


**AKADEMIA ODPORNOŚCI • KARTA PRACY DO WEBINARIUM**

# Bezpieczeństwo cyfrowe i dezinformacja

Zabezpiecz konta organizacji i przeciwcz spokojne sprostowanie.

ORGANIZACJA LUB GRUPA

MIEJSCOWOŚĆ

DATA

## 1 Kto ma dostęp do kont organizacji

Wpisz osoby i sprawdź zabezpieczenia.

| KONTO                           | KTO MA DOSTĘP | WERYFIKACJA<br>DWUETAPOWA | KOMU ODEBRAĆ DOSTĘP |
|---------------------------------|---------------|---------------------------|---------------------|
| Skrzynka mailowa                |               |                           |                     |
| Fanpage i media społecznościowe |               |                           |                     |
| Bankowość                       |               |                           |                     |
| Strona internetowa              |               |                           |                     |

## 2 Pięć rzeczy w tym tygodniu

Wpisz datę, gdy zrobisz.

|                                                           | ZROBIONE, DATA |
|-----------------------------------------------------------|----------------|
| 1 Menedżer haseł i osobne hasło do każdego konta          |                |
| 2 Weryfikacja dwuetapowa na mailu, w banku i na fanpage'u |                |
| 3 Kopia zapasowa dokumentów poza jednym komputerem        |                |
| 4 Aktualizacje systemu i aplikacji na telefonach zarządu  |                |
| 5 Przegląd, kto ma dostęp do fanpage'a i skrzynki         |                |

## 3 Gdy ktoś przejmie konto

Ustal z góry, kto co robi. Najpierw odzyskanie kontroli, potem zgłoszenie.

| ZADANIE                                                                                             | KTO U NAS | TELEFON |
|-----------------------------------------------------------------------------------------------------|-----------|---------|
| Zmienia hasło z innego urządzenia i włącza weryfikację dwuetapową                                   |           |         |
| Przy danych karty dzwoni do banku                                                                   |           |         |
| Zgłasza incydent na <a href="http://incydent.cert.pl">incydent.cert.pl</a> i uprzedza obserwujących |           |         |

#### 4 Po czym poznać fałszywą wiadomość

Opisz jedną podejrzaną wiadomość i zaznacz sygnały, które w niej były.

- ☐ Link albo załącznik, którego się nie spodziewasz
- ☐ Dziwny adres nadawcy
- ☐ Błędy i brak polskich znaków
- ☐ Pośpiech: zapłać, bo stracisz konto albo przesyłkę
- ☐ Prośba o dane logowania albo numer karty

Podejrzany SMS prześlij na 8080. Próbę oszustwa zgłoś na [incydent.cert.pl](https://incydent.cert.pl) albo w aplikacji mObywatel.  
Poradnik Bezpieczeństwa MSWiA, strona 40

#### 5 Sprostowanie w trzech zdaniach

Napisz spokojny wpis na lokalną grupę o nieprawdziwej informacji.

Co wiemy na pewno

Skąd to wiemy

Co robić teraz

Przykład: Woda w wodociągu jest zdatna do picia. Tak podał dziś urząd gminy na swojej stronie. Jeśli coś się zmieni, gmina wyda komunikat.

#### 6 Mini diagnoza

Zapytaj trzy starsze osoby, czy dostały ostatnio podejrzaną wiadomość.

Odpowiedziało tak: \_\_\_\_\_ z 3. Czego dotyczyły telefony: