Zanim klikniesz

Poradnik bezpieczeństwa IT dla firm. Co zrobić, gdy mail, telefon albo czat prosi o pieniądze, hasło lub kod.



25
sytuacji z życia firmy, każda na jednej karcie

Pierwsza godzina
co robić, gdy coś już się stało

Karta na biurko
do wycięcia i powieszenia przy komputerze

Stop. Sprawdź. Zgłoś.

SYSTEMBOX
BIAŁYSTOK · CAŁA POLSKA

Zanim klikniesz

PODTYTUŁ	Poradnik bezpieczeństwa IT dla firm
WYDANIE	1, listopad 2026. Stan źródeł: 28.11.2026
AUTOR	Sergiusz Siemak, SYSTEMBOX, Białystok
W SIECI	systembox.pl/poradniki/zanim-klikniesz
KONTAKT	kontakt@systembox.pl, +48 570 923 234
WOLNO	Drukować, kopiować i przekazywać dalej w całości, bez zmian w treści i bez opłat.
UWAGA	Poradnik opisuje dobre praktyki. Nie zastępuje porady prawnej ani umowy z bankiem. W razie zdarzenia liczą się komunikaty Twojego banku, CERT Polska i policji.

Jedna zasada na każdą sytuację

Mail, telefon, SMS, komunikator albo odpowiedź z czatu AI. Przestępcy zmieniają kanał, ale zawsze chcą tego samego: pośpiechu i Twojego zaufania.

1 **⊘ Stop**
Ktoś Cię pogania albo chodzi o pieniądze, hasło, kod lub instalację programu? Zatrzymaj się.

2 **Sprawdź**
Innym kanałem, który sam znasz: numer z umowy, a nie z maila, SMS-a ani odpowiedzi AI.

3 **Zgłoś**
Osobie od IT i na incydent.cert.pl. Także wtedy, gdy nic się nie stało.

TEST W 10 SEKUND

1. Czy ktoś mnie pogania?

2. Czy chodzi o pieniądze, hasło lub kod?

3. Czy prośba przyszła jednym kanałem?

4. Czy mogę to sprawdzić sam?

Dwa razy „tak” i nie możesz sprawdzić? Nie rób nic więcej.

Co znajdziesz w środku

Jedna zasada na każdą sytuację 3

01 Poczta 5

1.1 Faktura z nowym kontem 6
1.2 Mail z urzędu 8
1.3 Zamówienie w załączniku 10
1.4 Skrzynka pełna 12
1.5 Dziwny mail od Ciebie 14

02 Telefon 17

2.1 Dzwoni „bank” 18
2.2 Zdalny pulpit 20
2.3 Mundur na wideo 22
2.4 Głos szefa 24
2.5 Nowy numer 26
2.6 Kod SMS i BLIK 28

03 AI 31

3.1 Numer z AI 32
3.2 Dane w czacie 34
3.3 Program z polecenia AI 36
3.4 Decyzja z AI 38

04 Sprzęt i dostęp 41

4.1 Zgubiony laptop 42
4.2 Znaleziony pendrive 44
4.3 Dostęp dla firmy 46
4.4 Odejście pracownika 48
4.5 Jedno hasło 50

05 Pierwsza godzina 53

5.1 Podane hasło 54
5.2 Szyfrowanie plików 56
5.3 Przelew do oszusta 58
5.4 Przejęty fanpage 60
5.5 Wyciek danych 62

10 decyzji właściciela s. 64

Szkolenie w 30 minut s. 65

Źródła s. 66

Karta na biurko s. 68

Poczta 01

Najdroższe oszustwa w firmach zaczynają się od maila, który wygląda zupełnie zwyczajnie.



4 mln zł

Tyle straciły firmy, którym przestępcy podmieniali numery kont na fakturach z przejętych skrzynek.
Komunikat CBZC, 12.08.2026

1.1 Faktura z nowym kontem

1.2 Mail z urzędu

1.3 Zamówienie w załączniku

1.4 Skrzynka pełna

1.5 Dziwny mail od Ciebie

Kontrahent przysyła fakturę z nowym numerem konta

Nie płać, dopóki nie potwierdzisz zmiany telefonem na numer, który znasz. Brak potwierdzenia to brak przelewu.

KROK PO KROKU

1 **Przyszła faktura z nowym numerem.** Nawet z prawdziwego adresu kontrahenta.

↓

2 **Zadzwoń na numer, który znasz:** z umowy albo starej faktury. Nie z tego maila.

↓

Potwierdził zmianę?

NIE ALBO BRAK KONTAKTU

⊘ Stop

Nie płać. Przekaż mail osobie od IT i zgłoś na incydent.cert.pl.

TAK

☑ Sprawdź

Konto na białej liście VAT przy tym NIP. Zgadza się? Zapłać i zapisz, kto potwierdził.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- „zmieniliśmy bank”
- „trwa audyt”
- „stare konto zablokowane”
- „prosimy pilnie”
- „prosimy o dyskrecję”

Zrób

- ✓ Dzwoń na numer z umowy albo starej faktury
- ✓ Sprawdź konto na białej liście VAT
- ✓ Zapisz, kto i kiedy potwierdził zmianę

Nie rób

- ✕ Nie odpisuj na tego maila. Odpowie przestępca
- ✕ Nie płać „na razie połowy”
- ✕ Nie dzwoń na numer podany w mailu

JAK TO WYGLĄDAŁO NAPRAWDĘ

235 500 zł

Faktura z prawdziwego adresu sprzedawcy, ale z podmienionym kontem. Kupujący nie dodzwonił się, więc zapłacił. Sąd Najwyższy: bank nie musi sprawdzać, czy nazwa odbiorcy pasuje do numeru. Strata została w firmach.

Sąd Najwyższy, wyrok z 9.04.2025, II CSKP 966/23

! Decyzja dla właściciela

Każda zmiana konta: telefon na znany numer i podpis osoby, która zatwierdza przelewy. Bez wyjątków.

SPRAWDŹ SIĘ

Mail od stałego dostawcy, stopka i podpis jak zawsze, w treści nowy numer konta. Płacisz?

Nie. Najpierw telefon na numer z umowy. Prawdziwy adres nadawcy niczego nie dowodzi.

ZGŁOŚ	ONLINE	KONTRAHENT
Osobie od IT	**incydent.cert.pl**	**Uprzedź telefonem**

Mail „z urzędu skarbowego” każe kliknąć i poprawić JPK

Nie klikaj. Urząd nie przysyła linków do logowania. Sprawdź sprawę sam w e-Urzędzie Skarbowym albo na infolinii KAS.

KROK PO KROKU

1. **Mail z „urzędu” każe coś poprawić albo zapłacić.** Często z terminem 24 godzin.
2. **Nie klikaj linku.** Wejdź sam na podatki.gov.pl albo zadzwoń: 22 330 03 30.

Urząd potwierdza sprawę?

NIE

⊘ Stop

To oszustwo. Nie klikaj, nie odpisuj. Przekaż mail osobie od IT i zgłoś na incydent.cert.pl.

TAK

☑ Załatw sam

W e-Urzędzie Skarbowym, wchodząc z własnej zakładki, nie z maila.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- „korekta JPK_VAT”
- „pilne wezwanie”
- „kliknij, aby zweryfikować”
- „konto zostanie zablokowane”
- załącznik .zip

Zrób

- ✓ Wpisz adres urzędu sam
- ✓ Infolinia KAS: 22 330 03 30
- ✓ Najpierw pokaż mail księgowej

Nie rób

- ✕ Nie loguj się przez link z maila
- ✕ Nie otwieraj załącznika
- ✕ Nie podawaj numeru konta ani hasła

CO MÓWIĄ PRZEPISY I INSTYTUCJE

0 linków

Tyle linków mają prawdziwe powiadomienia KAS o JPK_VAT. Nie proszą też o logowanie. 16.10.2026 Ministerstwo Finansów ostrzegło przed fałszywymi mailami o „korekcie JPK_VAT", które wyłudzały dane i hasła.

Ministerstwo Finansów, podatki.gov.pl, 16.10.2026

! Decyzja dla właściciela

Ustal, kto odbiera pocztę z urzędów, i zasadę: sprawy urzędowe tylko przez e-Urząd i e-Doręczenia.

SPRAWDŹ SIĘ

Mail z logo KAS: „Wykryto błąd w JPK_VAT, popraw w 24 godziny", obok link do logowania. Co robisz?

Nie klikasz. Logujesz się sam do e-Urzędu Skarbowego albo dzwonisz na infolinię KAS.

ZGŁOŚ	ONLINE	INFOLINIA KAS
Osobie od IT	**incydent.cert.pl**	**22 330 03 30**

Nowy klient przysyła zamówienie w załączniku

Nie otwieraj archiwów ani plików programów. Poproś o zamówienie w treści maila albo pokaż plik osobie od IT.

KROK PO KROKU

1 **Nieznany nadawca, „zamówienie” w załączniku.** Albo „zapytanie ofertowe”.

↓

2 **Sprawdź rodzaj pliku:** .zip, .rar, .iso, .exe, .bat to czerwona flaga.

↓

To PDF od firmy, która istnieje?

