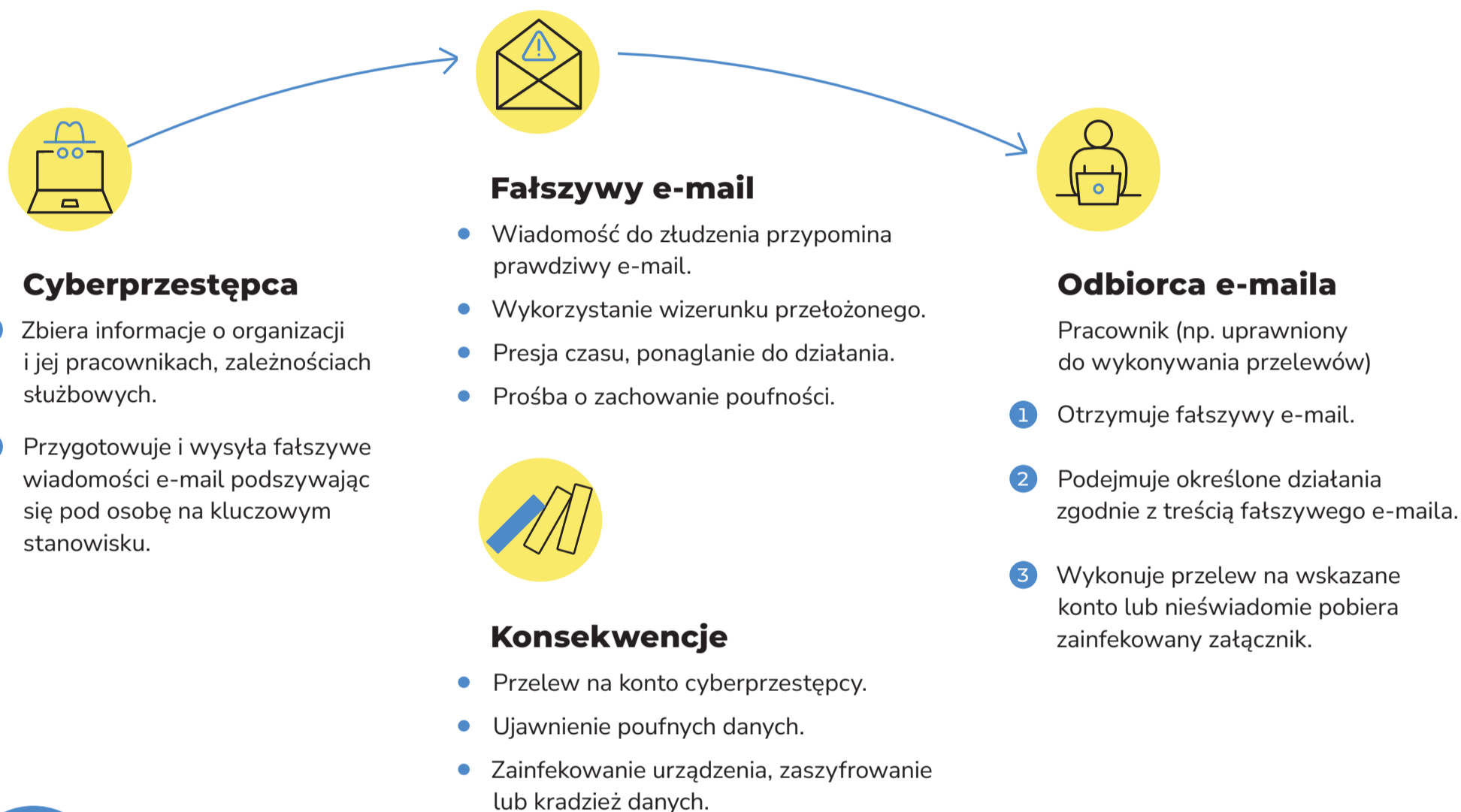




Atak typu Business E-mail Compromise

ATAK TYPU BUSINESS E-MAIL COMPROMISE (BEC) – znany również jako „oszustwo na dyrektora”, to oszustwo z użyciem socjotechniki, w którym cyberprzestępcy wykorzystują korespondencję e-mailową do wyłudzeń finansowych lub ujawniania poufnych danych firmowych.



Jak chronić organizację?

- 1 **ORGANIZUJ REGULARNE SZKOLENIA** i ćwiczenia-symulacje phishingowych, aby zwiększyć świadomość pracowników na temat cyberzagrożeń.
- 2 **UŻYWAJ NARZĘDZI** zabezpieczających takich jak:
 - filtrowanie e-maili,
 - oprogramowanie antywirusowe,
 - zapory sieciowe,
 - systemy wykrywania nietypowych aktywności.
- 3 **ZWERYFIKUJ I DOSTOSUJ UPRAWNIENIA DOSTĘPU** do systemów, aplikacji i danych, zgodnie z rolami pracowników, ograniczając im dostęp tylko do niezbędnych zasobów.
- 4 **ZABEZPIECZAJ DANE** organizacji i klientów poprzez szyfrowanie oraz regularne tworzenie kopii zapasowych, dzięki którym odzyskasz dane i zapewnisz ciągłość działania.
- 5 **USTAL PROCEDURY** dotyczące przelewów i płatności, aby uniknąć przekazania pieniędzy na konto oszustów.
- 6 **MONITORUJ AKTYWNOŚĆ** sieciową i działania pracowników, by uniknąć podejrzanych zachowań.