

LEKCJA 4

SCAM

– OSZUSTWA W SIECI



-500





Czym jest scam?

Scam to oszustwo polegające na wyłudzeniu danych i informacji, najczęściej w celu kradzieży środków pieniężnych. Oszuści wykorzystując socjotechnikę (najczęściej prześwietlenie aktywności ofiary w Internecie i wykorzystanie pozyskanych o niej informacji), próbują podszyć się pod znane witryny, firmy, osoby itp., aby zmylić potencjalną ofiarę.



Formy scamów

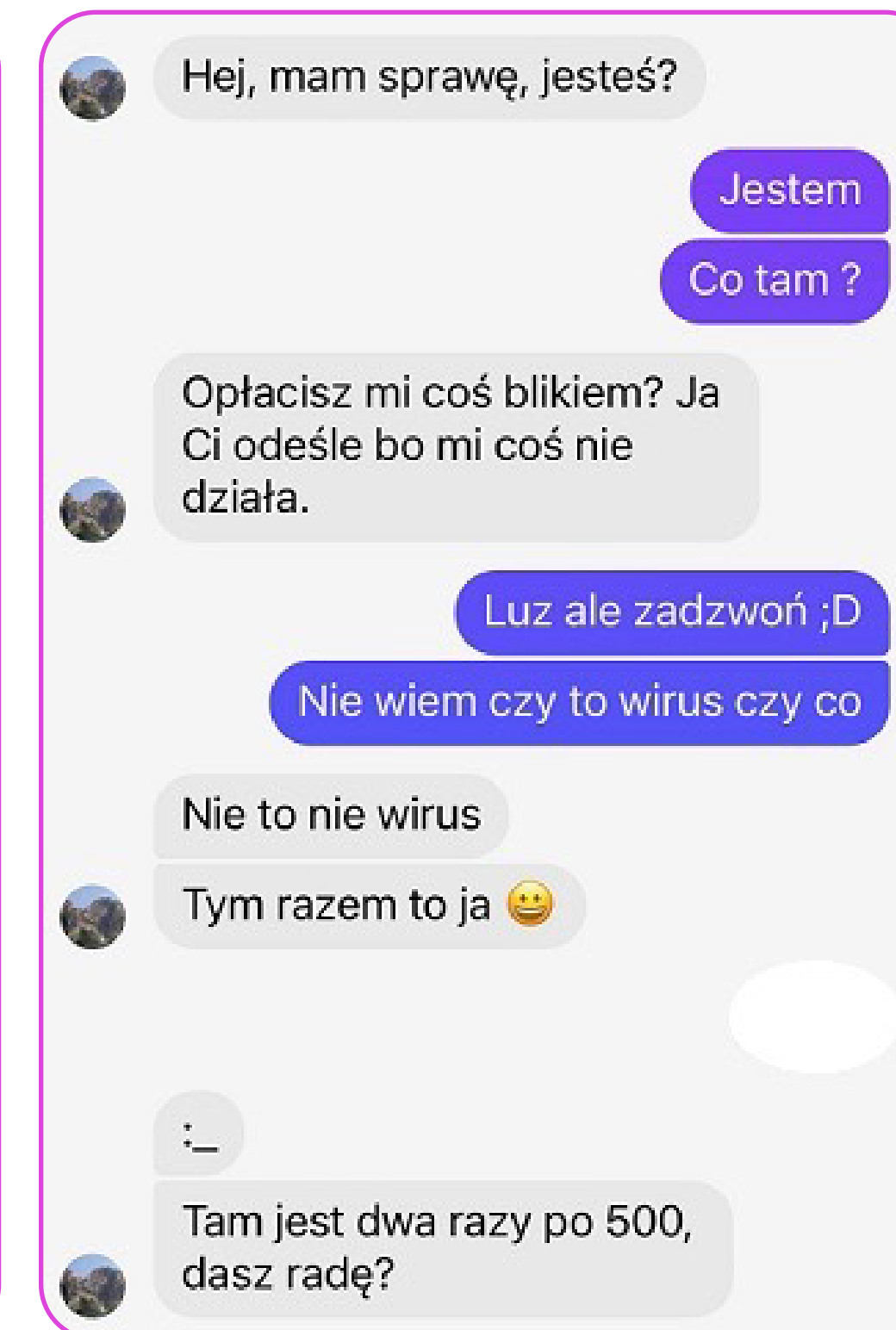
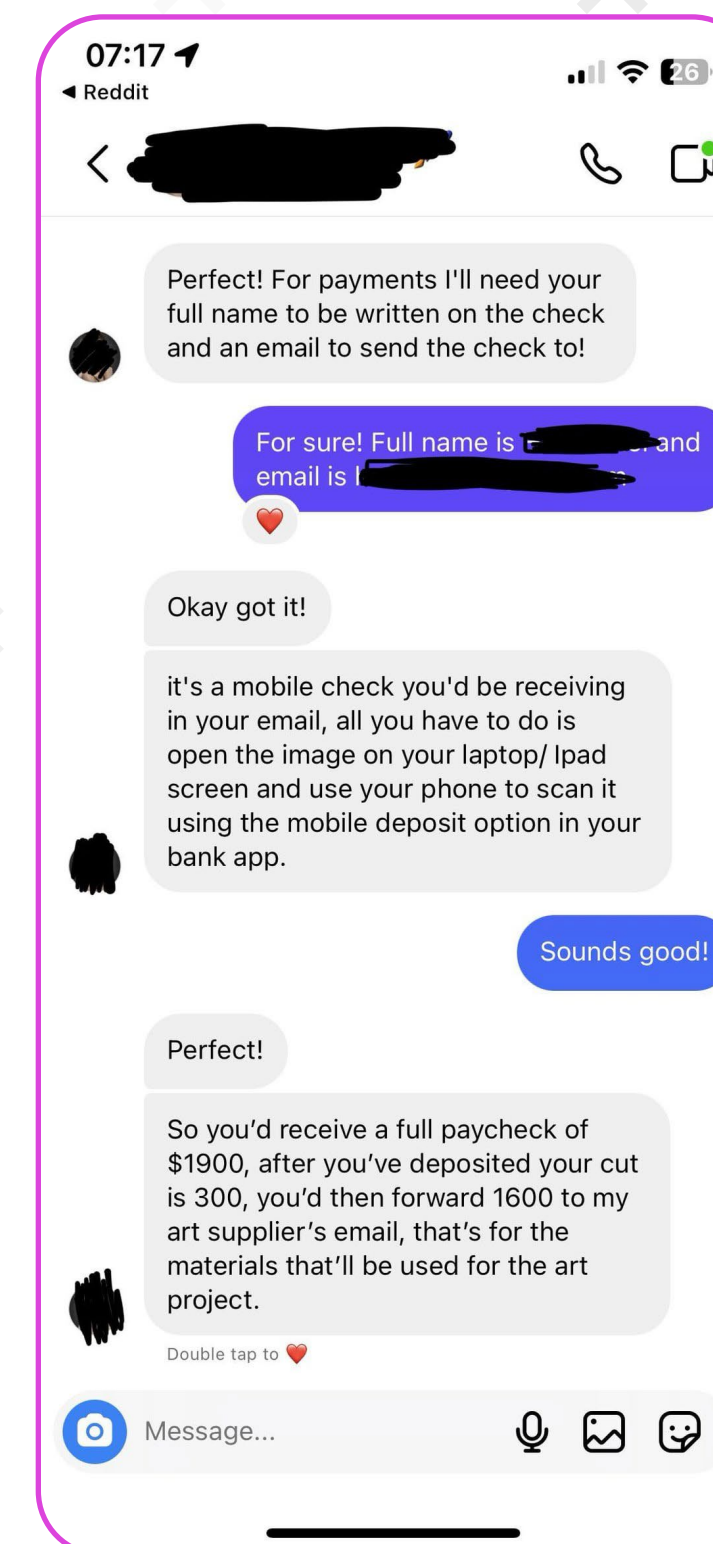
- ✕ Phishing
- ✕ Smishing
- ✕ Fałszywe oferty pracy
- ✕ Clickbaity
- ✕ Fałszywe sklepy internetowe



Przykłady

Phishing

Popularny scam na Instagramie - konta udające artystów proponują zapłatę kilkuset dolarów za zgodę na wykorzystanie zdjęcia do stworzenia obrazu, jednak aby przelać pieniądze - proszą o podanie Twoich danych osobistych. To służy im do wykradania hasła, a nawet danych bankowych. Czasami również informują Cię, że dostaniesz przelew, z którego część musisz oddać artyście - potem okazuje się, że przelew ten został wycofany.