NIE

⊘ Stop

Nie otwieraj. Nie uruchamiaj „żeby zobaczyć, co to”. Przekaż mail osobie od IT.

TAK

☑ Ostrożnie

Firma jest w KRS lub CEIDG? Odpowiedz i poproś o zamówienie w treści maila.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- „pilne zamówienie”
- „zapytanie ofertowe”
- plik .zip albo .rar
- nadawca z obcej domeny
- „otwórz, aby zobaczyć ceny”

Zrób

- ✓ Sprawdź firmę w KRS albo CEIDG
- ✓ Poproś o zamówienie w treści maila
- ✓ Pokaż podejrzany plik osobie od IT

Nie rób

- ✕ Nie otwieraj archiwów od nieznanych
- ✕ Nie włączaj makr w dokumentach
- ✕ Nie uruchamiaj plików .exe, .iso, .bat

JAK TO WYGLĄDAŁO NAPRAWDĘ

1 plik

W lipcu 2026 CERT Polska ostrzegał przed kampanią skierowaną do małych i średnich firm. „Klient” przysyłał zamówienie albo zapytanie ofertowe, a otwarcie załącznika instalowało program, który dawał przestępcy zdalny dostęp do komputera.

CERT Polska, ostrzeżenie z lipca 2026 (omówienia: Bankier.pl, 21.07.2026; money.pl)

! **Decyzja dla właściciela**

Poproś osobę od IT o blokadę plików programów w poczcie i o kopię zapasową, której infekcja nie zaszyfruje.

SPRAWDŹ SIĘ

„Dzień dobry, w załączniku zamówienie na 40 palet, prosimy o pilną wycenę”. Plik: zamowienie.zip. Otwierasz?

Nie. Prosisz o zamówienie w treści maila i sprawdzasz firmę w rejestrze.

ZGŁOŚ	ONLINE	PLIK
Osobie od IT	**incydent.cert.pl**	**Nie otwieraj**

„Twoja skrzynka jest pełna. Zaloguj się, żeby nie stracić poczty”

Nie loguj się z linku. Otwórz pocztę sam, tak jak zawsze, i sprawdź, czy komunikat jest tam.

KROK PO KROKU

1 **Mail straszy blokadą albo utratą poczty.** Albo „nietypowym logowaniem”.

↓

2 **Zamknij mail.** Otwórz pocztę sam, z zakładki albo aplikacji.

↓

Komunikat jest też w samej poczcie?

NIE

⊘ Stop

Mail był fałszywy. Usuń go i zgłoś. Hasło już podane? Przejdź do karty 5.1.

TAK

☑ Załatw tam

Zrób to, co mówi komunikat w samej poczcie, a nie w mailu.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- „skrzynka pełna”
- „ostatnie ostrzeżenie”
- „zweryfikuj konto”
- „masz 24 godziny”
- adres strony inny niż zwykle

Zrób

✓ Loguj się tylko z zakładki albo aplikacji

✓ Włącz drugi składnik logowania

✓ Pokaż mail osobie od IT

Nie rób

✕ Nie wpisuj hasła na stronie z linku

✕ Nie odpisuj na taki mail

✕ Nie przesyłaj go zespołowi „dla ostrożności”

CO MÓWIĄ PRZEPISY I INSTYTUCJE

0 próśb

Tyle razy prawdziwa firma albo instytucja poprosi Cię o login i hasło poza swoją oficjalną stroną lub aplikacją. Ministerstwo Cyfryzacji radzi: po podaniu danych na fałszywej stronie natychmiast zmień hasła.

Ministerstwo Cyfryzacji, gov.pl, komunikat o phishingu, 10.2024

! **Decyzja dla właściciela**

Włącz drugi składnik logowania na wszystkich skrzynkach firmowych. Samo wyłudzone hasło przestaje wystarczać.

SPRAWDŹ SIĘ

Mail: „Przekroczono limit skrzynki. Kliknij, aby zwiększyć miejsce”. Klikasz?

Nie. Otwierasz pocztę sam. Jeśli miejsca naprawdę brakuje, zobaczysz to w niej.

ZGŁOŚ	ONLINE	HASŁO PODANE?
Osobie od IT	**incydent.cert.pl**	**Karta 5.1**

Klient pyta, dlaczego wysłałeś mu dziwny mail

Twoja skrzynka mogła zostać przejęta. Zmień hasło z innego urządzenia i uprzedź kontrahentów telefonicznie.

KROK PO KROKU

1 **Klient dostał mail, którego nie pisałeś.** Albo fakturę z innym kontem.

↓

2 **Z innego, czystego urządzenia** zmień hasło do poczty.

↓

Masz dostęp do skrzynki?

NIE

⊘ Stop

Dzwoń teraz do osoby od IT. Odzyskanie konta idzie przez dostawcę poczty.

TAK

☑ Zabezpiecz

Wyloguj wszystkie sesje, usuń obce reguły przekierowania, włącz drugi składnik.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- klient pyta o fakturę, której nie było
- odpowiedzi, których nie pamiętasz
- nowe reguły w poczcie
- znikające maile
- logowanie z innego kraju

Zrób

✓ Zmień hasło z innego urządzenia

✓ Wyloguj wszystkie sesje w poczcie

✓ Zadzwoń do kontrahentów z ostatnich faktur

Nie rób

✕ Nie ostrzegaj klientów z tej samej skrzynki

✕ Nie kasuj śladów przed rozmową z IT

✕ Nie czekaj, aż „samo przejdzie”

JAK TO WYGLĄDAŁO NAPRAWDĘ

4 mln zł

Grupa rozbita przez CBZC w sierpniu 2026 przejmowała firmowe skrzynki, czytała korespondencję i podmieniała numery kont na fakturach. Straty firm przekroczyły 4 mln zł, a próby kolejnych wyłudzeń opiewały na 5,5 mln zł.

Komunikat CBZC, 12.08.2026 (omówienia: RMF24, TVP Info)

! Decyzja dla właściciela

Ustal z góry, kto i jak uprzedza klientów, gdy skrzynka zostanie przejęta. Telefonem, nie mailem.

SPRAWDŹ SIĘ

Klient: „Dostałem od Pana nowy numer konta, wszystko w porządku?”. Nie wysyłałeś. Co najpierw?

Mówisz klientowi, żeby nie płacił, zmieniasz hasło z innego urządzenia i dzwonisz do osoby od IT.

ZGŁOŚ	ONLINE	KLIENCI
Osobie od IT	**incydent.cert.pl**	**Telefonicznie**

Trzy rzeczy do zapamiętania

☑ **Nowy numer konta potwierdzasz telefonem**

na numer z umowy albo starej faktury. Bez potwierdzenia nie ma przelewu.

☑ **Nie logujesz się z linku w mailu**

Pocztę, bank i e-Urząd Skarbowy otwierasz sam, tak jak zawsze.

☑ **Załącznik od nieznajomego pokazujesz osobie od IT**

zwłaszcza archiwa i pliki programów.

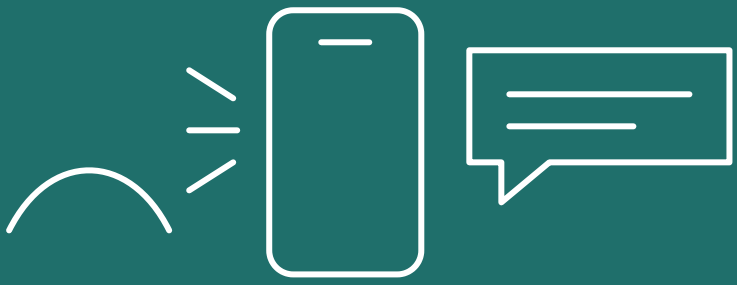
U NAS USTALONE

Zmiany kont potwierdza: _____

Pocztę z urzędów odbiera: _____

Telefon 02

Głos w słuchawce i twarz na wideo da się dziś podrobić. Bezpieczne jest tylko to, co sam sprawdzisz innym kanałem.



8080 Na ten numer przesyłasz podejrzany SMS. CERT Polska sprawdza go i blokuje niebezpieczne strony. CERT Polska

2.1 Dzwoni „bank”
2.2 Zdalny pulpit
2.3 Mundur na wideo
2.4 Głos szefa
2.5 Nowy numer
2.6 Kod SMS i BLIK

Dzwoni „bank”, „policja” albo „pomoc techniczna”

Rozłącz się i zadzwoń sam na numer z karty albo strony banku. Bank nie każe przelewać na „bezpieczne konto”.

KROK PO KROKU

1 **Ktoś z banku, policji albo pomocy technicznej** mówi, że pieniądze są zagrożone.

↓

2 **Rozłącz się.** Zadzwoń sam na numer z karty albo strony banku.

↓

Bank potwierdza sprawę?

NIE

⊘ Stop

To było oszustwo. Nic nie przelewaj, niczego nie instaluj. Zgłoś próbę w banku.

