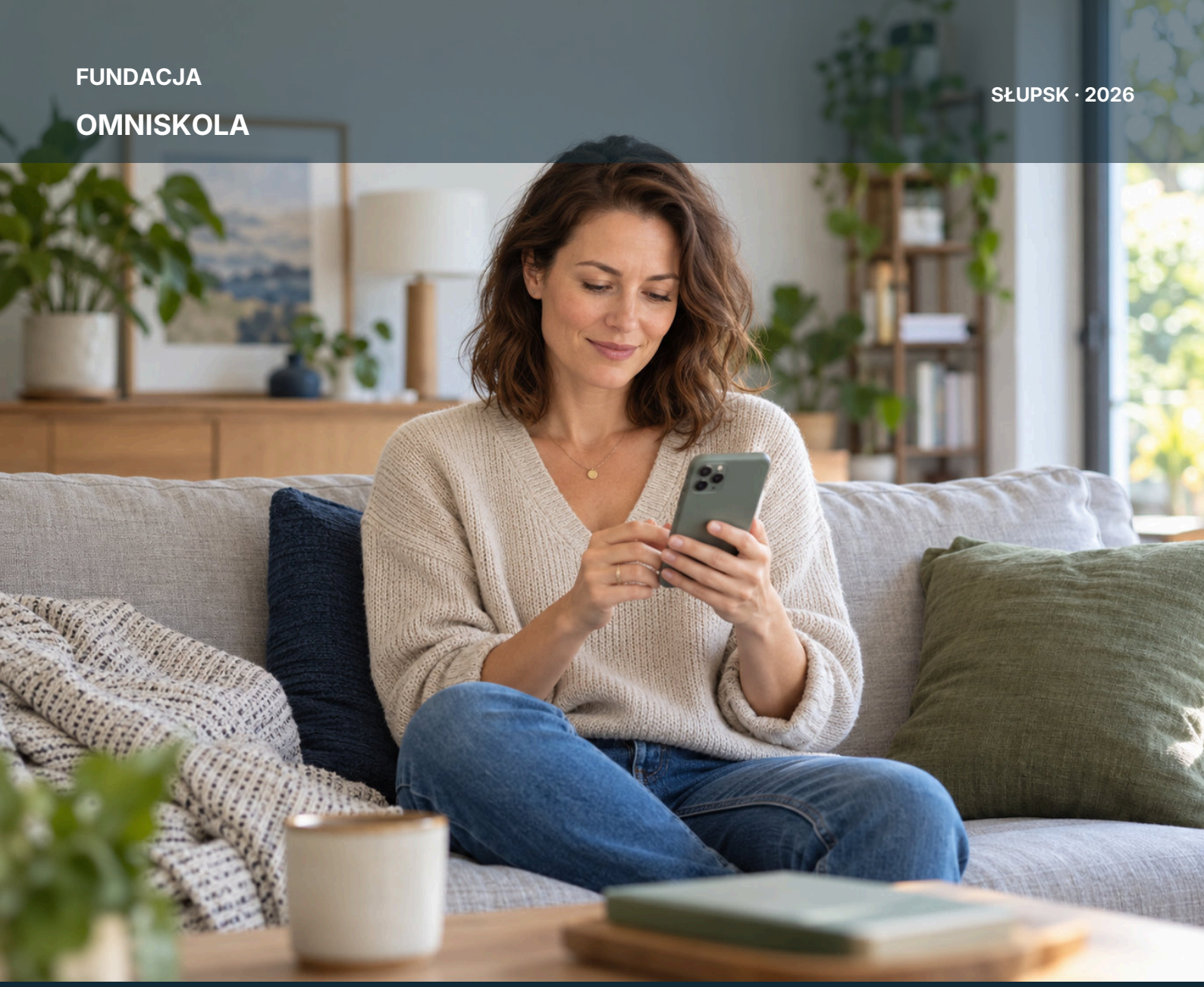
FUNDACJA
OMNISKOLA

SŁUPSK · 2026



PRAKTYCZNY PRZEWODNIK

Cyfrowa samoobrona

Jak rozpoznawać oszustwa, chronić swoje konta i podejmować bezpieczne decyzje w świecie AI.