źródło: cieszyn.policja.gov



Przykłady

Smishing

piątek, 30 października 2020



Nastąpiło wstrzymanie dostawy przesyłki z powodu nie prawidłowej wagi. Zapłac 1,29 aby wznowić Inpost24.net/394891?QFDYQW

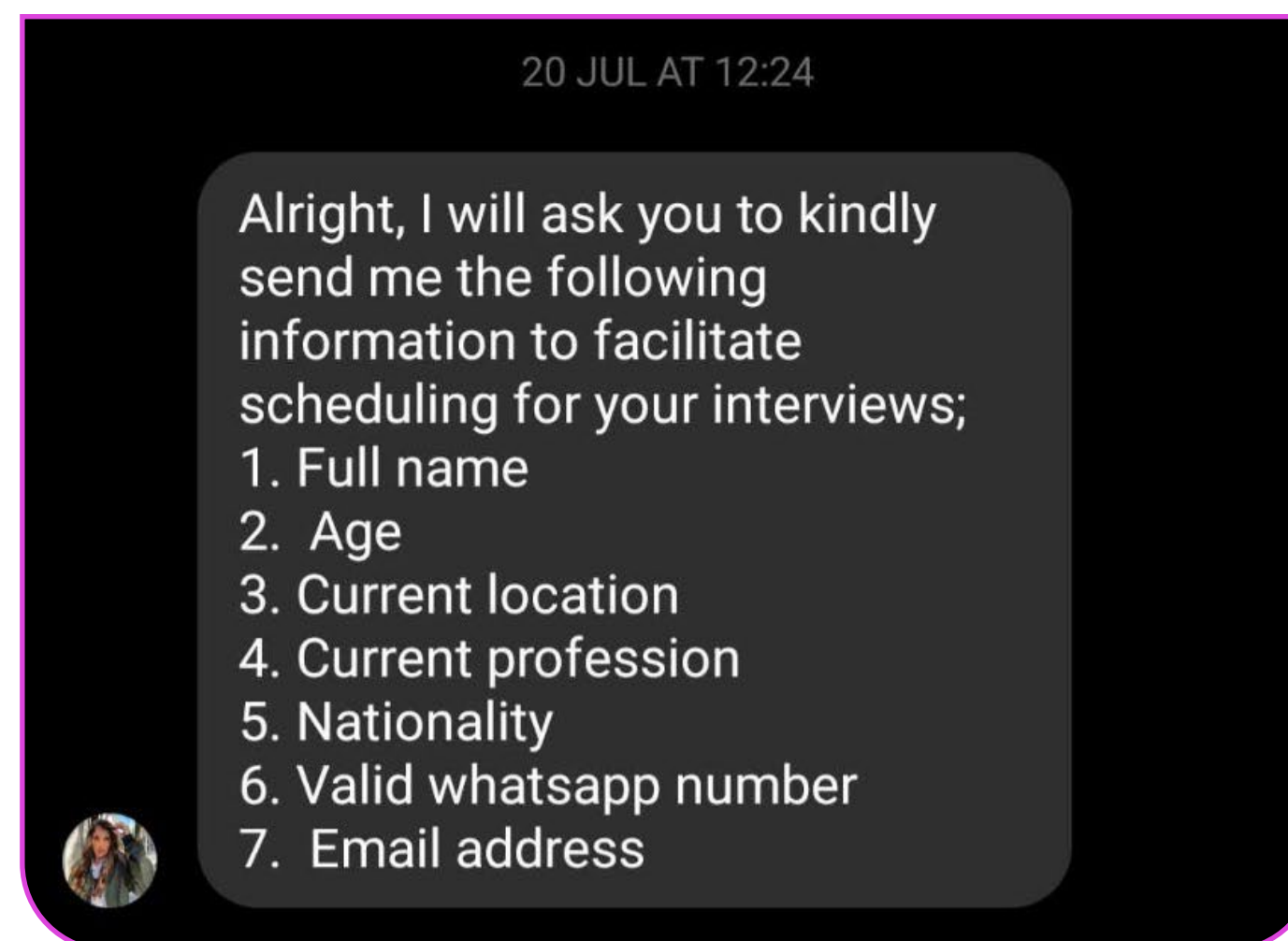
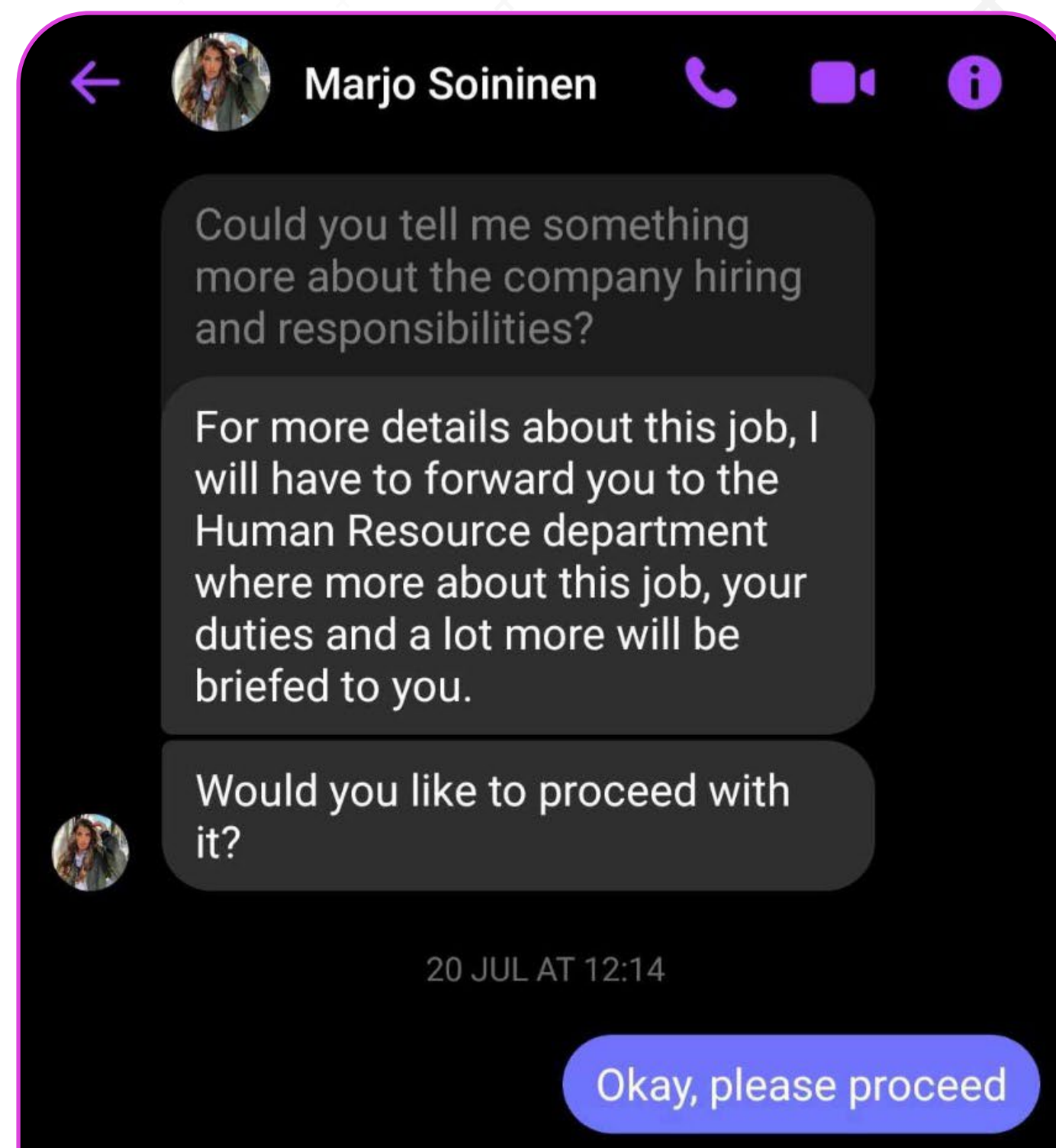
📌 20:49

