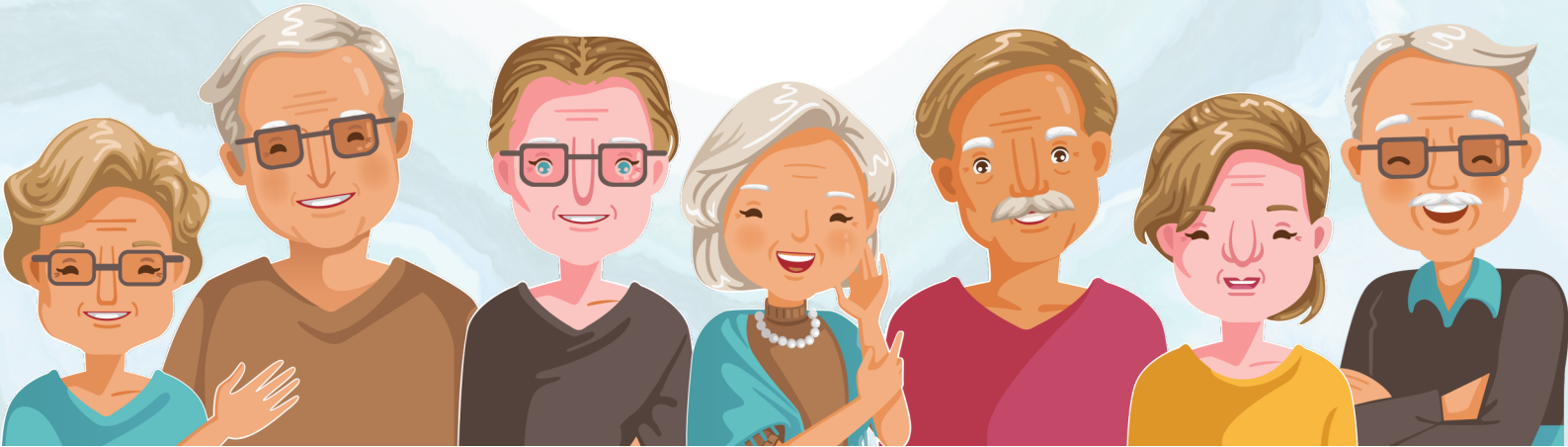
SENIORZY DLA SENIORÓW

MATERIAŁY DODATKOWE

Ćwiczenia i przykłady do kursu i podręcznika



MODUŁ 1
WYKŁAD: DLACZEGO CYBERPRZESTĘPSTWA DZIAŁAJĄ?
PRZYKŁAD NR 1

Udostępnij uczestnikom kursu poniższą rozmowę. Może ona zostać wyświetlona, odczyta na głos, warto zaangażować seniorów do odgrywania ról. Rozmowę można przeczytać/odegrać dwa razy, jeśli grupa wyrazi taką potrzebę.
Po odczytaniu rozmowy, przeprowadź dyskusję na temat: Dlaczego Pani Elżbieta zgodziła się na przekazanie danych do karty, jakich sposobów na wyłudzenie informacji użył złodziej? W razie potrzeby przypomnij uczestnikom „Sześć zasad wpływu" z wykładu numer 1. Uczestnicy mogą samodzielnie zapisać swoje spostrzeżenia, ale sugerujemy przeprowadzenie burzy mózgów , podczas której wypowiedzą się: co ich zaniepokoiło, co zrobili by inaczej?

Podkreśl: Podczas omawiania zadania podkreśl, że cyber przestępcy używają prawdziwych historii i sytuacji, wzbudzają poczucie winy, wyrzuty sumienia lub grają na chęci pomocy innym.

Scenariusz rozmowy:

Złodziej: Witam, nazywam się Monika Nowak, jestem wolontariuszem w organizacji PomocDlaUkrainy.pl, na pewno słyszała Pani o nas reportaż w stacji telewizyjnej TVN i TVP. Ostatnio kupiliśmy i przekazaliśmy obywatelom Ukrainy ponad milion środków ochrony osobistej i środków medycznych. Wspólnie z darczyńcami ocaliliśmy ponad 250 000 osób, w tym przede wszystkim dzieci. Chciałabym zapytać, jak ocenia Pani działalność charytatywną na rzecz pomocy Ukrainie?

Elżbieta Kowalska: Dzień dobry, tak, tak słyszałam, to wspaniale że ratujecie czyjeś życie, słyszałam, że te biedne dzieci strasznie tam cierpią.

Złodziej: Bardzo się cieszę, że zna Pani nasza organizację, popiera nasze działania i pomaganie innym. Jak Pani wie, zbieramy środki na ratowanie życia, na środki medyczne, szczególnie dla dzieci, które jak Pani wspomniała cierpią najbardziej. Bardzo nas cieszy, że w tym trudnym czasie są ludzie którzy otwierają swoje serca i nie są obojętni na cierpienie niewinnych dzieci.

Elżbieta Kowalska: Tak, to straszne, nie mogę sobie wyobrazić co przeżywają ci ludzie.

Złodziej: Za każdym razem kiedy jedziemy z transportem leków na Ukrainę, ludzie opowiadają nam jak bardzo się boją, jak są zagubieni, jak cierpią z powodu ran, odbierania im domów, śmierci bliskich. Dzięki wsparciu ludzi takich jak Pani, dajemy tym ludziom i dzieciom tak potrzebne poczucie wsparcia i bezpieczeństwa w tych okrutnych czasach wojny. Jak Pani wspomniała popiera nasze działania, wierzę że jest Pani również przychylna wsparciu materialnym cierpiących dzieci. Nikt przecież nie chce, aby cierpiały lub zmarły w skutek ran po postrzeleniach czy wybuchach bomb.

Elżbieta Kowalska: Uuummm, tak to oczywiste, popieram pomoc, bardzo chciałabym pomóc, ale jest teraz tyle wyłudzeń, ostatnio zaniosłam do naszego Kościoła koce i zabawki.