ZATRZYMAJ · SPRAWDŹ · POTWIERDŹ · DZIAŁAJ

Zacznij od 5 prostych kroków

Najważniejsze działania możesz wykonać jeszcze dziś.



260 783

unikalne incydenty cyberbezpieczeństwa zarejestrowane przez CERT Polska w 2025 r.

658 320

przeanalizowanych zgłoszeń — to nie liczba wszystkich oszustw ani poszkodowanych osób. [1]

PIĘĆ KROKÓW DO WIĘKSZEGO BEZPIECZEŃSTWA

1. **Poczta e-mail**

   Ustaw unikalne hasło i włącz dodatkowe potwierdzanie logowania.

2. **Telefon**

   Zablokuj ekran i włącz automatyczne aktualizacje systemu i aplikacji.

3. **Bliscy**

   Ustalcie sposób sprawdzania pilnych próśb o pieniądze lub kody.

4. **Kopia danych**

   Zrób kopię zdjęć i dokumentów; sprawdź, czy odzyskasz plik.

5. **Pomoc pod ręką**

   Zapisz numer swojego banku i adres incydent.cert.pl; SMS z linkiem przekaż na 8080.

Nie klikaj, nie podawaj kodu i nie zatwierdzaj płatności. Skontaktuj się z nadawcą przez znany, niezależny kanał.

W tym przewodniku

Poradnik, praktyczne przykłady i materiały do samodzielnej pracy.

01 **Najpierw zatrzymaj presję** 04
Prosta reakcja na presję i pośpiech.

02 **Wiadomości, linki i telefony** 06
Dopłaty, kody, oszuści podszywający się pod instytucje.

03 **Konta, które warto chronić** 08
Dobre hasła, MFA i odzyskiwanie dostępu.

04 **Telefon, komputer i prywatność** 10
Aktualizacje, aplikacje, kopie i bezpieczeństwo w sieci.

05 **AI, deepfake i klonowanie głosu** 12
Gdy głos lub obraz nie są wiarygodnym dowodem.

06 **Informacje w zwykły dzień i w kryzysie** 14
Źródło, kontekst, oficjalne komunikaty.

07 **Jeśli coś już się stało** 16
Zabezpieczenie pieniędzy, kont i dowodów.

08 **Zakupy i kody QR** 18
Bezpieczna płatność i sprawdzanie linków.

Ćwiczenia i karty do wydruku
Scenariusze i samoocena · od s. 20

Materiały źródłowe: CERT Polska, NASK, RCB oraz instytucje publiczne.

Najpierw zatrzymaj presję

Nie musisz rozstrzygać, czy wiadomość jest prawdziwa, kiedy ktoś wywiera na Ciebie presję.



„Przerwa nie jest stratą czasu.”

Zakończ rozmowę. Sprawdź prośbę samodzielnie i skontaktuj się z nadawcą przez znany, niezależny kanał.

Pierwsza minuta ma znaczenie

Pięć rzeczy, które warto zrobić, zanim odpowiesz.

CO ZROBIĆ W PIERWSZEJ MINUCIE?

1. Nie klikaj linku ani kodu QR z niespodziewanej wiadomości. Nie instaluj programu na prośbę rozmówcy.
2. Nie dyktuj hasła, kodu SMS, kodu BLIK ani danych karty. Bank nie potrzebuje hasła logowania.
3. Zakończ rozmowę. Otwórz aplikację samodzielnie lub zadzwoń na zapisany numer.
4. Przeczytaj autoryzację. Sprawdź odbiorcę, kwotę i rodzaj operacji. W razie niezgodności anuluj.
5. Zachowaj dowody. Nie rozsyłaj dalej niezweryfikowanego linku, nawet jako ostrzeżenia.



ZAPAMIĘTAJ

„Przerwa nie jest stratą czasu. Daje Ci kontrolę nad decyzją.”

Wiadomości, linki i telefony

Rozpoznawaj prośbę, a nie tylko logo nadawcy.

Wiadomość może przypominać kontakt od kuriera, banku, sklepu, urzędu lub znajomego. Może trafić SMS-em, e-mailem, przez komunikator, reklamę albo kod QR. Nazwę i wygląd nadawcy łatwo podrobić. [3]

PIĘĆ PYTAŃ PRZED KLIKNIĘCIEM

1 **Czy się spodziewam?**

Czy wiadomość dotyczy znanej mi, rzeczywistej sprawy?

