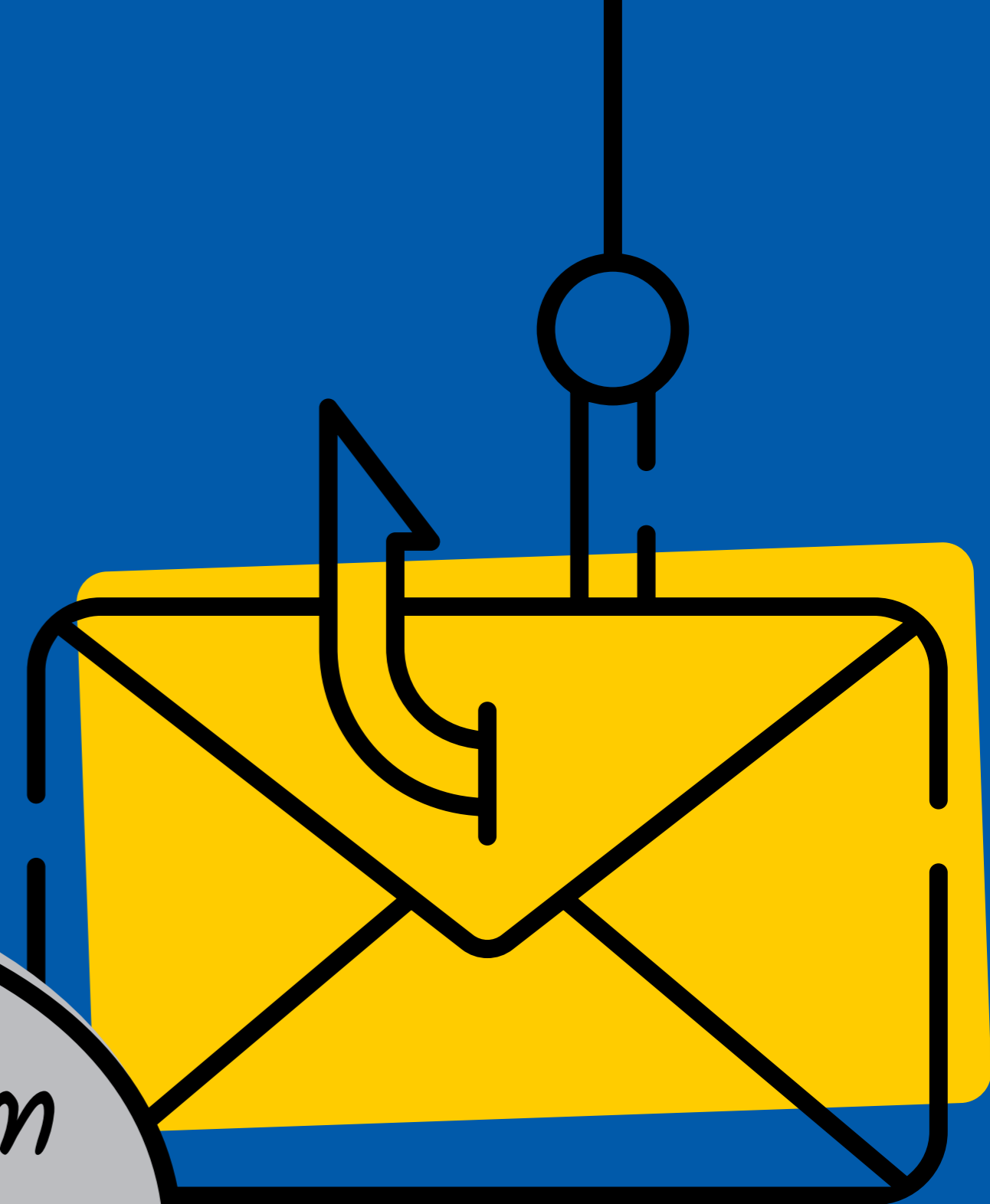




ATAKI RANSOMWARE CZĘSTO ZACZYNAJĄ SIĘ OD PHISHINGU



#NoMoreRansom
#CyberDialogues

Podstępny Bob przygotowuje złośliwego emaila do Alicji i używa socjotechniki, żeby wzbudzić jej zaufanie.



Malware gotowy do zainstalowania
Więcej informacji
OTWÓRZ



Twoje konto bankowe zostało zablokowane
Więcej informacji
OTWÓRZ

Alicja otwiera wiadomość e-mail i pobiera załącznik. To wszystko, czego potrzeba do infekcji ransomware!