Złodziej: Ma Pani prawo odczuwać wątpliwości, to skandaliczne, że ktoś próbuje zarobić na nieszczęściu innych, na szczęście jesteśmy znaną organizacją. Słyszała Pani również o naszej ostatniej akcji dostawy środków medycznych na Ukrainę, zdjęcia z naszego transportu na przejściu granicznym w Dorohusku obiegły całą Europę, skala dostarczonej pomocy była ogromna. Obecnie zbieramy na wyposażenie szpitala w Chersoniu, może nas Pani wesprzeć niewielką kwotą -10 zł?

Elzbieta Kowalska: Dobrze, ale nie wiem jak to zrobić?

Złodziej: Proszę się nie martwić, przeprowadzę Panią przez cały proces, to proste i zajmie tylko 2 minuty, proszę o przygotowanie karty do bankomatu oraz podanie numeru.

MODUŁ 1
WYKŁAD: DLACZEGO CYBERPRZESTĘPSTWA DZIAŁAJĄ?
PRZYKŁAD NR 2

Udostępnij uczestnikom kursu poniższą rozmowę. Może ona zostać wyświetlona, odczyta na głos, warto zaangażować seniorów do odgrywania ról. Rozmowę należy przeczytać/odegrać dwa razy.

1. Pierwsze odczytanie rozmowy, powinno dotyczy wyłącznie słów złodzieja i klientki;
2. Drugie odczytanie rozmowy powinno zostać przeprowadzone z komentarzem z nawiasów.

Po pierwszym odczytaniu rozmowy, przeprowadź dyskusję, dlaczego klientka zgodziła się na przekazanie danych karty, jakich sposobów użył złodziej? W razie potrzeby przypomnij uczestnikom „Sześć zasad wpływu" z wykładu numer 1. Niech uczestnicy zapisują swoją spostrzeżenia, uwagi, co ich zaniepokoiło, co zrobili by inaczej.
Po drugim czytaniu, przeprowadź dyskusję, dowiedz się czy podpowiedzi z nawiasów są zrozumiałe dla uczestników, czy coś ich zastanowiło, zwróciło ich uwagę?

Scenariusz rozmowy:

Oszust: Dzień dobry, z tej strony Maria Kowalczyk, jestem pracownikiem banku KaszIn, czy rozmawiam z właścicielem konta?

Oszust przedstawia się z imienia i nazwiska, dając nam fałszywe poczucie bezpieczeństwa. Dane są wymyślone, jednak z reguły ufamy bardziej osobom, które podają nam swoje imię i nazwisko. Ta technika usypia naszą czujność – wszystko dzieje się tak jak podczas standardowej rozmowy, gdy konsultant bankowy dzwoni do swoich klientów. Istnieje wiele sposób, aby wyłudzić dane użytkowników banków czy telefonów komórkowych. Złodzieje mogą nawet rozpocząć rozmowę od zwrócenia się do nas pełnym imieniem i nazwiskiem.

Klient: Dzień dobry, tak, przy telefonie.

Oszust: Dzwonię w bardzo pilnej sprawie, system odnotował podejrzaną transakcję na Pani koncie, podjęliśmy kroki, aby zabezpieczyć Pani środki, zablokowaliśmy chwilowo Pani konto, aby złodzieje nie mogli ukraść zgromadzonych oszczędności.

Numer telefonu z którego dzwoni oszust jest podpisany jako nasz bank – identyfikacja numeru jest łatwa do podrobienia. Oszust mówi powoli i zdecydowanie oraz używa języka który pasuje do pracownika banku. Po pierwszych sekundach, kiedy słyszymy że ktoś chciał ukraść nasze pieniądze czujemy się zestresowani, może nawet przerażeni sytuacją. Chcemy jak najszybciej działać. Dlatego odczuwamy ulgę, bo osoba która jest po drugiej stronie telefonu, uniemożliwiła to przestępstwo, czujemy się wdzięczni, ufamy tej osobie, gdyby chciała nam zaszkodzić, nie pomagałaby nam w tak ważnej sprawie.

Klient: Oh nie! To straszne, jak to możliwe, jak to się stało?

Oszust: Odnotowaliśmy próbę wykonania z Pani konta przelewu na nr konta rozpoznany przez system jako podejrzany, ktoś zalogował się z niemieckiego ID, z Hamburga, prawdopodobnie ktoś zdobył Pani dane, musimy zabezpieczyć konto, aby się to nie powtórzyło w przyszłości.

Oszust podaje szczegóły, które mają nas przekonać, że rozmawiamy z prawdziwym pracownikiem banku. Daje nam poczucie ulgi, że dzięki działaniom banku nie straciliśmy naszych pieniędzy, oszust powtarza kluczowe informacje, dając nam poczucie pewności że rozmawiamy z osobą kompetentną, która zna nasz temat, nie jest z przypadku. Czujemy się zobowiązani kontynuować rozmowę i podać wszelkie potrzebne informacje. Naszą czujność usypia też fakt, że złodziej nie chce od nas pieniędzy - a jedynie dane, które jak wiele osób mylnie uważa nie są ważne czy cenne. Oszust podczas całej rozmowy sprawia wrażenie zatroskanego naszym losem i jedynego, który może nam pomóc zabezpieczyć nasze środki finansowe. W zamian oczekuje - jak nam się wydaje - niewiele, tylko dane.

MODUŁ 1
WYKŁAD: DLACZEGO CYBERPRZESTĘPSTWA DZIAŁAJĄ?
PRZYKŁAD NR 2

Klient: Jak to się mogło stać, nie rozumiem, czy moje pieniądze są bezpieczne?

Oszust: Złodzieje mogli zainstalować na Pani komputerze złośliwe oprogramowanie, które umożliwiło im wejście na Pani konto, najważniejsze jest, aby działać szybko! Dopóki złodzieje mają dostęp do Pani konta, środki wciąż są zagrożone. Musimy przeprowadzić weryfikację danych logowania, po ich zmianie złodzieje, nie będą już w stanie ukraść Pani oszczędności.