2 **Czego żąda nadawca?**

Hasła, kodu, dopłaty, instalacji, dokumentu lub przelewu?

3 **Czy mam inną drogę?**

Czy mogę otworzyć oficjalną aplikację samodzielnie?

4 **Jaki to adres?**

Czy domena nie zawiera literówki, dodatku albo innej końcówki?

5 **Jak potwierdzić?**

Czy mogę zadzwonić pod numer zapisany dużo wcześniej?

Przykład: fałszywy SMS o dopłacie 1,23 zł

Niewielka kwota i znajoma nazwa firmy nie potwierdzają, że wiadomość jest prawdziwa.



1

ZATRZYMAJ

Nie otwieraj linku i nie podawaj danych.

2

SPRAWDŹ

Wejdź do aplikacji przewoźnika samodzielnie.

3

POTWIERDŹ

Sprawdź numer przesyłki u nadawcy.

4

ZGŁOŚ

Podejrzany SMS z linkiem przekaż na 8080.

PAMIĘTAJ

Sama informacja o dopłacie nie dowodzi oszustwa. To sygnał, by weryfikować prośbę innym kanałem.

Konta, które warto chronić

Poczta e-mail to często klucz do innych kont.



CZTERY NAWYKI, KTÓRE POMAGAJĄ

01 Jedno konto = jedno hasło

Długie, unikalne hasła chronią przed wykorzystaniem jednego wycieku w wielu serwisach. CERT Polska wskazuje co najmniej 14 znaków. [2]

02 Menedżer haseł

Tworzy i przechowuje trudne hasła, a Ty zapamiętujesz tylko mocne hasło główne.

03 MFA / 2FA

Włącz dodatkowy składnik logowania, przede wszystkim na poczcie i w banku.

04 Passkeys

Jeżeli dostępne, mogą ograniczać ryzyko wyłudzenia hasła przez podrobioną stronę. [18]

NIE ZMIENIAJ HASEŁ BEZ POWODU

Nie trzeba zmieniać wszystkich haseł według kalendarza. Zrób to natychmiast, gdy podejrzewasz wyciek, powtórzenie hasła lub przejęcie konta.

Dobre zabezpieczenie to plan B

PRZYGOTUJ ODZYSKIWANIE KONTA

1. Sprawdź numer telefonu i zapasowy adres e-mail do odzyskiwania dostępu.
2. Zapisz kody zapasowe MFA poza telefonem, który może się zgubić.
3. Przeglądaj zalogowane urządzenia i kończ obce sesje.
4. Usuń nieznane aplikacje z dostępem do konta; sprawdź przekazywanie poczty.
5. Włącz blokadę ekranu oraz możliwość zdalnego odnalezienia i zablokowania telefonu.

UWAGA NA FAŁSZYWE MFA

Jednorazowy kod może zostać wyłudzony, jeśli wpiszesz go na podrobionej stronie lub podyktujesz rozmówcy. Nie zatwierdzaj monitu logowania, którego sama/sam nie rozpoczęłaś/rozpoczęłeś.

Telefon, komputer i prywatność

Trzy codzienne nawyki, które realnie ograniczają ryzyko.



PROSTE ZASADY. DUŻA RÓŻNICA.

01

Aktualizuj

Włącz aktualizacje systemu, przeglądarki i aplikacji. To prosty sposób ograniczania znanych luk.

02

Sprawdzaj

Pobieraj programy z oficjalnych źródeł. Sprawdzaj nazwę wydawcy oraz uprawnienia aplikacji.

03

Rób kopie

Zapisuj ważne pliki w dodatkowej lokalizacji. Regularnie sprawdzaj, czy możesz je przywrócić.

Kłódka HTTPS szyfruje połączenie, ale nie dowodzi, że strona należy do prawdziwej instytucji.