TAK

☑ Rozmawiaj

Na połączeniu, które sam wykonałeś na znany numer.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- „pieniądze są zagrożone”
- „konto techniczne”
- „proszę się nie rozłączać”
- „nikomu o tym nie mówić”
- prośba o instalację aplikacji

Zrób

✓ Rozłącz się i oddzwoń na numer z karty

✓ Sprawdź rozmówcę w aplikacji banku, jeśli bank to oferuje

✓ Zgłoś próbę oszustwa w banku

Nie rób

✕ Nie przelewaj na „bezpieczne konto”

✕ Nie podawaj kodów ani PIN

✕ Nie instaluj niczego na prośbę dzwoniącego

CO MÓWIĄ PRZEPISY I INSTYTUCJE

Ten sam numer

CBZC i Komenda Główna Policji ostrzegają: podczas fałszywego połączenia na ekranie może się wyświetlić prawdziwy numer albo nazwa banku. Numer na wyświetlaczu niczego nie dowodzi.

Komunikat CBZC i KGP z 10.01.2023

! **Decyzja dla właściciela**

Przekaż zespołowi jedno zdanie: bank, policja ani informatyk nie każą przelewać pieniędzy na „bezpieczne konto”.

SPRAWDŹ SIĘ

„Dział bezpieczeństwa banku. Ktoś wyprowadza środki z konta firmy, przeniesiemy je na konto techniczne”. Co robisz?

Rozłączasz się i dzwonisz sam na numer z karty albo strony banku. „Konto techniczne” to znak oszustwa.

BANK	POLICJA	ONLINE
Numer z karty	**Zawiadomienie**	**incydent.cert.pl**

Ktoś prosi o zainstalowanie programu do zdalnej pomocy

Nie instaluj. Zdalnie łączy się z Twoim komputerem tylko Wasza osoba od IT i to Ty wiesz, że to ona.

KROK PO KROKU

1 **Ktoś prosi o instalację programu,** „żeby pomóc” albo „zabezpieczyć konto”.

↓

2 **Zapytaj siebie: czy to nasza osoba od IT,** z którą firma ma umowę?

↓

Połączenie zleciła Twoja firma?

NIE

⊘ Stop

Nie instaluj. Rozłącz się. Program już działa? Odłącz internet i dzwoń do IT.

TAK

☑ Tylko IT

Połączenie zaczyna Wasza osoba od IT, widzisz je i możesz przerwać.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- „pomogę Panu zdalnie”
- „proszę pobrać AnyDesk”
- „proszę podać kod z ekranu”
- pośpiech
- pomoc, której nie zamawiałeś

Zrób

✓ Pomoc zdalna tylko od Waszej osoby od IT

✓ Odłącz internet, jeśli program już działa

✓ Zgłoś zdarzenie od razu

Nie rób

✕ Nie podawaj kodu połączenia z ekranu

✕ Nie loguj się do banku przy zdalnym pulpicie

✕ Nie instaluj aplikacji z linku od rozmówcy

CO MÓWIĄ PRZEPISY I INSTYTUCJE

AnyDesk

Banki ostrzegają: przestępcy podający się za pracowników banku nakłaniają do instalacji programów do zdalnego pulpitu, takich jak AnyDesk czy TeamViewer, a potem przejmują urządzenie.

mBank, komunikaty o aplikacjach do zdalnego pulpitu, odczyt 28.11.2026

! **Decyzja dla właściciela**

Spisz, kto może łączyć się zdalnie z komputerami firmy. Każda inna prośba o zdalny dostęp to stop.

SPRAWDŹ SIĘ

Dzwoni „pomoc techniczna”: wykryto wirusa, trzeba połączyć się zdalnie. Instalujesz?

Nie. Rozłączasz się i informujesz Waszą osobę od IT. Producenci nie dzwonią sami w takich sprawach.

ZGŁOŚ	BANK	ONLINE
Osobie od IT	**Numer z karty**	**incydent.cert.pl**

Rozmówca na wideo pokazuje mundur albo legitymację

Obraz z kamery nie potwierdza, kim jest rozmówca. Rozłącz się i zadzwoń sam na 112 albo do komendy.

KROK PO KROKU

1 **Rozmowa wideo: mundur, legitymacja, pieczątka.** Straszą utratą oszczędności.

↓

2 **Rozłącz się.** Zadzwoń na 112 albo do komendy z oficjalnej strony.

↓

Policja potwierdza sprawę?

NIE

⊘ Stop

Oszustwo. Policja nie każe przelewać pieniędzy. Złóż zawiadomienie.

TAK

☑ Współpracuj

Na komendzie albo przez numer, który sam znalazłeś.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- rozmowa przez komunikator
- „sprawa jest tajna”
- „bezpieczne konto”
- „nie mówić w banku”
- legitymacja tuż przy kamerze

Zrób

- ✓ Rozłącz się i zadzwoń sam
- ✓ Porozmawiaj z kimś zaufanym przed decyzją
- ✓ Zgłoś próbę na policji

Nie rób

- ✕ Nie przelewaj i nie wypłacaj gotówki
- ✕ Nie instaluj aplikacji na prośbę rozmówcy
- ✕ Nie dochowuj „tajemnicy śledztwa” przed bankiem

JAK TO WYGLĄDAŁO NAPRAWDĘ

Mundur

21 lipca 2026 Komenda Główna Policji i FinCERT.pl ostrzegły przed „policjantami”, którzy dzwonią przez komunikator z kamerą, pokazują mundur i namawiają do przelewu na „bezpieczne konto”.

KGP i FinCERT.pl, 21.07.2026 (omówienie: Bankier.pl, 28.07.2026)

! Decyzja dla właściciela

Powiedz zespołowi wprost: policja, prokuratura i bank nigdy nie proszą o przelew ani wypłatę gotówki.

SPRAWDŹ SIĘ

Na wideo „policjant” w mundurze: Twoja księgowa jest podejrzana, trzeba zabezpieczyć środki firmy. Działasz?

Nie. Rozłączasz się i dzwonisz sam na 112 albo do komendy. Prawdziwa policja nie zabezpiecza pieniędzy przelewem.

ALARM	POLICJA	BANK
112	**Zawiadomienie**	**Numer z karty**

Szef prosi o pilny przelew głosem albo na wideo

Oddzwoń na numer szefa z kontaktów albo zapytaj o hasło kontrolne. Bez potwierdzenia nie ma przelewu.

KROK PO KROKU

1 **Szef dzwoni albo pisze: pilny przelew, poza procedurą.** „Jestem na spotkaniu”.

↓

2 **Oddzwoń na numer szefa z kontaktów** albo zapytaj o hasło kontrolne.

↓

Szef potwierdza na znanym numerze?

NIE

⊘ Stop

Nie przelewaj. Zgłoś. Za takie sprawdzenie nikt nie ponosi konsekwencji.

TAK

☑ Według procedury

Przelew z podpisem osoby, która go zatwierdza.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- „pilne, przed końcem dnia”
- „poza systemem”
- „nie mów nikomu”
- nowy numer albo komunikator
- głos trochę inny niż zwykle

Zrób

- ✓ Oddzwoń na numer z kontaktów
- ✓ Zapytaj o hasło kontrolne
- ✓ Trzymaj się procedury przelewów

Nie rób

- ✕ Nie przelewaj na podstawie samego głosu
- ✕ Nie odpisuj na nowym numerze
- ✕ Nie pomijaj drugiego podpisu „bo pilne”

JAK TO WYGLĄDAŁO NAPRAWDĘ

9%

pracowników w Polsce spotkało się na służbowym sprzęcie z próbą oszustwa, w której użyto sklonowanego głosu albo wizerunku znanej osoby.

„Cyberportret polskiego biznesu 2026”, ESET i DAGMA, badanie z marca 2026

! Decyzja dla właściciela

Wprowadź hasło kontrolne i zasadę: kto sprawdza polecenie szefa, nigdy nie ponosi za to konsekwencji.

SPRAWDŹ SIĘ

Głos szefa w telefonie: „Przelej 38 tys. zł kontrahentowi, faktura dojdzie później”. Co robisz?

Oddzwaniasz na numer szefa z kontaktów albo pytasz o hasło kontrolne. Bez tego nie ma przelewu.

ZGŁOŚ	SZEF	ONLINE
Osobie od IT	**Znany numer**	**incydent.cert.pl**

„Zmieniłem numer, napisz do mnie na WhatsAppie”

Zadzwoń na stary, znany numer tej osoby. Nie odpisuj na nowy, zanim nie porozmawiasz.

KROK PO KROKU

1 **SMS albo wiadomość: „to mój nowy numer”.** Zaraz potem prośba o pilny przelew.

↓

2 **Zadzwoń na stary, znany numer.** Nie odpisuj na nowy.

↓

Osoba potwierdza na starym numerze?

NIE

Stop

Nie przelewaj. Prześlij SMS na 8080 i zgłoś.

TAK

Zapisz numer

Dopiero po rozmowie na starym, znanym numerze.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- „zepsuł mi się telefon”
- „napisz na WhatsAppie”
- „pilnie potrzebuję”
- błędy w słowach „telefon”, „numer”
- prośba o BLIK

Zrób

✓ Dzwoń na stary numer

✓ Prześlij podejrzany SMS na 8080

✓ Ostrzeż osobę, pod którą się podszywano

Nie rób

✕ Nie przelewaj na prośbę z nowego numeru

✕ Nie podawaj kodów

✕ Nie dodawaj nowego numeru bez rozmowy

JAK TO WYGLĄDAŁO NAPRAWDĘ

999 na 1000

W tylu przypadkach, według eksperta CERT Orange Polska, rozmowa, w której nieznana osoba prosi o kontakt przez WhatsApp, okazuje się oszustwem.