Złodziej ma czas na rozmowę, wytłumaczy nam, wyjaśnia, złodziejowi się nie spieszy, chce zdobyć nasze zaufanie, jednocześnie wprowadzając poczucie pośpiechu, nie możemy tracić czasu. Jeśli nie będziemy działać teraz, możemy stracić pieniądze, mimo, że bank zrobił już tak wiele, żeby nam pomóc. Oszust wielokrotnie powtarza, słowa „zagrożenie", „ukraść".

Klient: Oczywiście, zrobię wszystko, żeby zabezpieczyć moje oszczędności, ale nie wiem co, nigdy nie używałam tych internetowych płatności, nie rozumiem, jak ukradli moje dane.

Oszust: Jestem tutaj, aby bezpiecznie przeprowadzić Panią przez całą procedurę, pomogę na każdym etapie, ale musimy działać zdecydowanie, złodzieje w każdej chwili mogą ponownie próbować zhakować Pani konto.

Oszust upewnia nas w przekonaniu że jest po to, aby nam pomóc, ponownie wprowadza atmosferę pośpiechu, ale w sposób który sugeruje, że to przez złodzieja musimy się spieszyć, a nie przez asystenta banku.

Klient: Dobrze, dobrze, czy mogę zadzwonić do wnuczka, on się zna na tych komputerach, pomoże.

Oszust: Oczywiście, ale niestety mamy bardzo mało czasu na działanie, złodzieje mogą w każdej chwili ponownie próbować ukraść Pani środki, jeśli ma Pani wątpliwości co do autentyczności naszej rozmowy, może się Pani rozłączyć i ponownie zadzwonić na nr infolinii banku, który się wyświetlił na telefonie. Proszę tylko pamiętać, jeśli nie przeprowadzimy weryfikacji w ciągu następnych 5 minut, możemy nie zdążyć na czas, aby ponownie zablokować niebezpieczną transakcję.

Oszust, potencjalnie daje nam możliwość zweryfikowania kim jest, skoro nie boi się bycia zdemaskowanym, w takim razie musi być prawdziwym pracownikiem banku. Złodziej dalej utrzymuje pośpiech, nerwową atmosferę, wymuszając na nas działanie).

Klient: Nie mogę stracić swoich oszczędności, co mam zrobić?

Oszust: Proszę się nie martwić, jeśli szybko dokonamy weryfikacji i zmiany danych, oszczędności będą bezpieczne. Proszę o przygotowanie Pani karty bankomatowej oraz dowodu osobistego, musimy przeprowadzić weryfikację Pani tożsamości – to standardowa procedura, przez którą musimy przejść, aby zabezpieczyć konto.

Oszust zapewnia nas o dobrych zamiarach, powołuje się na procedury bankowe, wszystko wydaje się bardzo profesjonalne, dokładnie tak jakbyśmy rozmawiali z przedstawicielem banku. Zdecydowany i spokojny ton głosu sprawia, że mimowolnie wykonujemy polecenia.

MODUŁ 1
WYKŁAD: DLACZEGO CYBERPRZESTĘPSTWA DZIAŁAJĄ?
PRZYKŁAD NR 2

Klient: Mam już kartę i dowód, co teraz?

Oszust: Proszę o podanie numeru PESEL, daty i miejsca urodzenia.

Pracownik banku, gazowni, policjant, urzędnik, nigdy nie poprosi nas o podanie danych z karty lub dowodu osobistego, proszenie o takie dane powinno od razu nas zaniepokoić.

Klient: No nie wiem, w telewizji dużo mówili, żeby nie podawać takich danych przez telefon, że to niebezpieczne.

Oszust: Tak jak mówiłam wcześniej mamy bardzo mało czasu, zdołaliśmy raz zablokować przelew, ale ponownie może się to nie udać, prosimy tylko o niezbędne dane. To tylko numer PESEL i dane urodzenia. Służące do wykonania weryfikacji i zablokowania transakcji. Jeśli boi się Pani zaufać pracownikowi banku, mogę podać Pani wewnętrzny numer identyfikacji pracownika, po którym bez problemu będzie Pani w stanie zweryfikować autentyczność przeprowadzanej weryfikacji, nie powinnam tego robić, ale jeśli dzięki temu poczuje się Pani bezpiecznej, proszę zapisać 236-66-01

Oszust robi nam przysługę podając dane, których jak twierdzi, nie powinien podawać. Ma to za zadanie wzbudzić w nas fałszywe poczucie bezpieczeństwa i zobowiązanie do odwdzięczenia się. Znów, słyszymy, że jest mało czasu. Oszust zapewnia, że przekazywane dane nie są wcale tak ważne.

Klient: Nie, oczywiście, już podaję.

Oszust: Dziękuję. Weryfikacja zakończyła się pozytywnie, Pani konto zostało zabezpieczone, zgłosiliśmy również przestępstwo na policję, za chwilę może kontaktować się z Panią aspirant Piotrkowski, który prowadzi sprawę, aby dopytać o szczegóły. Proszę czekać na kontakt. Gdyby pojawiły się jakieś pytania proszę o oddzwonienie na numer, który się Pani wyświetlił.

Oszust upewnia się, że nie zadzwonimy na policję aby zgłosić sprawę. Dodatkowo podkreśl, że w przypadku dodatkowych pytań mamy dzwonić na fałszywy numer. Znów jest dla nas uprzejmy i pomocny. Złodzieje, mogą po chwili zadzwonić znów i udawać policjanta, który rzekomo prowadzi sprawę. Wszystko po to, aby wyłudzić dalsze dane, zniechęcić nas do kontaktu z prawdziwą policją, co da im czas na "zniknięcie" i zatarcie śladów.

