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.

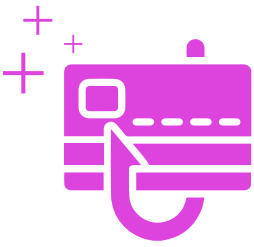
1. Najbardziej rozpowszechnione formy scamu to:

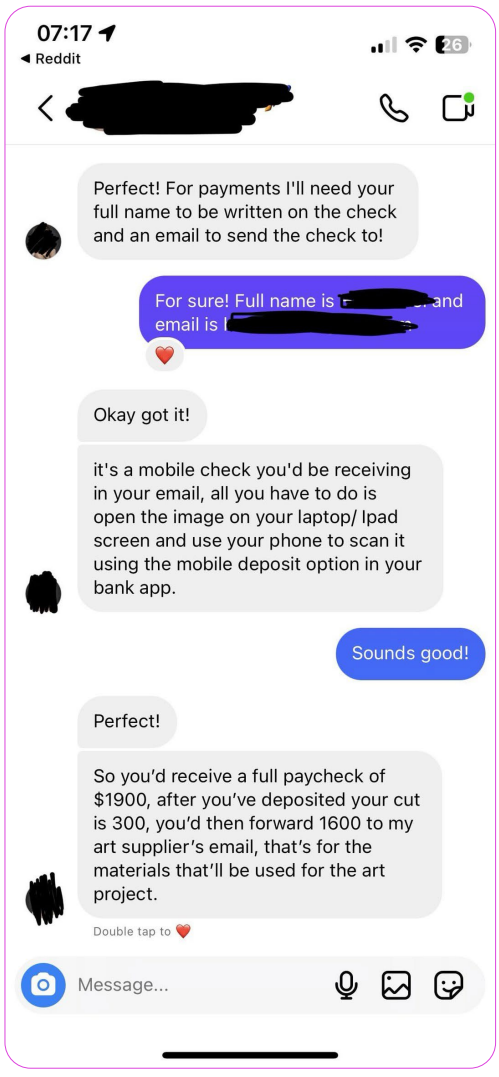
Phishing

Fałszywe wiadomości e-mail, łudząco przypominają korespondencję np. z banku, sklepu internetowego, platformy sprzedażowej itp. i zachęcają odbiorcę do kliknięcia w linki prowadzące do fałszywych stron oraz do podania swoich danych logowania bądź karty. Ostatnio, dość popularne stało się również tworzenie kont podszywających się pod znane osoby lub członków rodziny/przyjaciół i wysyłanie wiadomości z prośbami o przelewy natychmiastowe.

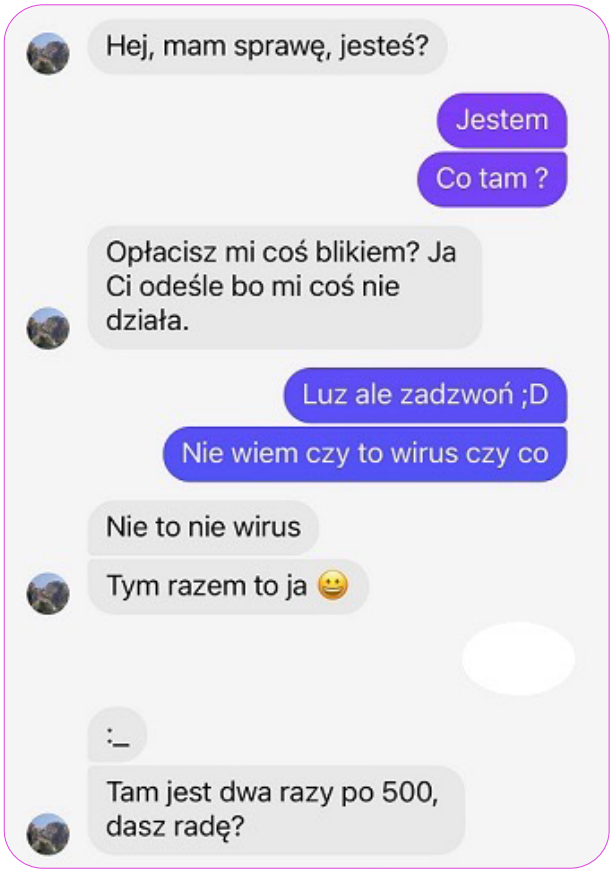
Przykład:

Popularny scam na Instagramie - konta udające artystów proponują zapłatę kilkuset dolarów za zgodę na wykorzystanie zdjęcia do stworzenia obrazu, jednak aby przelać pieniądze - proszę 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

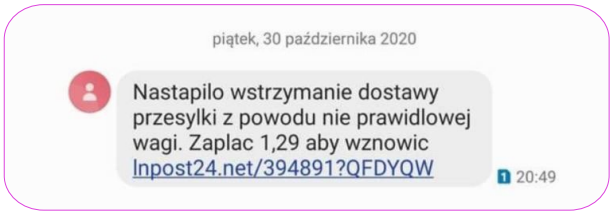


źródło: cieszyn.policja.gov

Smishing

Fałszywe SMS'y udające wiadomości od np. firmy kurierskiej lub z banku, zawierają przeważnie linki lub kody QR kierujące do fałszywych stron lub zainfekowane linki instalujące na urządzeniu programy szpiegujące

Przykład:



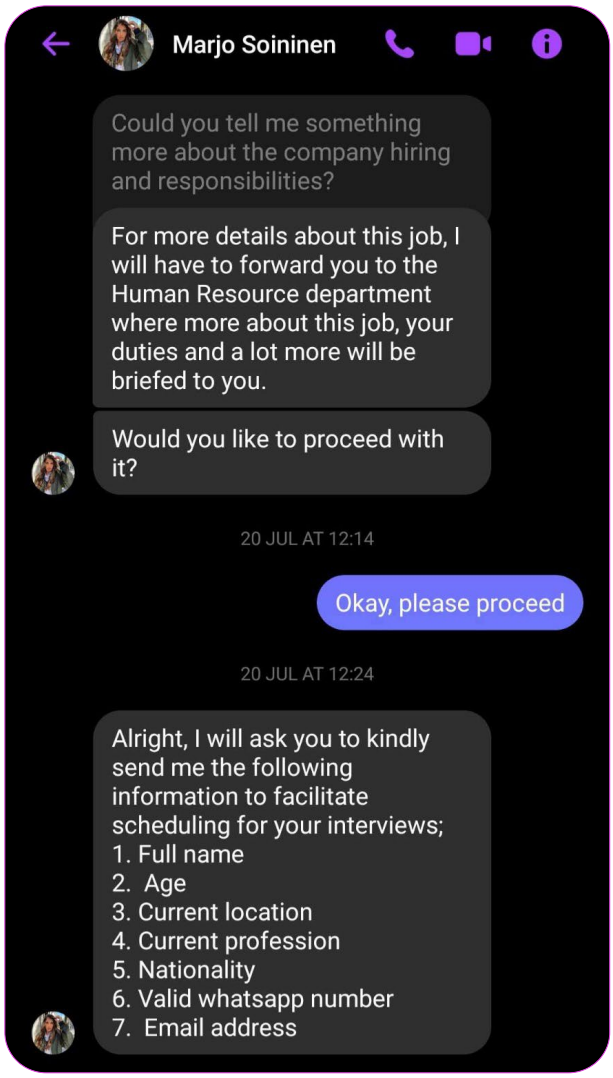
źródło: inpost.pl

Fałszywe oferty na grupach

Na wielu grupach i forach internetowych można spotkać fałszywe oferty, np. pracy, służące wykradaniu danych. Wyjątkowo często pojawiają się one w kontekście pracy zdalnej i dodatkowego dochodu. Oszuści często używają nowych kont, generycznego imienia i nazwiska, np. James Williams oraz zdjęcia pobranego z sieci. Przedstawiają ofertę pracy, która jest zbyt dobra, by mogła być prawdziwa, ale szczegóły chcą przekazać tylko w prywatnej wiadomości - po czym proszą o numer WhatsApp, Signala bądź Telegrama.

W ten sposób mogą kontynuować dowolne oszustwo (nierzadko wciągając ludzi w multi level marketing bądź inne scamy dotyczące inwestycji) w szyfrowanych aplikacjach i ciężej jest pociągnąć ich do odpowiedzialności.