CERT Orange Polska (omówienie: Telepolis, 20.06.2024)

! **Decyzja dla właściciela**

Zmiany numerów współpracowników i kontrahentów potwierdzamy rozmową, nigdy samą wiadomością.

SPRAWDŹ SIĘ

Wiadomość od „wspólnika”: „Mam nowy numer, przelej dziś zaliczkę dostawcy”. Co robisz?

Dzwonisz na jego stary numer. Dopóki nie porozmawiacie, nic nie przelewasz.

SMS	ONLINE	OSOBA
8080	**incydent.cert.pl**	**Stary numer**

Ktoś prosi o kod z SMS-a albo kod BLIK

Kodu nie podaje się nikomu. Kod wpisujesz sam, tylko przy operacji, którą sam zacząłeś.

KROK PO KROKU

1 **Ktoś prosi o kod z SMS-a albo BLIK.** Przez telefon, w czacie albo na portalu ogłoszeń.

↓

2 **Przeczytaj, czego dotyczy kod:** przelewu, logowania, nowego urządzenia?

↓

To Ty zlecasz tę operację?

NIE

⊘ Stop

Nie podawaj kodu. Zakończ rozmowę albo czat. Kod już podany? Dzwoń do banku.

TAK

☑ Wpisz sam

Tylko w swojej aplikacji, przy operacji, którą sam zacząłeś.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- prośba o BLIK z konta znajomego
- „to tylko weryfikacja”
- „zwrot nadpłaty”
- „zatwierdź BLIK”
- „kupujący” z portalu ogłoszeń

Zrób

- ✓ Czytaj treść SMS-a z kodem
- ✓ Wpisuj kody tylko u siebie
- ✓ Dzwoń do banku, gdy coś podałeś

Nie rób

- ✕ Nie dyktuj kodów przez telefon
- ✕ Nie zatwierdzaj BLIK, którego nie zlecałeś
- ✕ Nie przesyłaj zrzutów ekranu z kodem

CO MÓWIĄ PRZEPISY I INSTYTUCJE

0 kodów

O tyle kodów poprosi Cię w rozmowie prawdziwy bank, policja albo kurier. Ministerstwo Cyfryzacji: przedstawiciele banku nigdy nie poproszą o PIN, ani na stronie, ani przez telefon.

Ministerstwo Cyfryzacji, gov.pl, 10.2024; KGP i operator BLIK, odczyt 28.11.2026

! Decyzja dla właściciela

Kody z banku widzi i wpisuje tylko osoba, która zleca operację. Nikt jej o nie nie pyta.

SPRAWDŹ SIĘ

„Kurier”: żeby doręczyć paczkę, potrzebuje kodu, który zaraz przyjdzie SMS-em. Podajesz?

Nie. Kod z SMS-a zatwierdza operację w banku albo logowanie. Kurier nigdy go nie potrzebuje.

BANK	SMS	ONLINE
Numer z karty	**8080**	**incydent.cert.pl**

Trzy rzeczy do zapamiętania

☑ **Rozłączasz się i dzwonisz sam**

na numer z karty, umowy albo kontaktów. Nigdy na numer podany przez rozmówcę.

☑ **Głos i obraz niczego nie dowodzą**

Polecenie przelewu potwierdzasz oddzwonieniem albo hasłem kontrolnym.

☑ **Kodów i zdalnego dostępu nie dajesz nikomu**

Kod wpisujesz sam, a zdalnie łączy się tylko Wasza osoba od IT.

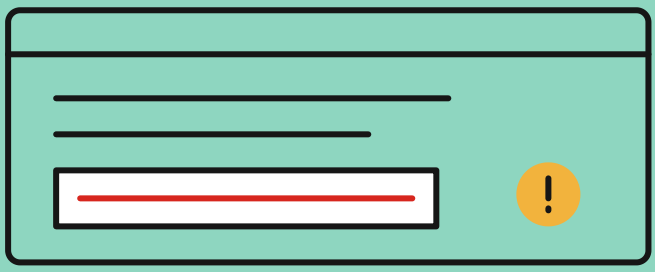
U NAS USTALONE

Hasło kontrolne znają: _____

Zdalnie może łączyć się: _____

AI 03

Czat podpowiada szybko i pewnym tonem. To nie znaczy, że ma rację ani że wie, czyj to numer telefonu.



62% pracowników w Polsce korzysta z AI w pracy. Zasady na piśmie ma 27% firm. ESET i DAGMA, 2026

3.1 Numer z AI

3.2 Dane w czacie

3.3 Program z polecenia AI

3.4 Decyzja z AI

Czat albo podsumowanie AI podaje numer infolinii lub link

Numer i adres bierz z umowy, faktury albo oficjalnej strony wpisanej samemu. Odpowiedź AI może podać numer oszusta.

KROK PO KROKU

1 **Czat albo podsumowanie AI podaje numer lub link.** Do banku, kuriera, dostawcy.

↓

2 **Weź numer z umowy albo faktury** lub ze strony, której adres wpisujesz sam.

↓

Numery się zgadzają?

NIE

⊘ Stop

Nie dzwoń i nie klikaj. Zgłoś błędną odpowiedź w narzędziu.

TAK

☑ Dzwoń

Na numer z dokumentu, nie z czatu.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- numer inny niż na fakturze
- link do nieznanej domeny
- „infolinia 24/7”
- prośba o udostępnienie ekranu
- opłata za „pomoc”

Zrób

✓ Numery bierz z umów i faktur

✓ Adres strony wpisuj sam

✓ Zapisz ważne numery w kontaktach firmy

Nie rób

✕ Nie dzwoń pod numer z AI bez sprawdzenia

✕ Nie loguj się z linku z czatu

✕ Nie udostępniaj ekranu „konsultantowi”

JAK TO WYGLĄDAŁO NAPRAWDĘ

1 telefon

Media opisały klienta, który zadzwonił pod numer linii wycieczkowej podany w podsumowaniu AI Google. Po drugiej stronie był oszust. Podobne fałszywe numery trafiały też do odpowiedzi czatów.

Washington Post, 08.2025 (omówienia: Interia, Spider’s Web)

! **Decyzja dla właściciela**

Zrób firmową listę ważnych numerów: bank, kurier, dostawcy, IT. Powieś ją obok karty na biurko.

SPRAWDŹ SIĘ

Pytasz czat o numer infolinii firmy kurierskiej. Dostajesz numer i link. Dzwonisz?

Najpierw porównujesz z numerem z umowy albo oficjalnej strony, której adres wpisujesz sam.

ZGŁOŚ	ONLINE	LISTA
Osobie od IT	**incydent.cert.pl**	**Numery firmy**

Pracownik chce wkleić dane klienta do czatu AI

Wklejaj tylko do narzędzia zatwierdzonego przez firmę i tylko dane, na które pozwalają zasady. Gdy nie wiesz, zapytaj.

KROK PO KROKU

1 **Chcesz wkleić umowę, dane klienta albo arkusz.** „Żeby szybciej podsumować”.

↓

2 **Sprawdź firmowe zasady:** które narzędzie i jakie dane są dozwolone.

↓

Narzędzie i dane są dozwolone?

NIE

⊘ Stop

Nie wklejaj. Usuń nazwiska i numery albo zapytaj osobę od IT.

TAK

☑ Pracuj

W zatwierdzonym narzędziu, na koncie firmowym.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- prywatne konto w czacie
- nazwiska i PESEL-e w tekście
- umowy i ceny
- hasła albo klucze
- „to tylko na chwilę”

Zrób

✓ Używaj narzędzia zatwierdzonego przez firmę

✓ Usuwaj nazwiska, PESEL-e i numery kont

✓ Pytaj, gdy nie wiesz

Nie rób

✕ Nie wklejaj haseł ani kluczy

✕ Nie używaj prywatnego konta do danych firmy

✕ Nie wrzucaj całych baz klientów

JAK TO WYGLĄDAŁO NAPRAWDĘ

27%

firm ma spisane zasady korzystania z AI, a z AI w pracy korzysta 62% pracowników. W pozostałych firmach każdy decyduje sam, co wkleja do czatu.

„Cyberportret polskiego biznesu 2026", ESET i DAGMA

! Decyzja dla właściciela

Spisz zasady AI na jednej stronie: jedno zatwierdzone narzędzie, czego nie wklejamy i kogo pytać.

SPRAWDŹ SIĘ

Pracownik wkleja do darmowego czatu listę 200 klientów z adresami, „żeby posortować". Problem?

Tak. Dane klientów trafiają poza firmowe zasady. Sortuje się w arkuszu, a AI dostaje dane bez nazwisk.

PYTAJ	ZASADY AI	WYCIEK?
Osobę od IT	**1 strona**	**Karta 5.5**

AI poleca program, wtyczkę albo aplikację do zainstalowania

Instaluje tylko osoba od IT, z oficjalnej strony producenta. AI potrafi polecić coś, co nie istnieje albo jest pułapką.