MODUŁ 2
TYPY OSZUSTW
ĆWICZENIA I PRZYKŁADY

Ćwiczenie nr 1

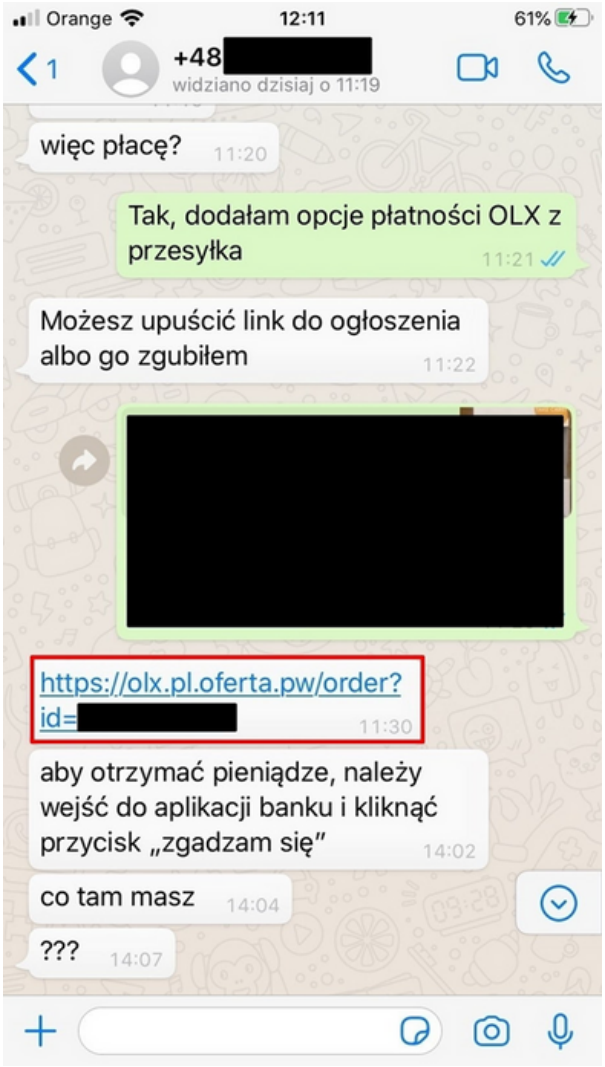
DYSKUSJA. Omów z uczestnikami kursu:

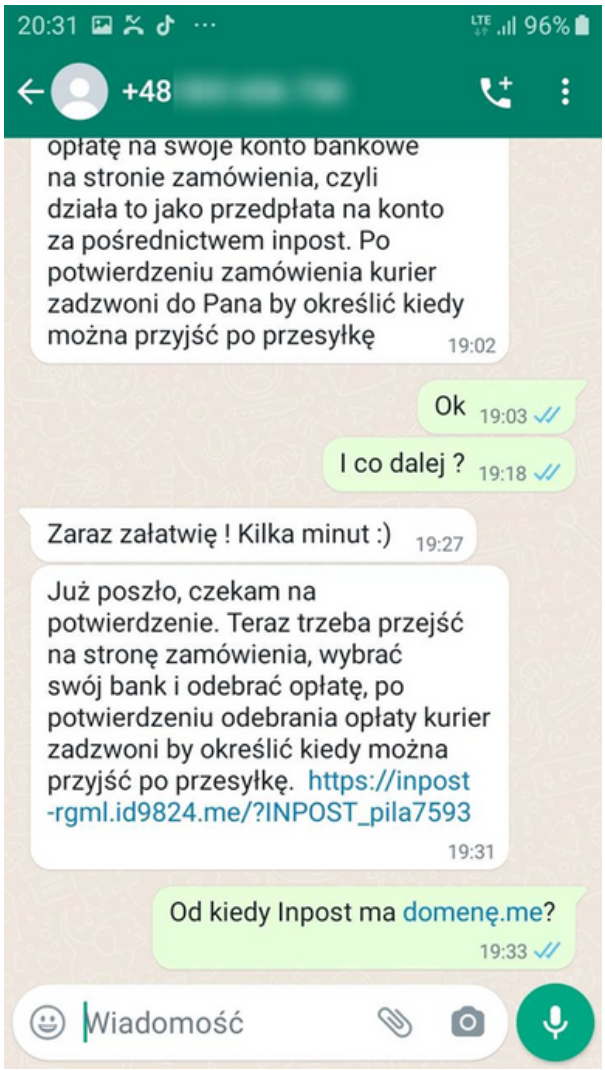
1. Czy którykolwiek uczestnik/uczestniczka lub jego/jej przyjaciele/krewni zetknęli się z kradzieżą danych lub próbą ich wyłudzenia?
2. W jakim celu oszuści mogą wykorzystywać Twoje dane osobowe? Czy zgodzisz się z twierdzeniem że mogą je wykorzystywać do „prania brudnych pieniędzy", oszustw podatkowych, brania pożyczek?

Ćwiczenie nr 2

PRACA SAMODZIELNA. Udostępnij uczestnikom poniższe przykłady i rozpocznij dyskusję:

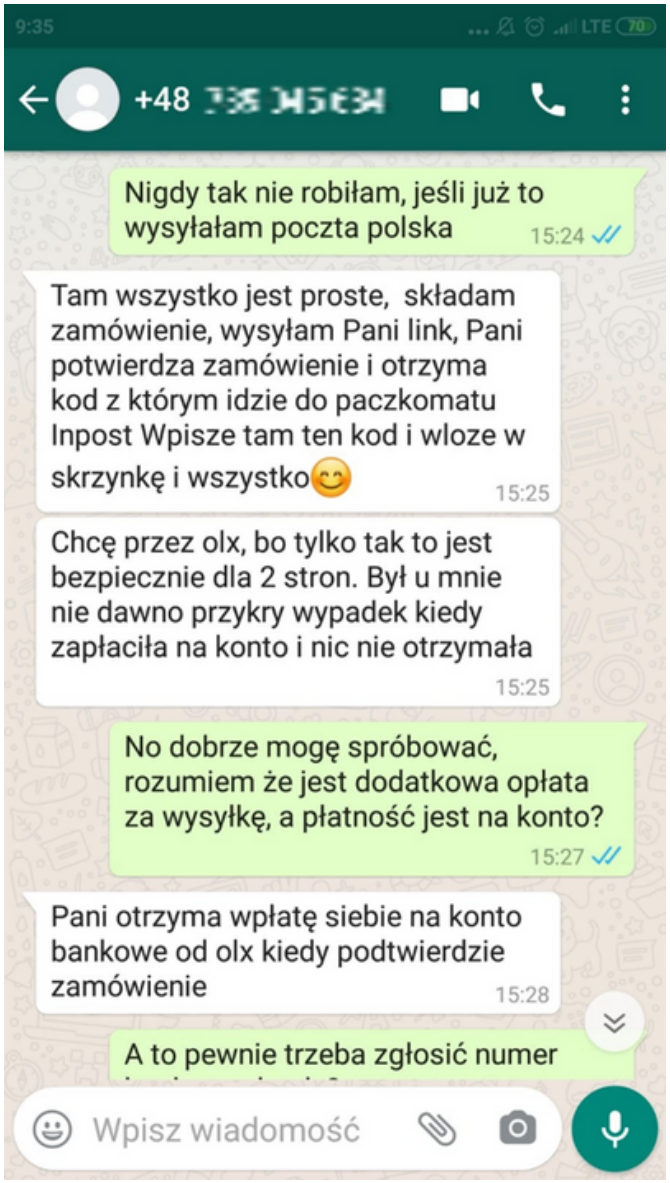
1. Czy widzicie coś podejrzanego? (dziwny link, opis, brak dodatkowych pytań od kupującego, literówki, dziwna konstrukcja zdań)?
2. Co możecie zrobić, aby uniknąć oszustwa? (nie klikać udostępnionego linku, poprosić o płatność przez platformę).

