

# Pierwsza godzina po incydencie

Do wydruku i powieszenia przy biurku księgowości.

Tę stronę wypełniasz dzisiaj i wieszasz na ścianie. Reszta dokumentu zostaje w segregatorze.

| Kto                                                         | Numer (wpisz długopisem) |
|-------------------------------------------------------------|--------------------------|
| Bank — zespół fraudowy (numer z odwrotu karty, nie z maila) | .....                    |
| Osoba decyzyjna w firmie                                    | .....                    |
| Informatyk / firma IT                                       | .....                    |
| Kontrahent — numer z umowy, nie ze stopki maila             | .....                    |

## Minuta 0–15: zatrzymaj pieniądze

- ☐ **Dzwoń do banku:** „zgłaszam nieautoryzowany przelew, proszę o wstrzymanie i kontakt z bankiem odbiorcy”. Podaj datę, kwotę i rachunek odbiorcy. Numer zgłoszenia: .....
- ☐ **Wstrzymaj kolejne płatności** do tego odbiorcy i całą paczkę przelewów.
- ☐ **Nie odpisuj na wiadomość, która wywołała przelew** — odpowiedź czyta atakujący.

## Minuta 15–30: zamknij drzwi

- ☐ **Zmień hasło do skrzynki** z urządzenia, o którym wiesz, że jest czyste.
- ☐ **Sprawdź reguły w poczcie** (Ustawienia → Filtry) i skasuj te, których nie zakładałeś. Tu zwykle siedzi atak.
- ☐ **Wyloguj wszystkie sesje**, sprawdź ostatnie logowania pod kątem obcych krajów.
- ☐ Jeżeli otwarto załącznik: **odłącz komputer od sieci, ale go nie wyłączaj** — ślady giną przy zamknięciu systemu.

## Minuta 30–60: powiadom i udokumentuj

- ☐ **Zadzwoń do kontrahenta** na numer sprawdzony — jego skrzynka może być źródłem.
- ☐ **Ostrzeż zespół telefonicznie**, nie mailem z zaatakowanej skrzynki.
- ☐ **Zrzuty ekranu z pełnym nagłówkiem nadawcy**, zanim ktoś zacznie sprzątać skrzynkę.
- ☐ **Zgłoś incydent:** incydent.cert.pl lub mObywatel, oraz policja. Numer: .....
- ☐ **Zapisz oś czasu:** co przyszło, o której, kto kliknął, kiedy poszedł przelew.

## Czego NIE robić w pierwszej godzinie

| Odruch                                          | Dlaczego szkodzi                                                         |
|-------------------------------------------------|--------------------------------------------------------------------------|
| Odpisać na maila i zapytać, czy to na pewno oni | Odpowiedź czyta atakujący, nie kontrahent                                |
| Zadzwonić na numer podany w tej wiadomości      | Numer jest częścią ataku                                                 |
| Skasować podejrzaną wiadomość                   | Znika jedyny dowód i nagłówki                                            |
| Wyłączyć komputer „na wszelki wypadek”          | Giną ślady w pamięci; przy szyfrowaniu bywa gorzej po restarcie          |
| Czekać do rana, bo „i tak bank nie działa”      | Fraudowe linie banków działają całą dobę; po nocy przelew jest już dalej |
| Zapłacić okup, żeby mieć spokój                 | Płatność nie gwarantuje odzyskania danych i finansuje kolejny atak       |

## Kiedy sprawa dotyczy danych osobowych

Jeżeli wyciekły dane osobowe (klientów, pracowników, kontrahentów), zgłoszenie do Prezesa UODO robi się **w ciągu 72 godzin** od stwierdzenia naruszenia. Licznik rusza w momencie, w którym się dowiedziałeś — nie w momencie, w którym skończyliście wyjaśniać sprawę. Wpisz tutaj, kto to robi: .....

## Następnego dnia, na spokojnie

1. Sprawdź, czy ktoś w firmie używał tego samego hasła gdzie indziej. Zwykle używał.
2. Włącz dwuskładnikowe logowanie na **wszystkich** skrzynkach, nie tylko na zaatakowanej. Atakujący nie wchodzi przez prezesa, tylko przez handlowca albo księgowość.
3. Wpisz do procedury obiegu faktur jedno zdanie: **każda zmiana numeru rachunku wymaga telefonu na numer, który mieliśmy wcześniej.**
4. Ustal, kto z zespołu w ogóle nie wiedział, co robić. To jest lista osób na najbliższe szkolenie.

*Procedurę opracował Daniel Kacprowicz na podstawie warsztatów prowadzonych w firmach i instytucjach publicznych. Dokument jest bezpłatny — możesz go drukować i rozdawać w swojej firmie bez pytania o zgodę. [szkolimy24.com](http://szkolimy24.com) · [biuro@szkolimy24.com](mailto:biuro@szkolimy24.com)*

### Potrzebujesz z tym pomocy?

Prowadzę szkolenia dla instytucji publicznych z bezpieczeństwa pracy, cyberbezpieczeństwa i praktycznego wykorzystania sztucznej inteligencji. Jeżeli chcesz omówić wyniki albo szkolenie dla swojego zespołu — napisz przez formularz na stronie.

[szkolimy24.com/procedura](https://szkolimy24.com/procedura)