KROK PO KROKU

1 **Czat poleca program, wtyczkę albo rozszerzenie.** „Zainstaluj, to rozwiąże problem”.

↓

2 **Zapytaj osobę od IT,** czy to znany produkt z oficjalnego źródła.

↓

IT zatwierdza instalację?

NIE

⊘ Stop

Nie instaluj. Zostaw to osobie od IT.

TAK

☑ Instaluje IT

Z oficjalnej strony producenta, według listy programów firmy.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- nazwa, której nikt nie zna
- link do pobrania z czatu
- „darmowa pełna wersja”
- dostęp do wszystkich stron
- prośba o prawa administratora

Zrób

✓ Instaluje tylko osoba od IT

✓ Pobieraj z oficjalnej strony producenta

✓ Pracuj na koncie bez uprawnień administratora

Nie rób

✕ Nie instaluj nic z linku z czatu

✕ Nie wklejaj do systemu poleceń z czatu

✕ Nie dawaj rozszerzeniom dostępu do wszystkiego

JAK TO WYGLĄDAŁO NAPRAWDĘ

20%

próbek kodu wygenerowanych przez modele AI w badaniu z 2025 roku polecało pakiet, który nie istniał. Przestępcy rejestrują takie wymyślone nazwy i wkładają w nie złośliwy kod.

USENIX Security 2025, 576 tys. próbek kodu z 16 modeli

! Decyzja dla właściciela

Odbierz pracownikom uprawnienia administratora. Programy instaluje osoba od IT, według listy.

SPRAWDŹ SIĘ

Czat radzi zainstalować nieznane rozszerzenie, które „naprawi plik PDF”. Instalujesz?

Nie. Pytasz osobę od IT. Nieznane rozszerzenie z polecenia AI to typowa furtka dla złośliwego kodu.

ZGŁOŚ	ONLINE	INSTALUJE
Osobie od IT	**incydent.cert.pl**	**Tylko IT**

Chcesz podjąć decyzję na podstawie odpowiedzi AI

Liczby, przepisy, terminy i wyroki sprawdzaj u źródła. Za tekst z AI odpowiada ten, kto go podpisuje.

KROK PO KROKU

1 **AI podaje przepis, termin, stawkę albo wyrok.** Brzmi pewnie i konkretnie.

↓

2 **Sprawdź u źródła:** ustawa, urząd, umowa, księgowa.

↓

Źródło to potwierdza?

NIE

Stop

Nie decyduj na tej podstawie. Zapytaj specjalistę.

TAK

Działaj

I zapisz, skąd wiesz, że to prawda.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- brak linku do źródła
- sygnatura, której nie ma
- „zgodnie z art.”
- argument pasuje idealnie
- bardzo pewny ton

Zrób

- ✓ Sprawdzaj liczby i przepisy u źródła
- ✓ Proś AI o źródła i otwieraj je
- ✓ Konsultuj sprawy prawne i podatkowe

Nie rób

- ✕ Nie podpisuj pisma z AI bez sprawdzenia
- ✕ Nie wysyłaj klientom „faktów” z czatu
- ✕ Nie traktuj pewnego tonu jak dowodu

JAK TO WYGLĄDAŁO NAPRAWDĘ

3 orzeczenia

Pełnomocnik przedsiębiorcy powołał w zażaleniu do NSA trzy orzeczenia. Żadne nie mówiło tego, co napisał. Sąd skrytykował bezrefleksyjne korzystanie z AI przez zawodowego pełnomocnika.

NSA, postanowienie z 23.06.2026, I FZ 104/26

! **Decyzja dla właściciela**

Ustal zasadę: za każdy tekst z AI odpowiada osoba, która go podpisuje i wysyła.

SPRAWDŹ SIĘ

Czat podaje termin zapłaty podatku i numer przepisu. Wpisujesz do kalendarza?

Dopiero po sprawdzeniu u źródła: na stronie urzędu albo u księgowej.

PYTAJ	ŹRÓDŁO	ODPOWIADA
Księgowa, prawnik	**Zawsze link**	**Kto podpisuje**

Trzy rzeczy do zapamiętania

- [x] **Numery, linki i programy bierzesz ze źródła**

  z umowy albo oficjalnej strony, nie z odpowiedzi czatu.

- [x] **Do czatu trafia tylko to, na co pozwalają zasady**

  i tylko w narzędziu zatwierdzonym przez firmę.

- [x] **Za tekst z AI odpowiada ten, kto go podpisuje**

  Liczby, przepisy i terminy sprawdzasz u źródła.

U NAS USTALONE

Zatwierdzone narzędzie AI: _____

O dane w czacie pytamy: _____

Sprzęt i dostęp

04

Laptopy, pendrive’y, hasła i konta byłych pracowników. Najczęściej zawodzi to, czego nikt nie spisał.



85% firm w Polsce miało w ostatnim roku incydent cyberbezpieczeństwa. ESET i DAGMA, 2026

4.1 Zgubiony laptop

4.2 Znaleziony pendrive

4.3 Dostęp dla firmy

4.4 Odejście pracownika

4.5 Jedno hasło

Zginął laptop albo telefon służbowy

Zgłoś od razu, nawet jeśli „może się znajdzie”. Zmień hasła, zablokuj urządzenie zdalnie i oceń, czy wyciekły dane.

KROK PO KROKU

1. **Laptop albo telefon zginął lub został skradziony.** W pracy, w aucie, w podróży.
2. **Zgłoś od razu osobie od IT.** Liczy się każda godzina.

Dysk był zaszyfrowany?

NIE ALBO NIE WIEM

⊘ Pilnie

Zmień hasła, zablokuj urządzenie i oceń z IT, czy zgłosić naruszenie.

TAK

☑ Zablokuj

Zablokuj i wyczyść zdalnie, zmień hasła do kont z tego urządzenia.

CO SPRAWDZIĆ OD RAZU

- szyfrowanie dysku
- klucz odzyskiwania
- hasła zapisane w przeglądarce
- poczta na telefonie
- aplikacja banku

Zrób

- ✓ Zgłoś zgubienie w ciągu godziny
- ✓ Zmień hasła do poczty i banku
- ✓ Zablokuj urządzenie zdalnie

Nie rób

- ✕ Nie czekaj, aż „może się znajdzie”
- ✕ Nie zostawiaj laptopa w aucie na widoku
- ✕ Nie trzymaj haseł w pliku na pulpicie

JAK TO WYGLĄDAŁO NAPRAWDĘ

15 tys. zł

Służbowy laptop z danymi skradziono z samochodu w czasie delegacji. Szyfrowanie dysku było w jej własnych zaleceniach, ale włączono je dopiero po kradzieży. NSA utrzymał karę UODO 3 listopada 2026.

NSA, wyrok z 3.11.2026 (omówienie: prawo.pl, 11.2026)

! **Decyzja dla właściciela**

Szyfrowanie na każdym laptopie i telefonie służbowym, klucze odzyskiwania w jednym bezpiecznym miejscu.

SPRAWDŹ SIĘ

Handlowiec zgubił w pociągu laptop. Hasło do systemu było. To wystarczy?

Nie. Hasło do systemu nie zastępuje szyfrowania dysku. Zgłoś od razu i zmieńcie hasła.

ZGŁOŚ	KRADZIEŻ	DANE OSÓB
Osobie od IT	**Policja**	**Ocena 72 h**

Ktoś znalazł pendrive na parkingu albo w biurze

Nie podłączaj go do żadnego komputera. Oddaj osobie od IT. Nieznany nośnik to najprostszy sposób na wirusa.

KROK PO KROKU

1. **Na parkingu albo w biurze leży pendrive.** Czasem z napisem „wypłaty” albo „poufne”.

2. **Nie podłączaj go nigdzie.** Nawet „żeby oddać właścicielowi”.

Osoba od IT może go sprawdzić?

NIE

Nie podłączaj

Zniszcz albo zachowaj do decyzji IT. Nie sprawdzaj sam.

TAK

Oddaj IT

Sprawdzi go na odizolowanym komputerze albo zniszczy.

PO CZYM POZNASZ PUŁAPKĘ

- napis „wypłaty” albo „poufne”
- leży przy wejściu
- brak właściciela
- nowy, nieużywany
- zostawiony na recepcji

Zrób

✓ Oddaj nośnik osobie od IT

✓ Szyfruj własne pendrive'y z danymi

✓ Przenoś pliki przez firmowy dysk w chmurze

Nie rób

✕ Nie podłączaj nieznanych nośników

✕ Nie otwieraj plików „żeby znaleźć właściciela"

✕ Nie noś danych klientów na prywatnym pendrivie

JAK TO WYGLĄDAŁO NAPRAWDĘ

10 tys. zł

Tyle wyniosła kara dla sądu rejonowego po zgubieniu przez kuratora niezaszyfrowanego pendrive'a z danymi 400 osób. NSA ją utrzymał. Nośnik łatwo zgubić, a nieznany łatwo podrzucić.