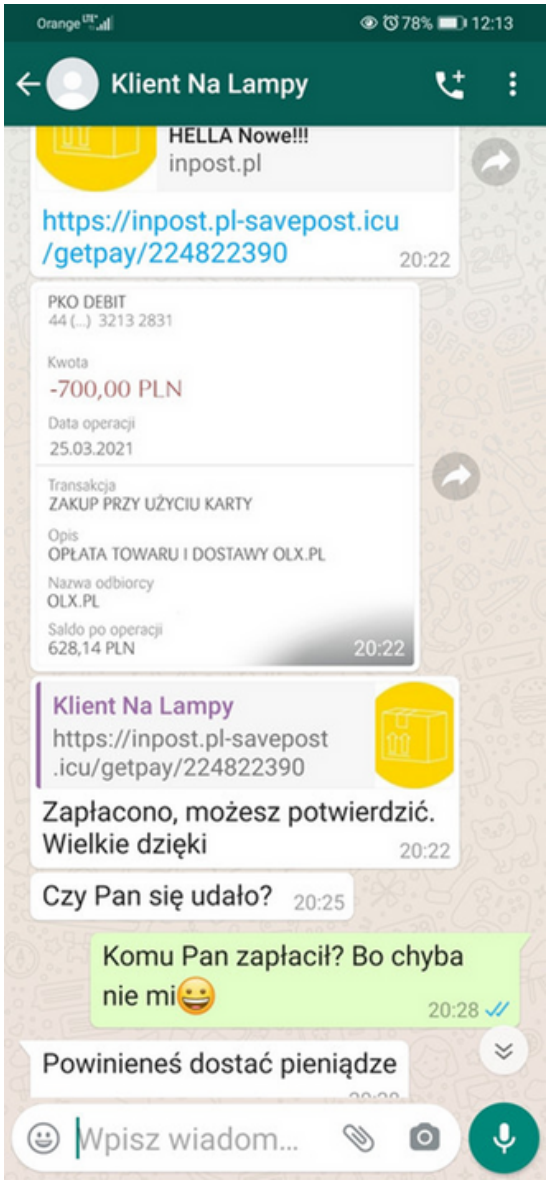




Materiały źródłowe

https://www.auto-swiat.pl/porady/kupno-i-sprzedaz/oszustwa-na-olx-jak-uwazac-na-oszustow-mozesz-duzo-stracic/g8k2e78
https://www.knf.gov.pl/dla_rynku/CSIRT_KNF/Aktualnosci?articleId=73548&p_id=18
https://radomskie.info/uwaga-na-oszustow-na-portalach-sprzedazowych/
https://businessinsider.com.pl/twoje-pieniadze/plaga-oszustw-internetowych-jest-juz-masowa-klienci-olx-inpostu-poczty-polskiej-traca/4wy200v