źródło: inpost.pl



Przykłady

Falszywe oferty na grupach



źródło: screenshoty własne autora



Przykłady

Fałszywe sklepy internetowe

o naszym sklepie

Piganion Limited
OFFICE UNIT B ON 9/F
THOMSON COMMERCIAL
BUILDING 8 THOMSON ROAD
Hong Kong

- niepewny dostawca

WODOODPORNĄ BIŻUTERIA

BEZPŁATNA WYSYŁKA POWYŻEJ 129.99 zł
DOŻYWOTNIA GWARANCJA KOLORU
POWRÓT BEZ PROBLEMU

- automatyczne tłumaczenie

DO 70% ZNIŻKI (Przelewy24)

NAJWIĘKSZA
WYPRZEDAŻ W
HISTORII!

DO 70% ZNIŻKI

- granie na emocjach, zachęcenie

klejnotyodliesbeth.pl

- brak symbolu kłódki

źródło: klejnotyodliesbeth.pl

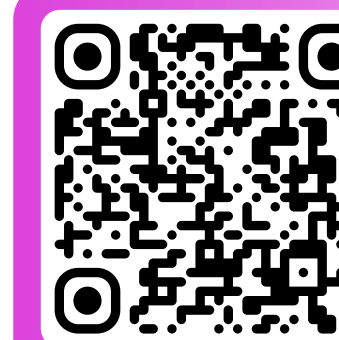


- zdjęcia pobrane z innych stron
(tutaj: z Aliexpress)



Jak chronić się przed scamem?

- × Pomyśl, zanim klikniesz
- × Gdy ktoś prosi Cię o przelew lub podanie prywatnej informacji, zadzwoń do niego i upewnij się, czy to na pewno on
- × Uważaj na reklamy oraz rozdania, super promocje. Sprawdzaj czy w adresie strony czy nazwie sklepu nie ma literówki - np. Żabkaa zamiast Żabka
- × **Zgłaszaj podejrzane wiadomości!**
- × Przesyłaj podejrzane wiadomości SMS na numer: **8080**
- × Skorzystaj z darmowego narzędzia Trend Micro do weryfikacji bezpieczeństwa strony:
global.sitesafety.trendmicro.com/





Co robić, gdy dasz się oszukać?

1. Poproś o pomoc dorosłego.
2. Wyloguj swoje konta ze wszystkich urządzeń i zmień swoje hasła.
3. Jeśli podejrzewasz, że ktoś mógł wykraść dane Twoich kart - zadzwoń do swojego banku i od razu je zastrzeż!
4. Spróbuj skontaktować się ze swoimi znajomymi i ostrzeż ich, że Twoje konto mogło zostać przejęte.
5. Zgłoś podejrzenie przejęcia konta administratorom serwisu.
6. Zgłoś zdarzenie pod adresem **incydent.cert.pl** lub pod numer **8080**





Dyskusja

1. Czy kiedykolwiek ktoś próbował Cię oszukać w Internecie lub za pomocą SMSów? Jak zareagowałeś?
2. Czy znasz przypadki, w których ktoś został oszukany przez swoją nieuwagę? Jakie były tego konsekwencje?
3. Co robić w przypadku podejrzenia przejęcia konta?
4. Czy spotkałeś się kiedyś z nieprawdziwą reklamą lub ofertą?
5. Co zrobisz, gdy napisze do Ciebie Twój ulubiony YouTuber?



Utrwalenie wiedzy

Opisz sytuację, w której Ty lub ktoś, kogo znasz, natknął się na próbę scamu internetowego. Jakiego sposobu użył cyberprzestępca? Jak zareagowała potencjalna ofiara? Czy jej reakcja była odpowiednia, a może wręcz przeciwnie? Co mogłoby się stać, gdyby ofiara scamu wykonała polecenia oszusta?