Zasada 3–2–1 i prywatność



ZASADA 3–2–1 W PRAKTYCE

3
kopie ważnych danych

2
różne rodzaje nośników

1
kopia poza urządzeniem / domem

Kopia zapasowa to plan powrotu

Zapisuj zdjęcia i dokumenty na więcej niż jednym nośniku. Co jakiś czas sprawdź, czy możesz naprawdę odzyskać plik z kopii — to ważniejszy test niż samo istnienie kopii. [11]

NIE UDOSTĘPNIAJ CAŁEGO SWOJEGO ŻYCIA

Adres, plan wyjazdu, zdjęcie dokumentu, numer rezerwacji, widok kluczy czy miejsce stałego pobytu pomagają oszustowi zbudować wiarygodną historię. Nie musisz znikać z internetu — zdecyduj, co publikujesz, komu pokazujesz posty i kiedy udostępniasz lokalizację. [5, 14]

AI, deepfake i klonowanie głosu

Twoją ochroną jest niezależne potwierdzenie, nie idealny wzrok.

Głos znajomej osoby może zostać podrobiony. Obraz, nagranie i głos mogą być syntetyczne lub zmienione. Również autentyczne materiały mogą być stare albo opisane nieprawdziwie. Sam realistyczny wygląd nie wystarcza. [8, 15]



GDY BLISKI PILNIE PROSI O PIENIĄDZE

1. Nie decyduj w trakcie nagrania lub rozmowy, nawet jeśli rozpoznajesz głos.
2. Rozłącz się i oddzwoń na numer zapisany wcześniej w kontaktach.
3. Potwierdź prośbę drugim kanałem lub u innej bliskiej osoby.
4. Ustal z rodziną pytanie kontrolne albo wspólną metodę weryfikacji.
5. Nie podawaj kodu BLIK ani kodów logowania; sprawdzaj dane przelewu.

Nie ufaj samemu nagraniu

PIĘĆ SPOSOBÓW NA SPRAWDZENIE

1. **Źródło**
   Znajdź pierwotną publikację; sprawdź, kto ją zamieścił.

2. **Data i miejsce**
   Porównaj opis z datą i miejscem wydarzenia.

3. **Pełny kontekst**
   Znajdź całość nagrania albo wypowiedzi, nie tylko wycinek.

4. **Druga opinia**
   Sprawdź niezależne, wiarygodne źródła.

5. **Żądanie działania**
   Czy treść nakłania do przelewu, kliknięcia lub natychmiastowego udostępnienia?



NIE MASZ POTWIERDZENIA?

Nie masz potwierdzenia? Nie udostępniaj jako faktu. Możesz powiedzieć: „Nie mam potwierdzenia — sprawdzam”.

Informacje w sieci i w kryzysie

Źródło • data • kontekst • niezależne potwierdzenie



SPRAWDŹ INFORMACJĘ W CZTERECH KROKACH

1 **ŹRÓDŁO**

Kto to opublikował? Czy możesz dotrzeć do oryginalnego komunikatu?

2 **DATA I MIEJSCE**

Czy sprawa dotyczy dziś właściwego miasta i sytuacji?

3 **DOWÓD I KONTEKST**

Czy widzisz pełny dokument, materiał lub wypowiedź?

4 **POTWIERDZENIE**

Czy niezależne wiarygodne źródła przekazują to samo?

UWAGA NA EMOCJE

Silny strach lub złość, a do tego prośba „podaj pilnie dalej”, są dobrym powodem, by zwolnić.

Gdy wiadomość dotyczy zagrożenia

Gdy pojawia się alarmująca wiadomość o Słupsku

Nie podejmuj decyzji na podstawie samego zrzutu ekranu. Otwórz samodzielnie stronę Rządowego Centrum Bezpieczeństwa, oficjalne komunikaty służb oraz miasta lub województwa. Alert RCB dotyczy prawdopodobieństwa bezpośredniego zagrożenia życia lub zdrowia na znaczącym obszarze, a najmniejszą jednostką wysyłki jest powiat. Brak SMS-a nie dowodzi braku lokalnego zagrożenia. [12, 17]

112

NUMER ALARMOWY

Najpierw zadbaj o bezpieczeństwo i stosuj się do poleceń służb. W razie potrzeby natychmiastowej interwencji dzwoń pod 112. Nie ujawniaj czyjegoś miejsca pobytu lub szczegółów ewakuacji.