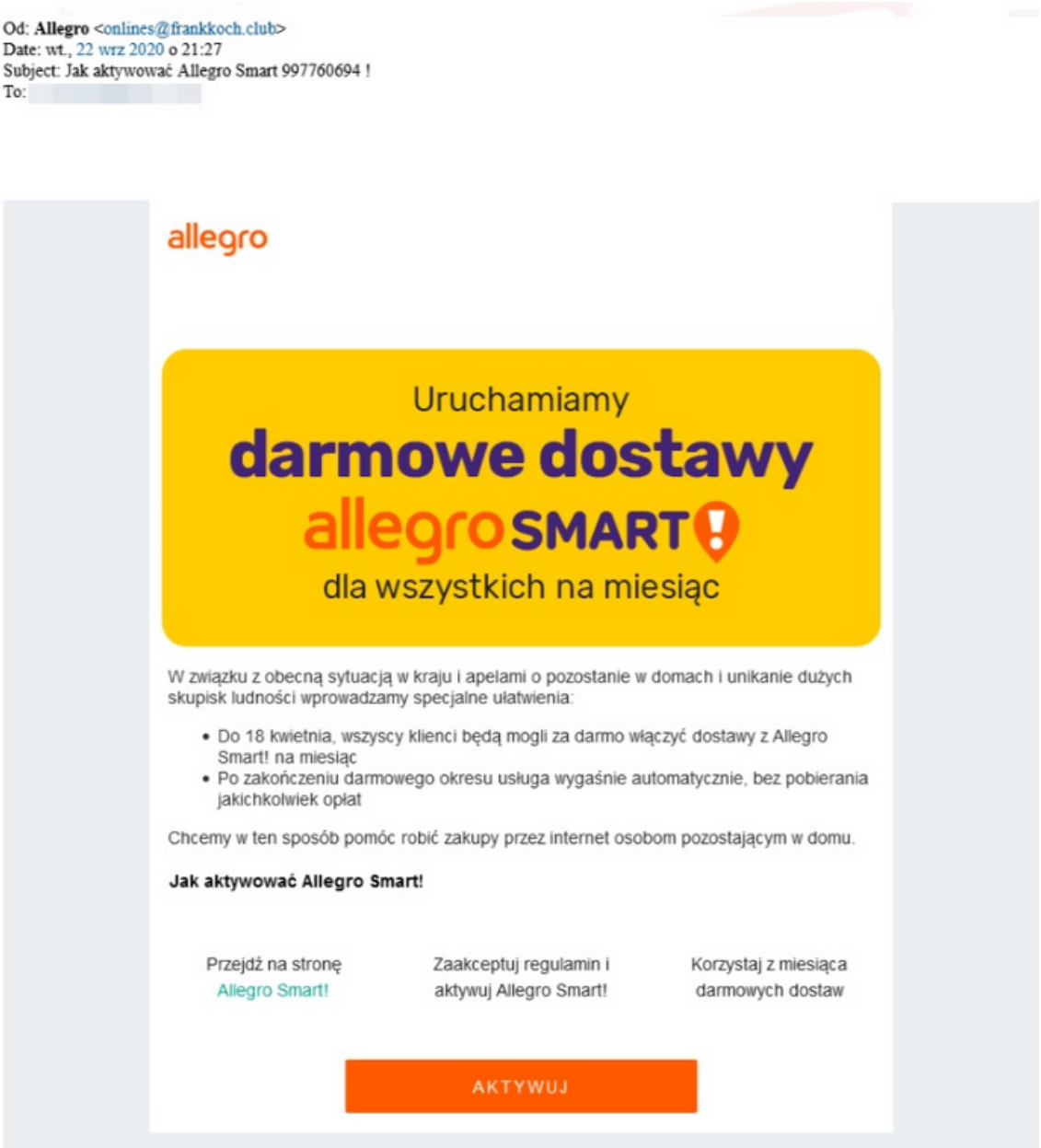


Materiały źródłowe

https://www.auto-swiat.pl/porady/kupno-i-sprzedaz/oszustwa-na-olx-jak-uwazac-na-oszustow-mozesz-duzo-stracic/g8k2e78
https://www.knf.gov.pl/dla_rynku/CSIRT_KNF/Aktualnosci?articleId=73548&p_id=18
https://radomskie.info/uwaga-na-oszustow-na-portalach-sprzedazowych/
https://businessinsider.com.pl/twoje-pieniadze/plaga-oszustw-internetowych-jest-juz-masowa-klienci-olx-inpostu-poczty-polskiej-traca/4wy200v

Ćwiczenie nr 3

PRACA SAMODZIELNA. Udostępnij uczestnikom kursu kartę nr. 3. Poprosić ich o wypowiedzenie się na temat pokazanej wiadomości pochodzącej rzekomo z popularnego sklepu internetowego. Czy dostrzegają elementy, wskazujące na oszustwo? Czy coś ich zaniepokoiło, zwróciło uwagę?



Od: **Allegro** <onlines@frankkoch.club>
Date: wt., 22 wrz 2020 o 21:27
Subject: Jak aktywować Allegro Smart 997760694 !
To:

allegro

Uruchamiamy
darmowe dostawy
allegro SMART!
dla wszystkich na miesiąc

W związku z obecną sytuacją w kraju i apelami o pozostanie w domach i unikanie dużych skupisk ludności wprowadzamy specjalne ułatwienia:

- Do 18 kwietnia, wszyscy klienci będą mogli za darmo włączyć dostawy z Allegro Smart! na miesiąc
- Po zakończeniu darmowego okresu usługa wygaśnie automatycznie, bez pobierania jakichkolwiek opłat

Chcemy w ten sposób pomóc robić zakupy przez internet osobom pozostającym w domu.

Jak aktywować Allegro Smart!

Przejdź na stronę Allegro Smart!	Zaakceptuj regulamin i aktywuj Allegro Smart!	Korzystaj z miesiąca darmowych dostaw

AKTYWUJ

Ćwiczenie nr 4

PRACA W GRUPACH. Podziel uczestników kursu na mniejsze grupy. Udostępnij im kartę numer 4. Poproś o wykonanie krótkiego przewodnika, niech przedstawią w kilku punktach – jak uniknąć internetowego oszustwa dobroczynnego. Nie wszystkie pola musza być wypełnione, jeśli grupa ma więcej wskazówek niech je zapisze, piktogramy nie są podpowiedzią a jedynie dodatkową grafiką.