Decyzja UODO DKN.5131.22.2021; WSA II SA/Wa 3309/21; NSA (omówienie: prawo.pl, 30.09.2024)

! Decyzja dla właściciela

Zdecyduj, czy firma w ogóle używa pendrive'ów. Jeśli tak: tylko szyfrowane i spisane.

SPRAWDŹ SIĘ

Na recepcji leży pendrive z naklejką „Premie 2026". Sprawdzisz, czyj to?

Nie podłączasz go. Oddajesz osobie od IT.

ODDAJ	SWÓJ ZGUBIONY	ONLINE
Osobie od IT	**Zgłoś od razu**	**incydent.cert.pl**

Firma zewnętrzna prosi o stały dostęp do Waszych systemów

Dostęp tylko imienny, tylko do potrzebnego systemu, z datą końca i wpisem w umowie. Nigdy „admin na zawsze”.

KROK PO KROKU

1 **Dostawca programu albo serwisant chce stałego dostępu.** „Żeby szybciej pomagać”.

↓

2 **Ustal: kto, do czego, na jak długo** i jak to zapisać w umowie.

↓

Dostęp jest w umowie i ma datę końca?

NIE

⊘ Nie dawaj

Bez umowy, imiennego konta i daty końca nie ma dostępu.

TAK

☑ Daj wąski

Imienne konto, tylko do potrzebnego systemu, wyłączane po pracy.

PO CZYM POZNASZ, ŻE COŚ JEST NIE TAK

- „dajcie nam admina”
- jedno konto dla całej firmy serwisowej
- hasło przesłane mailem
- dostęp „na zawsze”
- brak umowy powierzenia danych

Zrób

✓ Imienne konto dla każdej osoby z zewnątrz

✓ Dostęp tylko do potrzebnego systemu

✓ Co kwartał przegląd, kto ma dostęp

Nie rób

✕ Nie dawaj admina „na wszelki wypadek”

✕ Nie przesyłaj haseł mailem

✕ Nie zostawiaj dostępu po zakończeniu prac

JAK TO WYGLĄDAŁO NAPRAWDĘ

350 tys. zł

Firma straciła dostęp do danych po ataku ransomware. Zewnętrzny informatyk przez lata nie informował o lukach w serwerze. UODO ukarał firmę kwotą ponad 350 tys. zł, a informatyka kwotą 9,8 tys. zł.

Decyzja Prezesa UODO z 12.11.2024

! Decyzja dla właściciela

Wymagaj od firmy IT pisemnego raportu: co jest nieaktualne i co grozi. Bez raportu nie ma przedłużenia umowy.

SPRAWDŹ SIĘ

Serwisant programu księgowego prosi o hasło administratora do serwera „na stałe”. Dajesz?

Nie. Osobne konto, tylko do programu, z datą końca i wpisem w umowie.

ZGŁOŚ	UMOWA	PRZEGLĄD
Osobie od IT	**Zakres dostępu**	**Co kwartał**

Pracownik odchodzi z firmy

W dniu odejścia zamknij wszystkie jego dostępy według listy i zmień hasła, które znał. Także gdy rozstajecie się w zgodzie.

KROK PO KROKU

1. **Pracownik kończy pracę w firmie.** Także „na dobrych warunkach”.

2. **Według listy zamknij dostępy:** poczta, programy, PUE ZUS, bank, chmura.

Wszystko zamknięte w dniu odejścia?

NIE

⊘ Zamknij dziś

Każdy dzień otwartego konta to ryzyko. Zmień też hasła wspólne.

TAK

☑ Zapisz

Datę i listę zamkniętych dostępów, podpisaną z protokołem sprzętu.

GDZIE ZOSTAJĄ DOSTĘPY

- PUE ZUS
- bankowość firmowa
- poczta i telefon
- pliki w chmurze
- portale i media społecznościowe

Zrób

✓ Prowadź listę dostępów każdego pracownika

✓ Zamknij konta w dniu odejścia

✓ Zmień hasła, które znał

Nie rób

✕ Nie zostawiaj konta „na wszelki wypadek”

✕ Nie odkładaj tego na po urlopie

✕ Nie zostawiaj telefonu z aplikacją banku

JAK TO WYGLĄDAŁO NAPRAWDĘ

5 logowań

Byłemu pracownikowi banku nie odebrano dostępu do profilu firmy w PUE ZUS. W ciągu 8 miesięcy po odejściu zalogował się tam 5 razy. NSA utrzymał decyzję UODO 6 marca 2026.

Decyzja UODO utrzymana przez NSA 6.03.2026

! **Decyzja dla właściciela**

Zrób listę kontrolną odejścia pracownika i podpisuj ją razem z protokołem zdania sprzętu.

SPRAWDŹ SIĘ

Księgowa odeszła miesiąc temu. Jej login do PUE ZUS i bankowości wciąż działa. Ryzyko?

Tak. Zamknij dostęp dziś i sprawdź historię logowań.

IT	BANK	ZUS
Lista dostępów	**Odwołaj uprawnienia**	**Odwołaj dostęp**

Całe biuro loguje się jednym hasłem

Każdy ma własne konto i własne hasło w menedżerze haseł. Na poczcie i w banku do tego drugi składnik logowania.

KROK PO KROKU

1 **Całe biuro zna jedno hasło.** Do poczty, programu albo komputera.

↓

2 **Każdy dostaje własne konto** i własne hasło w menedżerze haseł.

↓

Każdy ma własne konto?

NIE

⊘ Zmień to

Do czasu zmiany: hasło wspólne zmieniaj po każdym odejściu i nie wysyłaj go mailem.

TAK

☑ Dobrze

Dołóż drugi składnik logowania na poczcie i w banku.

PO CZYM POZNASZ PROBLEM

- hasło na karteczce przy monitorze
- hasło w mailu do zespołu
- „wszyscy znają hasło”
- to samo hasło w kilku miejscach
- nikt nie wie, kto je zmienił

Zrób

- ✓ Osobne konto dla każdej osoby
- ✓ Menedżer haseł dla firmy
- ✓ Drugi składnik na poczcie i w banku

Nie rób

- ✕ Nie wysyłaj haseł mailem ani SMS-em
- ✕ Nie zapisuj ich na karteczkach
- ✕ Nie używaj jednego hasła w kilku miejscach

CO MÓWIĄ PRZEPISY I INSTYTUCJE

1 hasło

Przy jednym wspólnym haśle nie da się ustalić, kto co zrobił. CERT Polska zaleca zmieniać hasło wtedy, gdy mogła je poznać inna osoba. Przy haśle całego biura to jest zawsze.

CERT Polska, rekomendacje dotyczące haseł, 01.2022; poradnik o poczcie, odczyt 28.11.2026

! Decyzja dla właściciela

Wprowadź menedżer haseł dla firmy. Hasła wspólne tylko tam, gdzie nie da się inaczej.

SPRAWDŹ SIĘ

Hasło do programu magazynowego zna 6 osób, w tym dwie, które już odeszły. Co robisz?

Zmieniasz hasło dziś i zakładasz osobne konta tam, gdzie program na to pozwala.

IT	HASŁA	ODEJŚCIE
Osobne konta	**Menedżer haseł**	**Zmień hasło**

Trzy rzeczy do zapamiętania

☑ **Zgubiony sprzęt zgłaszasz od razu**

Na zaszyfrowanym dysku nikt obcy nie odczyta plików.

☑ **Każdy ma własne konto i własne hasło**

Dostępy są imienne, z datą końca, zamykane w dniu odejścia.

☑ **Aktualizacje instalują się same**

System i programy bez aktualizacji mają znane luki. Programy instaluje osoba od IT.

U NAS USTALONE

Klucze odzyskiwania są: _____

Aktualizacji pilnuje: _____

Pierwsza godzina 05

Gdy coś już się stało, liczy się kolejność. Ten rozdział mówi, co zrobić najpierw, a czego nie ruszać.



260,8 tys. incydentów zarejestrował CERT Polska w 2025 roku, wobec 103,4 tys. rok wcześniej.
CERT Polska

5.1 Podane hasło

5.2 Szyfrowanie plików

5.3 Przelew do oszusta

5.4 Przejęty fanpage

5.5 Wyciek danych

Kliknąłem w link i podałem hasło

Nie wstydź się, liczy się czas. Z innego urządzenia zmień hasło, wyloguj wszystkie sesje i od razu zgłoś.

KROK PO KROKU

1. **Podałeś hasło albo kod na podejrzanej stronie.** Albo otworzyłeś dziwny załącznik.

2. **Z innego urządzenia zmień hasło** i wyloguj wszystkie sesje.

Udało się zmienić hasło?

NIE

⊘ Dzwoń do IT

Konto mogło zostać przejęte. Odzyskiwanie razem z osobą od IT i dostawcą usługi.

TAK

☑ Dokończ

Zmień to hasło wszędzie, gdzie go używałeś, włącz drugi składnik i zgłoś.