Dbaj o higienę informacyjną

Wybierz kilka wiarygodnych źródeł i sprawdzaj je w określonych porach. Wyłącz zbędne powiadomienia. Szybkość nie jest tym samym co pewność.

Jeśli coś już się stało

Konkretne kroki po ujawnieniu hasła, kodu lub pieniędzy.

1

Zabezpiecz konto

Zmień hasło na oficjalnej stronie serwisu. Wyloguj inne sesje i włącz dodatkowe potwierdzanie logowania.

2

Skontaktuj się z bankiem

Jeżeli ujawniono dane karty, kod płatniczy lub pieniądze, zadzwoń pilnie na oficjalny numer banku.

3

Zgłoś incydent

Podejrzany SMS prześlij na 8080, a fałszywą stronę lub inne zdarzenie zgłoś na incydent.cert.pl.

4

Zachowaj dowody

Zapisz wiadomości, adresy stron, numer rachunku i potwierdzenia przelewów. Sprawę zgłoś Policji.

5

Ostrzeż bliskich

Jeśli oszust przejął Twoje konto, sprawdź, czy nie kontaktuje się z innymi osobami w Twoim imieniu.

WAŻNE Nie trać czasu na rozmowę z oszustem. Im szybciej zareagujesz, tym większa szansa na ograniczenie szkód.

Gdzie szukać pomocy?

PIERWSZY KROK ZALEŻY OD SYTUACJI

1

Podejrzany SMS

Przekaż oryginał na 8080.

2

Fałszywa strona / e-mail

Zgłoś przez incydent.cert.pl.

3

Zagrożone konto

Użyj oficjalnego odzyskiwania konta.

4

Ryzyko utraty pieniędzy

Pilnie bank, następnie Policja / CBZC.

5

Dane osobowe

Administrator / platforma; w sprawach ochrony danych także UODO.

6

Program zdalnego dostępu

Przerwij połączenie. Nie loguj się do banku na tym urządzeniu.
Skontaktuj się z bankiem z innego zaufanego urządzenia. [19]

Bezpieczne zakupy w sieci

ZANIM ZAPŁACISZ

1

Cena i pośpiech

Porównaj cenę w kilku sklepach. Duża przecena i licznik czasu mogą skłaniać do pochopnej decyzji.

2

Sprawdź sprzedawcę

Poszukaj danych firmy, sposobu kontaktu i opinii także poza stroną sklepu.

3

Samodzielnie otwórz sklep

Nie przechodź do płatności z reklamy lub wiadomości. Sprawdź adres strony i domenę.

4

Przeczytaj autoryzację

Przed zapłatą sprawdź kwotę, odbiorcę i rodzaj operacji. W razie niezgodności nie zatwierdzaj.

5

Pobranie i płatność kartą

Pobranie nie gwarantuje zawartości paczki. Po problemie z płatnością kartą zapytaj bank o reklamację.

6

Gdy coś budzi wątpliwość

Skontaktuj się z bankiem, zachowaj dowody i zgłoś incydent. Poradnik: cert.pl/falszywe-sklepy/

Kody QR i fałszywe linki

SPRAWDŹ, ZANIM OTWORZYSZ

1

Co może zawierać kod?

Kod QR może otwierać stronę, uruchamiać płatność lub parować urządzenie. Sam kod nie potwierdza bezpieczeństwa.

2

Sprawdź pochodzenie

Kod w wiadomości, ogłoszeniu lub na naklejce może prowadzić do podrobionej strony. Potwierdź go inną drogą.

3

Obejrzyj adres

Przed otwarciem sprawdź podgląd i domenę. Nazwa usługi w dalszej części adresu nie dowodzi jej autentyczności.

4

Otwórz znaną aplikację

Przy płatnościach i logowaniu uruchom aplikację lub wpisz znany adres samodzielnie, zamiast korzystać z kodu.

5

Uważaj na parowanie

Nie skanuj kodu, by dać komuś dostęp do wiadomości lub konta. Sprawdź, jakie urządzenia są połączone.

6

Jeśli podałaś lub podałeś dane

Otwórz oficjalną stronę, zmień hasło i zakończ obce sesje. Przy ryzyku utraty pieniędzy skontaktuj się z bankiem.