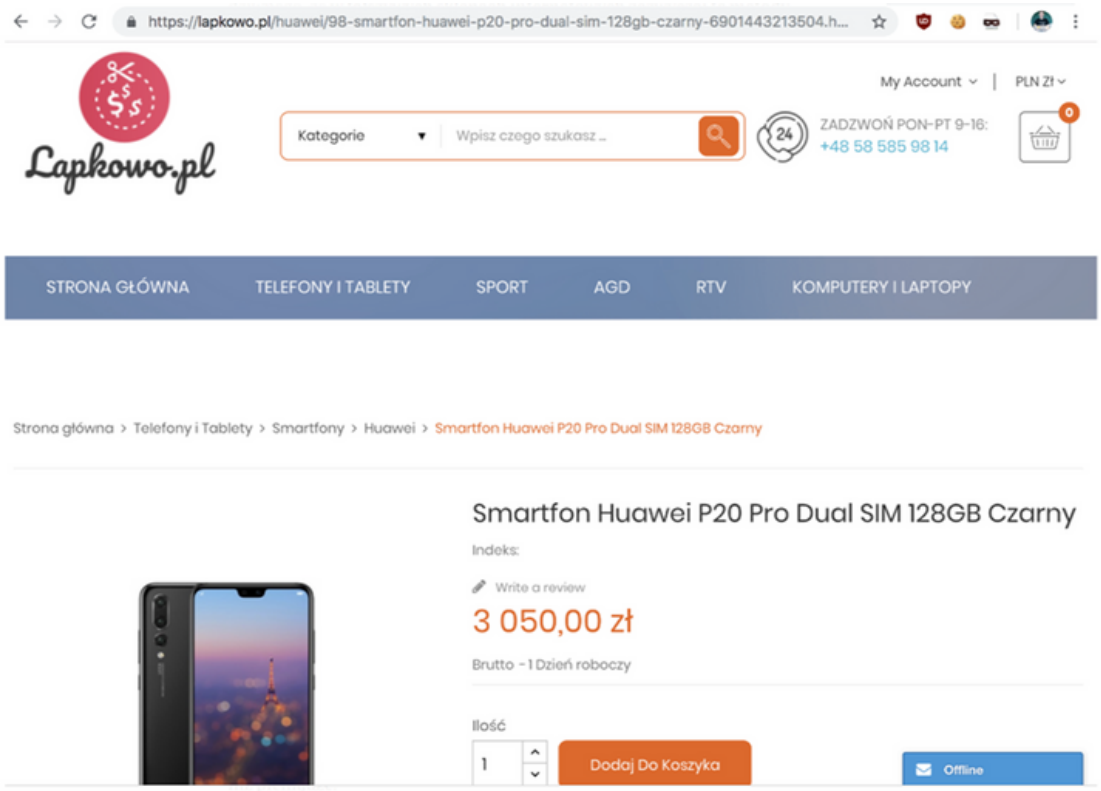
Przykładowe odpowiedzi: 1. Sprawdź daną organizację charytatywną; 2. Sprawdź jakie akcje wspierają; 3. Czy są aktywni w social mediach?; 4. Poproś o identyfikator i pełną nazwę organizacji; 5. Nie płać kartami podarunkowymi, przelewem bankowym, nie przekazuj pieniędzy w pośpiechu.

Przewodnik, jak uniknąć internetowych przestępstw charytatywnych

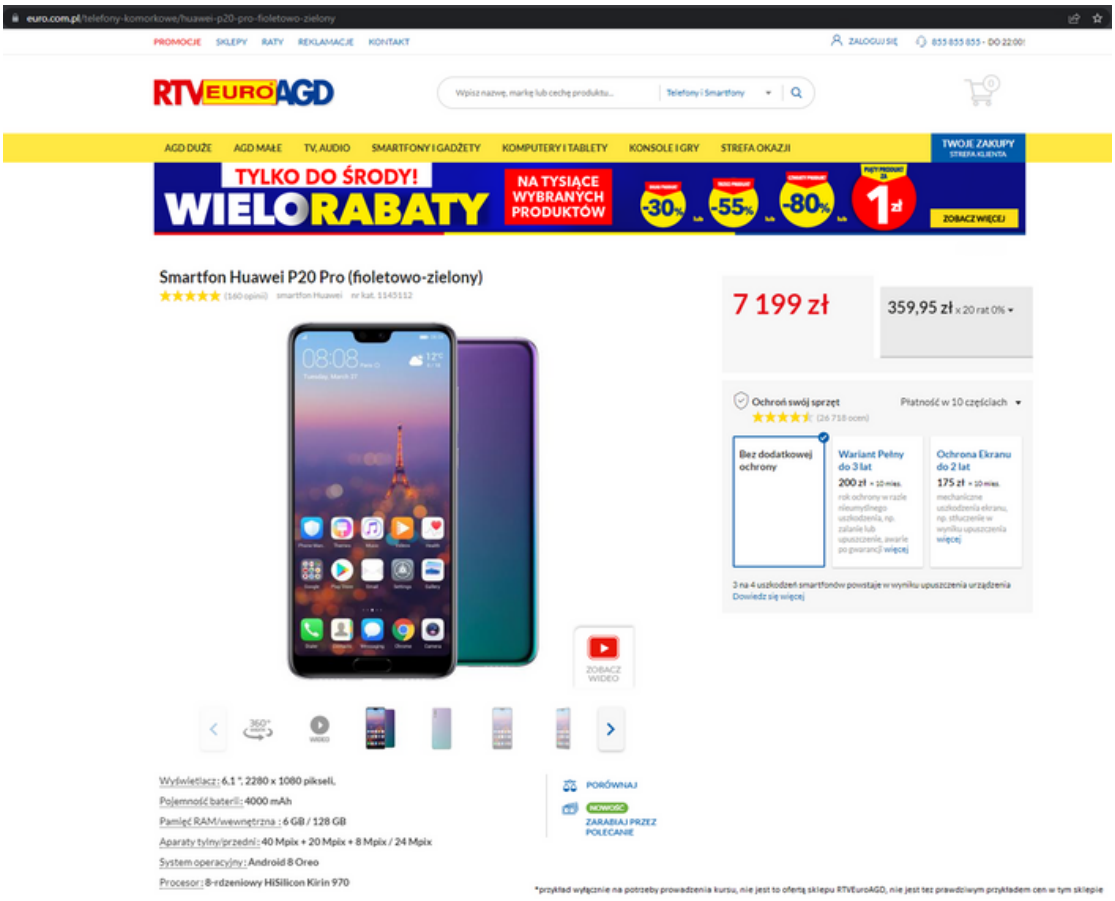
MODUŁ 2
TYPY OSZUSTW
ĆWICZENIA I PRZYKŁADY

Przykład nr 1

DYSKUSJA. Pokaz uczestnikom obydwie karty (przykład, w części został stworzony na potrzeby kursu, aby ukazać różnicę w cenie produktu). Zapytaj na co zwrócili uwagę, co wzbudziło by ich podejrzenia? Zapytaj uczestników o ich zdanie na temat fałszywych sklepów internetowych: czy się z nimi spotkali? widzieli fałszywe oferty?