PIERWSZA GODZINA, PO KOLEI

zmiana hasła · **wylogowanie sesji** · **drugi składnik** · **reguły w poczcie** · **zgłoszenie do IT**

Zrób

- ✓ Zmień hasło z innego urządzenia
- ✓ Wyloguj wszystkie aktywne sesje
- ✓ Zgłoś to od razu, bez wstydu

Nie rób

- ✕ Nie ukrywaj błędu
- ✕ Nie loguj się dalej z zainfekowanego komputera
- ✕ Nie czekaj, aż coś się stanie

CO MÓWIĄ PRZEPISY I INSTYTUCJE

Teraz

Ministerstwo Cyfryzacji: jeśli podałeś dane na fałszywej stronie albo uruchomiłeś podejrzany załącznik, natychmiast zmień hasła. CERT Polska dodaje: sprawdź historię logowań i zakończ aktywne sesje.

Ministerstwo Cyfryzacji, gov.pl, 10.2024; CERT Polska, poradnik o poczcie, odczyt 28.11.2026

! **Decyzja dla właściciela**

Powiedz zespołowi głośno: za zgłoszenie własnego błędu nikt nie zostanie ukarany. Ukryty błąd kosztuje więcej.

SPRAWDŹ SIĘ

Pracownik po godzinie przyznaje, że wpisał hasło na dziwnej stronie. Jak reagujesz?

Dziękujesz za zgłoszenie i od razu zmieniacie hasło. Złość sprawi, że następnym razem nikt nic nie powie.

ZGŁOŚ	ONLINE	BANK?
Osobie od IT	**incydent.cert.pl**	**Numer z karty**

Pliki przestają się otwierać, na ekranie żądanie okupu

Odłącz komputer od sieci i zadzwoń do osoby od IT. Nie płać od razu i niczego nie kasuj.

KROK PO KROKU

1. **Pliki zmieniają nazwy i się nie otwierają.** Na ekranie żądanie okupu.
2. **Odłącz komputer od sieci:** kabel i Wi-Fi. Zadzwoń do IT.

Masz kopię poza siecią?

NIE

⊘ Nie płać od razu

Zgłoś do CERT Polska. Zachowaj zaszyfrowane pliki: bywają narzędzia do odszyfrowania.

TAK

☑ Odtwórz

Z kopii, gdy osoba od IT oczyści komputery.

PIERWSZA GODZINA, PO KOLEI

odłącz od sieci · zdjęcie ekranu z żądaniem · telefon do IT · zgłoszenie do CERT · nie kasuj zaszyfrowanych plików

Zrób

- ✓ Odłącz zainfekowany komputer od sieci
- ✓ Zrób zdjęcie ekranu z żądaniem
- ✓ Zgłoś do CERT Polska i na policję

Nie rób

- ✕ Nie płać od razu
- ✕ Nie kasuj zaszyfrowanych plików
- ✕ Nie podłączaj dysku z kopią do zainfekowanej sieci

JAK TO WYGLĄDAŁO NAPRAWDĘ

3 godziny

Tyle wystarczyło, żeby zaszyfrować wszystkie bazy operacyjne średniej firmy logistycznej, opisanej przez ekspertów ESET. Zaczęło się od załącznika w mailu. Przez wiele dni nie mogła śledzić przesyłek ani realizować zleceń.

Eksperci ESET (Rzeczpospolita, 15.06.2026)

! **Decyzja dla właściciela**

Kopia poza siecią i test odtworzenia co kwartał. To zamienia atak w kilka godzin przestoju zamiast tygodni.

SPRAWDŹ SIĘ

Rano na ekranie żądanie okupu, pliki na dysku sieciowym się nie otwierają. Pierwszy ruch?

Odłączasz komputer od sieci i dzwonisz do osoby od IT. Bez płacenia i bez kasowania czegokolwiek.

IT	ONLINE	POLICJA
Natychmiast	**incydent.cert.pl**	**Zawiadomienie**

Pieniądze poszły na konto oszusta

Dzwoń do banku natychmiast, potem policja i CERT. Każda godzina zmniejsza szansę na zatrzymanie pieniędzy.

KROK PO KROKU

1 **Pieniądze poszły na konto oszusta.** Po podmienionej fakturze albo telefonie.

↓

2 **Natychmiast zadzwoń do banku** na numer z karty albo strony.

↓

Przelew jeszcze czeka na wysłanie?

NIE

⊘ Zgłoś wszędzie

Bank, zawiadomienie na policji z zaświadczeniem, CERT. Potem reklamacja w banku.

TAK

☑ Anuluj

Anuluj przelew w bankowości i potwierdź to z bankiem.

PRZYGOTUJ DO ZGŁOSZENIA

- numer i kwota przelewu
- godzina wysłania
- mail albo SMS od oszusta
- podmieniona faktura
- dane prawdziwego kontrahenta

Zrób

- ✓ Dzwoń do banku od razu
- ✓ Złóż zawiadomienie na policji, weź zaświadczenie
- ✓ Zachowaj maile i faktury

Nie rób

- ✕ Nie czekaj do jutra
- ✕ Nie płać „za odzyskanie pieniędzy”
- ✕ Nie kasuj korespondencji z oszustem

CO MÓWIĄ PRZEPISY I INSTYTUCJE

1 telefon

Jak najszybciej poinformuj bank, złóż zawiadomienie na policji i weź zaświadczenie, zgłoś sprawę do CERT. Banki często uznają przelew zlecony przez oszukaną osobę za autoryzowany i odmawiają zwrotu. W takim sporze pomaga Rzecznik Finansowy.

Rzecznik Finansowy, webinarium „Nieautoryzowane transakcje”, 7.12.2023

! Decyzja dla właściciela

Zapisz, kto ma prawo dzwonić do banku w sprawie blokady i gdzie jest numer. W stresie nikt go nie znajdzie.

SPRAWDŹ SIĘ

Po trzech godzinach wychodzi, że faktura miała podmienione konto. Czekasz na wyjaśnienia kontrahenta?

Nie. Dzwonisz do banku teraz, potem policja i CERT. Wyjaśnienia mogą poczekać.

BANK	POLICJA	ONLINE
Numer z karty	**Zaświadczenie**	**incydent.cert.pl**

Ktoś przejął firmowy fanpage

Odzyskuj przez facebook.com/hacked z własnej przeglądarki, zablokuj kartę podpiętą do reklam i uprzedź klientów innym kanałem.

KROK PO KROKU

1. **Nie możesz się zalogować na fanpage** albo widzisz obce posty i reklamy.
2. **Wejdź na facebook.com/hacked** z własnej przeglądarki, nie z linku.

Odzyskałeś dostęp?

NIE

⊘ Zgłaszaj

Dalej przez facebook.com/hacked. Zablokuj kartę do reklam, uprzedź klientów.

TAK

☑ Posprzątaj

Usuń obcych administratorów, zmień hasło, włącz drugi składnik.

SPRAWDŹ OD RAZU

- lista administratorów
- płatności za reklamy
- nowe posty i wiadomości
- adres e-mail do logowania
- podpięte aplikacje

Zrób

✓ Odzyskuj przez facebook.com/hacked

✓ Zablokuj kartę podpiętą do reklam

✓ Uprzedź klientów innym kanałem

Nie rób

✕ Nie klikaj w maile „od Meta” z linkiem

✕ Nie płać „za odblokowanie strony”

✕ Nie zakładaj od razu nowej strony

JAK TO WYGLĄDAŁO NAPRAWDĘ

30 000

kont na Facebooku przejęto w jednej kampanii opisanej w maju 2026. Głównie strony firm i konta reklamowe. Fałszywe maile wyglądały jak ostrzeżenia o naruszeniu zasad.

Malwarebytes, 4.05.2026

! Decyzja dla właściciela

Dwóch administratorów z drugim składnikiem. Stroną zarządza się z kont firmowych, nie z prywatnych pracownika.

SPRAWDŹ SIĘ

Rano na fanpage’u firmy reklama „promocji -90%”, której nie zlecałeś. Pierwszy ruch?

facebook.com/hacked z własnej przeglądarki, blokada karty w banku i ostrzeżenie dla klientów innym kanałem.

FACEBOOK	BANK	KLIENCI
facebook.com/hacked	**Zablokuj kartę**	**Inny kanał**

Dane klientów albo pracowników trafiły w złe ręce

Spisz fakty od razu i oceń ryzyko. Gdy naruszenie może zagrozić ludziom, zgłoszenie do UODO ma 72 godziny.

KROK PO KROKU

1 **Dane trafiły tam, gdzie nie powinny.** Mail do złej osoby, zgubiony laptop, atak.

↓

2 **Spisz fakty:** co, kiedy, czyje dane, ilu osób dotyczy.

↓

Ryzyko dla tych osób jest mało prawdopodobne?

NIE

⊘ Zgłoś w 72 h

Zgłoś do UODO, a przy wysokim ryzyku powiadom osoby, których dane dotyczą.

TAK

☑ Opisz

Wpisz zdarzenie do rejestru naruszeń firmy z uzasadnieniem.

SPISZ OD RAZU

- co się stało
- kiedy to stwierdzono
- jakie dane
- ilu osób dotyczy
- co już zrobiono

Zrób

✓ Spisz fakty od razu

✓ Oceń ryzyko z osobą od danych osobowych

✓ Zapisz zdarzenie w rejestrze naruszeń

Nie rób

✕ Nie ukrywaj zdarzenia

✕ Nie odkładaj oceny na koniec tygodnia

✕ Nie usuwaj śladów

CO MÓWIĄ PRZEPISY I INSTYTUCJE

72 godziny

Tyle ma administrator danych na zgłoszenie naruszenia do UODO od jego stwierdzenia, chyba że ryzyko dla osób jest mało prawdopodobne. Każde naruszenie trzeba udokumentować.