Przećwicz i sprawdź siebie

Trzy sytuacje bardzo podobne do tych z codziennego życia.

TRZY SYTUACJE DO PRZEĆWICZENIA

01

A / BLIK od znajomego

„Zgubiłem portfel, podeślij szybko kod, oddam wieczorem”. Nie wysyłaj kodu. Zadzwoń na znany numer i sprawdź autoryzację w banku.

02

B / Telefon „z banku”

Rozmówca chce zdalnie „chronić pieniądze” i każe instalować program. Rozłącz się, nie instaluj, skontaktuj się z bankiem. [19]

03

C / Pilne nagranie o Słupsku

W grupie osiedlowej krąży alarmujący film. Sprawdź datę, miejsce i oficjalne komunikaty; nie udostępniaj dalej bez potwierdzenia.

Mini-quiz: znasz odpowiedzi?

1

Logo banku i poprawna polszczyzna — czy to dowód?

Nie. Otwórz aplikację samodzielnie i sprawdź prośbę.

2

Czy można dyktować kod MFA rozmówcy z banku?

Nie. Nie przekazuj haseł ani kodów jednorazowych.

3

Czy HTTPS gwarantuje uczciwość strony?

Nie. Szyfruje połączenie, nie weryfikuje uczciwości witryny.

4

Co zrobić z podejrzanym SMS-em z linkiem?

Przekaż bez zmian na 8080. To nie infolinia.

5

Czy zgłoszenie do CERT wystarczy po utracie pieniędzy?

Nie. Pilnie zadzwoń do banku i zgłoś sprawę Policji.

6

Jak sprawdzić pilną prośbę od bliskiej osoby?

Rozłącz się i oddzwoń na numer zapisany wcześniej.

Sprawdź swoją pewność

Porównaj, czego dowiedziałaś / dowiedziałeś się z poradnika.

Oceń pewność w każdym obszarze na skali 1–5. Wypełnij raz przed lekturą, a drugi raz po przeczytaniu poradnika. To samoocena do własnego użytku — nie wpisuj danych osobowych.

OBSZAR	PRZED	PO
Rozpoznawanie phishingu i wyłudzeń	1 2 3 4 5	1 2 3 4 5
Rozpoznawanie socjotechniki	1 2 3 4 5	1 2 3 4 5
Zabezpieczanie kont, haseł i danych	1 2 3 4 5	1 2 3 4 5
Rozpoznawanie ryzyk AI i deepfake	1 2 3 4 5	1 2 3 4 5
Reagowanie na incydent	1 2 3 4 5	1 2 3 4 5
Ocena wiarygodności informacji	1 2 3 4 5	1 2 3 4 5

JAK CZYTAĆ SKALĘ?

1 — bardzo niska • 2 — niska • 3 — średnia • 4 — dobra • 5 — bardzo dobra.

10 zasad na co dzień

1. Zatrzymuję się, gdy ktoś wywiera presję czasu lub każe zachować tajemnicę.
2. Nie przekazuję haseł, kodów logowania, BLIK ani kodów odzyskiwania.
3. Otwieram bank, urząd i kuriera przez własną aplikację lub znany adres.
4. Sprawdzam odbiorcę, kwotę i rodzaj zatwierdzanej operacji.
5. Mam różne, długie hasła do kont i korzystam z menedżera haseł.
6. Mam MFA na poczcie, w banku i ważnych profilach.
7. Aktualizuję urządzenia i kontroluję uprawnienia aplikacji.
8. Robię kopie ważnych danych i sprawdzam możliwość ich odtworzenia.
9. Pilne prośby bliskich weryfikuję przez zapisany numer.
10. Alarmujące wiadomości sprawdzam u źródła i nie rozsyłam plotek.

ZACHOWAJ NA PÓŹNIEJ / 8080 · incydent.cert.pl · 112

Słownik bez żargonu

Prosto o technologiach i bezpieczeństwie.