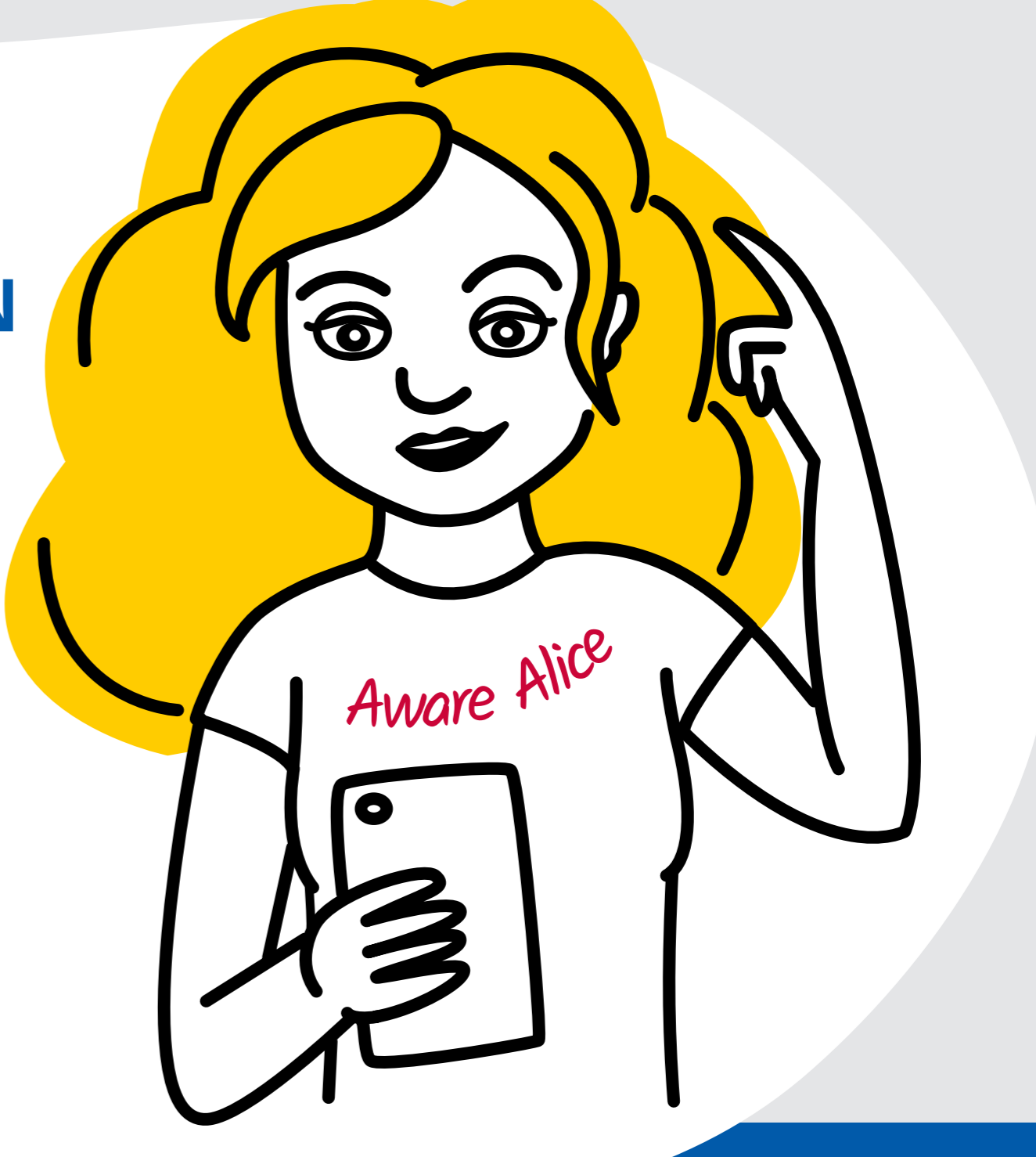
Podstępny Bob blokuje dokumenty i zdjęcia Alicji, żądając od niej zapłaty za odzyskanie danych.



Uważna Alicja postanawia się zatrzymać i pomyśleć. Uleganie szantażowi przestępców nie wchodzi w grę!
#NIE PŁAĆ

Ona wie, co należy zrobić: wykonać dwa proste kroki!

1. ZRESETOWAĆ TELEFON DO USTAWIENIŃ FABRYCZNYCH
2. PRZYWRÓCIĆ DANE Z KOPII ZAPASOWEJ W CHMURZE



CHROŃ SIĘ PRZED #RANSOMWARE

PAMIĘTAJ:
CHROŃ SWOJE URZĄDZENIA I PLIKI, PRZESTRZEGAJĄC PROSTYCH ZASAD BEZPIECZEŃSTWA.



1. REGULARNIE TWÓRZ KOPIĘ ZAPASOWĄ DANYCH
2. NIE KLIKAJ W NIEOCZEKIWANE LUB PODEJRZANE WIADOMOŚCI E-MAIL I SMS
3. CHROŃ SWOJE DANE OSOBOWE

WIĘCEJ WSKAZÓWEK ZNAJDZIESZ NA STRONIE: <https://www.nomoreransom.org>