Przykład:



źródło: screenshoty własne autora

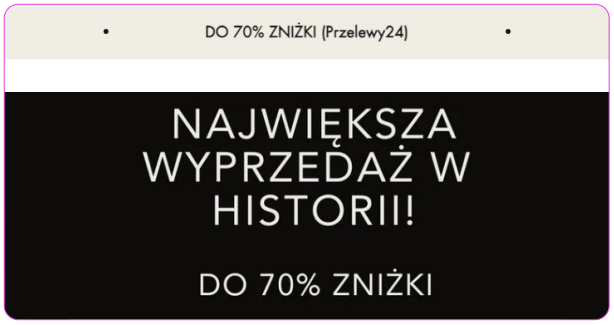
Fałszywe sklepy internetowe

Często też można natknąć się na fałszywe ogłoszenia dotyczące przedmiotów. Strony te często reklamują się na mediach społecznościowych i zdarza się, że stosują nawet takie same opisy, np. przedstawiając rzewną historię o upadku rodzinnej firmy i ogłaszając wyprzedaż kolekcji. Wszystko może wyglądać dobrze na początku – po „zakupie" możesz otrzymać potwierdzenie zamówienia i informację o wysyłce, jednak paczka nigdy do Ciebie nie dotrze, pieniądze nie zostaną zwrócone, a dodatkowo – oszust może znać dane Twojej karty. Zdjęcia, których używają, łatwo można znaleźć na innych stronach za pomocą wyszukiwania obrazem (a teraz często też stwarzane są przez AI).

Przykład:

– niepewny dostawca

– automatyczne tłumaczenie



– granie na emocjach, zachęcenie

– brak symbolu kłódki

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

źródło: klejnotyodliesbeth.pl

Clickbaity

To najczęściej nagłówki artykułów, które wykorzystują sensacyjne słowa, prowokacyjne twierdzenia lub tajemnicze zapowiedzi, żeby nakłonić odbiorcę do kliknięcia w tekst czy reklamę z zainfekowanym linkiem (opisane szerzej w poprzedniej lekcji).

2. Jak chronić się przed scamem?

1. Think before you click - zastanów się za każdym razem, zanim klikniesz w link bądź będziesz chciał podzielić się prywatną informacją.
2. Jeśli znajomy prosi Cię o przelew lub podanie numeru telefonu, skontaktuj się z nim innym kanałem, by potwierdzić prawdziwość prośby lub zadaj tej osobie pytanie weryfikujące, na które tylko ona będzie znała odpowiedź - np. Gdzie się poznaliśmy?. Jeśli dostajesz taką prośbę od osoby publicznej, którą obserwujesz - sprawdź czy konto, z którego została wysłana wiadomość, jest zweryfikowane.
3. Uważaj na reklamy oraz rozdania, szczególnie w okolicach Świąt lub Black Friday - wiele oszustów wykorzystuje okresy promocyjne i ekscytację okazjami, by uśpić czujność odbiorców. Zawsze sprawdzaj czy w adresie strony czy nazwie sklepu nie ma literówki - np. Żabkaa zamiast Żabka. Uważaj szczególnie na oferty limitowane - chcą wywołać na Tobie presję.
3. **Zgłaszaj podejrzane wiadomości!** Podejrzane wiadomości email: wejdź na stronę pod adresem **incydent.cert.pl**. Wskaż, że chcesz zgłosić incydent jako osoba fizyczna. Wybierz odpowiednią kategorię – „Podejrzana wiadomość e-mail". Przesyłaj podejrzane wiadomości SMS na numer: **8080**.
4. Skorzystaj z darmowego narzędzia Trend Micro do weryfikacji bezpieczeństwa strony: **global.sitesafety.trendmicro.com/**

3. Co robić, jeśli dasz się oszukać lub klikniesz w zainfekowany link?

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 do CERT.

Do CERT możesz zgłaszać takie incydenty cyberbezpieczeństwa, jak: złośliwe domeny wyłudzające dane osobowe lub pieniądze, podejrzane wiadomości e-mail i SMS, fałszywe sklepy internetowe, próby podszywania się, złośliwe oprogramowanie, np. próbki wirusów, ransomware, podatności w oprogramowaniu i aplikacjach internetowych, nielegalne treści oraz inne incydenty, które nie pasują do powyższych kategorii.

Pytania do młodzieży:

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?