Phishing	Podszywanie się pod osobę lub instytucję, aby wyłudzić dane, kliknięcie lub płatność.
Smishing	Phishing przez SMS.
Socjotechnika	Wywieranie wpływu przez zaufanie, presję, strach lub obietnicę korzyści.
MFA / 2FA	Uwierzytelnianie z użyciem niezależnych kategorii składników. 2FA to dokładnie dwa składniki; MFA — co najmniej dwa. [18]
Passkey	Logowanie kluczem kryptograficznym powiązanym z właściwą usługą.
Deepfake	Obraz, dźwięk lub film wygenerowany albo zmieniony przez AI w sposób przypominający rzeczywistość.
Dezinformacja	Celowe rozpowszechnianie fałszywych lub wprowadzających w błąd treści dla korzyści lub wyrządzenia szkody. [13]
Kopia zapasowa	Dodatkowy zapis danych pozwalający odzyskać je po awarii, utracie lub kradzieży.

Źródła i dalsza pomoc

Sprawdzenie źródeł: 29 września 2026 r. W razie incydentu korzystaj z aktualnych komunikatów.

01 **Raport roczny CERT Polska za 2025 r.**
Statystyki zgłoszeń i zarejestrowanych incydentów.

02 **Hasła — dobre praktyki (CERT Polska)**
Hasła, menedżer, MFA, passkeys.

03 **Rozpoznanie phishingu (CERT Polska)**
Sygnały ryzyka, reakcja po ujawnieniu danych.

04 **Bezpieczeństwo telefonu (CERT Polska)**
Aktualizacje, aplikacje i urządzenia.

05 **Bezpieczeństwo kont w social mediach (CERT Polska)**
MFA, sesje i zabezpieczanie profilu.

06 **Zasady zgłaszania incydentów (CERT Polska)**
Zgłoszenia CERT, SMS na 8080.

07 **Zastrzeż PESEL (mObywatel)**
Oficjalna usługa i sposoby skorzystania.

08 **Usta, głos, treść, tło — NASK**
Poszlaki deepfake, 15.01.2025.

09 **Dobre nawyki — BLIK**
Weryfikacja próśb i transakcji.

10 **Planujesz wyjście na koncert? — CERT Polska**
Archiwalny przykład oszustwa z biletami.

Źródła i dalsza pomoc

Sprawdzenie źródeł: 29 września 2026 r. W razie incydentu korzystaj z aktualnych komunikatów.

11 **Kopie zapasowe w pigułce — Ministerstwo Cyfryzacji**
Kopie danych i test przywracania.

12 **Alert RCB — pytania i odpowiedzi**
Zasady działania ostrzeżeń.

13 **Chroń się przed dezinformacją — NASK**
Weryfikacja źródła i kontekstu.

14 **Jak chronić dane osobowe? — UODO**
Ograniczanie informacji o sobie.

15 **Deepfakes — UKE**
Ryzyko podszywania się przez syntetyczny głos i obraz.

16 **Zgłoś cyberoszustwo — CBZC**
Zabezpieczenie dowodów i zgłoszenie.

17 **Co zgłaszać? Numer alarmowy 112 — gov.pl**
Właściwe użycie numeru ratunkowego.

18 **Uwierzytelnianie wieloskładnikowe — CERT Polska**
MFA i 2FA.

19 **Ataki z użyciem AnyDesk — CERT Polska**
Zdalny dostęp i postępowanie po incydencie.

O projekcie



ODPORNI CYFROWO

Ten przewodnik powstał w ramach projektu „Odporni cyfrowo – cyberbezpieczeństwo i samoobrona informacyjna w czasach AI”, realizowanego przez Fundację OmniSkola w Słupsku. Materiał pomaga dorosłym mieszkańcom podejmować bezpieczniejsze decyzje w sieci.

Finansowanie i partnerzy

PROJEKT I FINANSOWANIE

Projekt dofinansowany w ramach Funduszu AKUMULATOR SPOŁECZNY, ze środków Rządowego Programu Wsparcia Organizacji Pozarządowych MOC MAŁYCH SPOŁECZNOŚCI.

PARTNERZY I INSTYTUCJE WSPIERAJĄCE

Akumulator społeczny

Rządowy Program Wsparcia Organizacji Pozarządowych Moc Małych Społeczności

NIW Narodowy Instytut Wolności – Centrum Rozwoju Społeczeństwa Obywatelskiego

CIO

KOMITET DO SPRAW POŻYTKU PUBLICZNEGO