RODO, rozporządzenie UE 2016/679, art. 33 ust. 1 i 5

! Decyzja dla właściciela

Wyznacz osobę, która ocenia naruszenia, i trzymaj pod ręką wzór zgłoszenia. Liczy się czas od stwierdzenia.

SPRAWDŹ SIĘ

Pracownica wysłała listę płac do całego zespołu zamiast do księgowej. Co teraz?

Prosisz odbiorców o usunięcie, spisujesz fakty i oceniasz, czy zgłosić naruszenie do UODO w 72 godziny.

OCENIA	UODO	REJESTR
Osoba od danych	**72 godziny**	**Zawsze**

10 decyzji właściciela

Żadna z nich nie wymaga dużego budżetu. Wymaga decyzji szefa i jednej osoby, która ją wdroży. Zaznacz to, co już działa w Twojej firmie.

01	**Zmiana numeru konta tylko po telefonie** na numer z umowy, z podpisem osoby, która zatwierdza przelewy. → s. 7, 59	☐
02	**Drugi składnik logowania wszędzie** poczta, bank, fanpage, konta reklamowe. Samo hasło przestaje wystarczać. → s. 13, 61	☐
03	**Kopia zapasowa poza siecią** i test odtworzenia co kwartał. Kopia, której nikt nie odtworzył, jest nadzieją. → s. 11, 57	☐
04	**Automatyczne aktualizacje, pracownicy bez uprawnień administratora** Programy instaluje osoba od IT, według listy. → s. 37	☐
05	**Szyfrowanie laptopów i telefonów** z kluczami odzyskiwania w jednym bezpiecznym miejscu. → s. 43, 45	☐
06	**Menedżer haseł dla firmy** Hasła wspólne tylko tam, gdzie nie da się inaczej. → s. 51	☐
07	**Lista kontrolna odejścia pracownika** podpisywana razem z protokołem zdania sprzętu. → s. 49	☐
08	**Zasady AI na jednej stronie** jedno narzędzie, czego nie wklejamy, kto odpowiada za tekst. → s. 35, 39	☐
09	**Hasło kontrolne i zgłaszanie bez kary** Kto sprawdza polecenie szefa albo zgłasza swój błąd, nie ponosi konsekwencji. → s. 25, 55	☐
10	**Plan pierwszej godziny** kto dzwoni do banku, kto ocenia wyciek danych, gdzie leżą numery. → s. 59, 63	☐

Szkolenie w 30 minut

5 min	20 min	5 min
Zasada	Pięć sytuacji, po 4 minuty	Ustalenia

Przy każdej sytuacji: przeczytaj pytanie na głos. Każdy mówi, co by zrobił, zanim ktokolwiek zna odpowiedź. Potem przeczytaj odpowiedź i przypadek z karty. Zapytaj: **czy u nas ktoś by to sprawdził i jak?**

1 Mail od stałego dostawcy, stopka i podpis jak zawsze, w treści nowy numer konta. Płacisz? → odpowiedź s. 7

2 „Dział bezpieczeństwa banku. Ktoś wyprowadza środki z konta firmy, przeniesiemy je na konto techniczne”. Co robisz? → odpowiedź s. 19

3 Głos szefa w telefonie: „Przelej 38 tys. zł kontrahentowi, faktura dojdzie później”. Co robisz? → odpowiedź s. 25

4 Pytasz czat o numer infolinii firmy kurierskiej. Dostajesz numer i link. Dzwonisz? → odpowiedź s. 33

5 Pracownik po godzinie przyznaje, że wpisał hasło na dziwnej stronie. Jak reagujesz? → odpowiedź s. 55

☑ Na koniec ustalcie

Kto jest osobą od IT. Kto zatwierdza przelewy. Jakie jest hasło kontrolne. Wpiszcie to na karcie na biurko i powieście ją przy komputerach.

Nikt nie jest oceniany. Liczą się pytania, nie wynik. Za kwartał powtórzcie z pięcioma innymi kartami.

Skąd to wiemy

Każdy przypadek ma publiczne źródło: wyrok, decyzję urzędu, komunikat policji lub CERT, badanie albo artykuł. Omówienia podajemy w nawiasie. „Odczyt” to dzień, w którym sprawdziliśmy stronę bez daty. Nazw poszkodowanych firm nie podajemy. Stan źródeł: 28.11.2026.

01 Poczta

5 4 mln zł strat firm na podmienionych kontach: Komunikat CBZC, 12.08.2026

1.1 Sąd Najwyższy, wyrok z 9.04.2025, II CSKP 966/23

1.2 Ministerstwo Finansów, podatki.gov.pl, 16.10.2026

1.3 CERT Polska, ostrzeżenie z lipca 2026 (omówienia: Bankier.pl, 21.07.2026; money.pl)

1.4 Ministerstwo Cyfryzacji, gov.pl, komunikat o phishingu, 10.2024

1.5 Komunikat CBZC, 12.08.2026 (omówienia: RMF24, TVP Info)

02 Telefon

17 Numer 8080 do zgłaszania SMS: CERT Polska, odczyt 28.11.2026

2.1 Komunikat CBZC i KGP z 10.01.2023

2.2 mBank, komunikaty o aplikacjach do zdalnego pulpitu, odczyt 28.11.2026

2.3 KGP i FinCERT.pl, 21.07.2026 (omówienie: Bankier.pl, 28.07.2026)

2.4 „Cyberportret polskiego biznesu 2026”, ESET i DAGMA, badanie z marca 2026

2.5 CERT Orange Polska (omówienie: Telepolis, 20.06.2024)

2.6 Ministerstwo Cyfryzacji, gov.pl, 10.2024; KGP i operator BLIK, odczyt 28.11.2026

03 AI

31 62% pracowników korzysta z AI, 27% firm ma zasady: „Cyberportret polskiego biznesu 2026”, ESET i DAGMA

3.1 Washington Post, 08.2025 (omówienia: Interia, Spider’s Web)

3.2 „Cyberportret polskiego biznesu 2026”, ESET i DAGMA

3.3 USENIX Security 2025, 576 tys. próbek kodu z 16 modeli

3.4 NSA, postanowienie z 23.06.2026, I FZ 104/26

04 Sprzęt i dostęp

41 85% firm z incydentem w ostatnim roku: „Cyberportret polskiego biznesu 2026”, ESET i DAGMA

4.1 NSA, wyrok z 3.11.2026 (omówienie: prawo.pl, 11.2026)

4.2 Decyzja UODO DKN.5131.22.2021; WSA II SA/Wa 3309/21; NSA (omówienie: prawo.pl, 30.09.2024)

4.3 Decyzja Prezesa UODO z 12.11.2024

4.4 Decyzja UODO utrzymana przez NSA 6.03.2026

4.5 CERT Polska, rekomendacje dotyczące haseł, 01.2022; poradnik o poczcie, odczyt 28.11.2026

05 Pierwsza godzina

53 260,8 tys. incydentów w 2025 r. (103,4 tys. rok wcześniej): CERT Polska, raport roczny

5.1 Ministerstwo Cyfryzacji, gov.pl, 10.2024; CERT Polska, poradnik o poczcie, odczyt 28.11.2026

5.2 Eksperci ESET (Rzeczpospolita, 15.06.2026)

5.3 Rzecznik Finansowy, webinarium „Nieautoryzowane transakcje”, 7.12.2023

5.4 Malwarebytes, 4.05.2026

5.5 RODO, rozporządzenie UE 2016/679, art. 33 ust. 1 i 5

Pozostałe

Karta na biurko: 112; incydent.cert.pl i 8080 (CERT Polska); 22 330 03 30 (Krajowa Informacja Skarbowa); facebook.com/hacked (Meta).

Aktualizacje (s. 52 i 64): NCSC, Small Business Guide, odczyt 28.11.2026.

Kolory i znaki: norma ISO 3864 (barwy bezpieczeństwa).

Znalazłeś błąd albo nowszy przypadek?

Napisz: kontakt@systembox.pl. Poprawiamy poradnik przy każdym wydaniu. Poradnik jest bezpłatny. Możesz go drukować i przekazywać dalej bez zmian w treści.

Gdy coś się dzieje

Zagrożenie życia lub mienia	**112**
Pieniądze wyszły z konta	**numer z karty banku**
Zgłoszenie incydentu	**incydent.cert.pl**
Podejrzany SMS: prześlij na	**8080**
Mail „z urzędu skarbowego”	**22 330 03 30**
Przejęty fanpage	**facebook.com/hacked**

WPISZ SWOJE NUMERY

Osoba od IT .....

Kto zatwierdza przelewy .....

Hasło kontrolne znają .....

Stop | **Sprawdź** | **Zgłoś**

ZANIM KLIKNIESZ
WYDANIE 2026

SYSTEMBOX · opieka informatyczna
Białystok i 50 km, zdalnie cała Polska
systembox.pl/opieka-it · +48 570 923 234