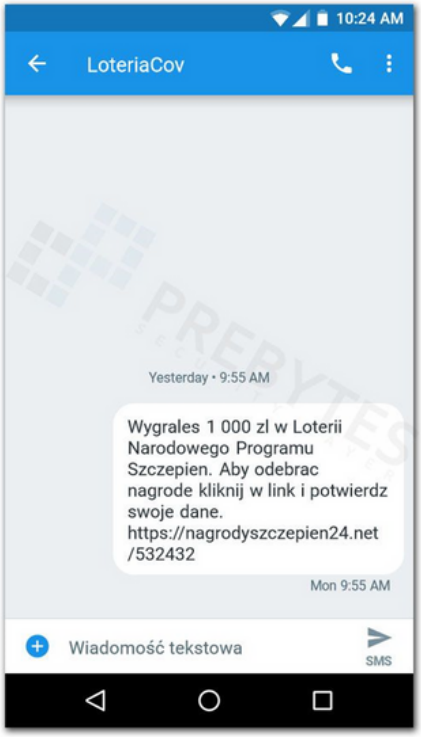


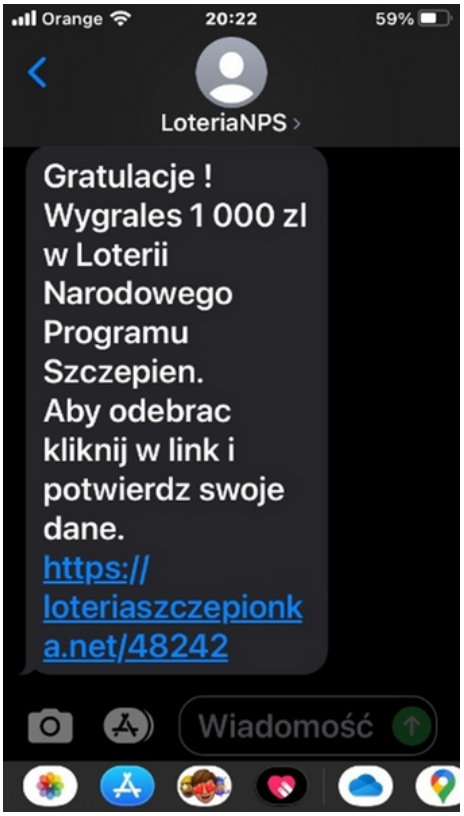
Source: https://kwestiabezpieczenstwa.pl/zakupy-online/

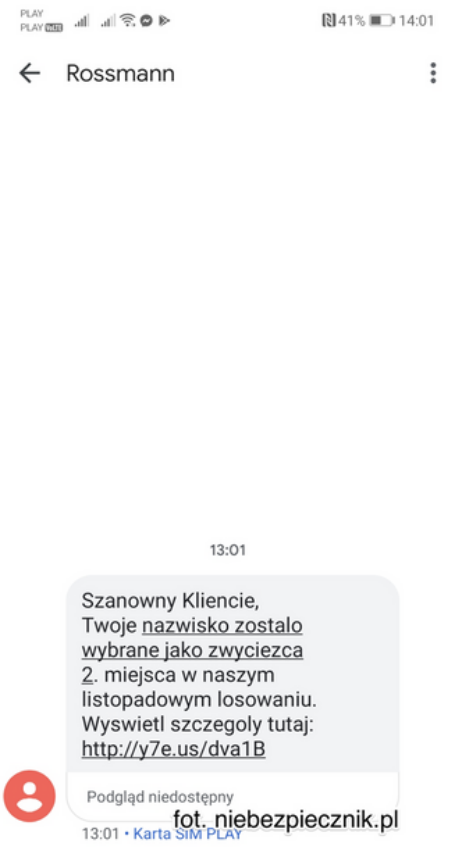


Przykład nr 2

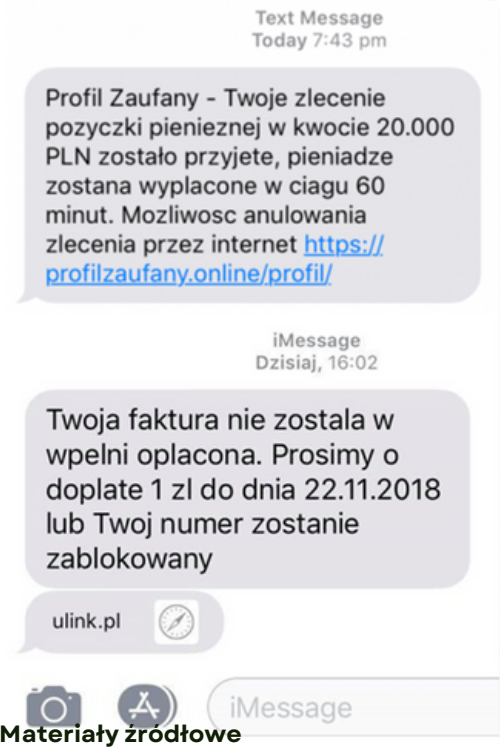
DYSKUSJA. Udostępnij uczestnikom kartę z przykładem nr 2. Rozpocznij dyskusję, zapytaj czy otrzymali kiedyś podobne smsy? Dopytaj: czy widzą elementy wskazujące na próbę oszustwa?

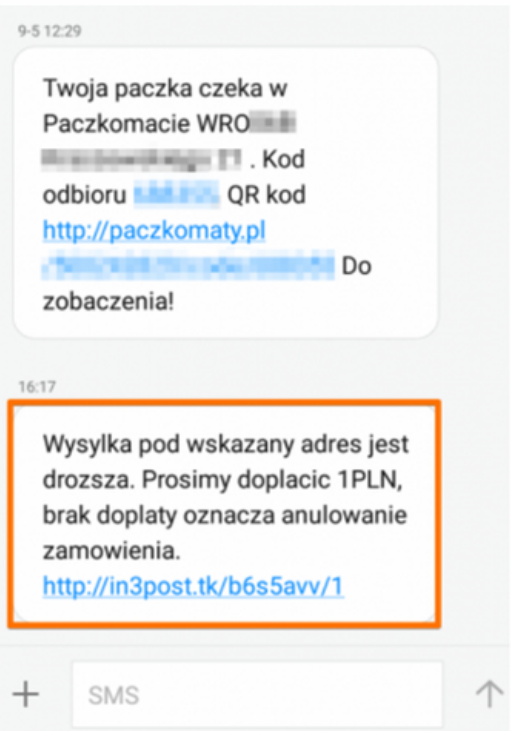


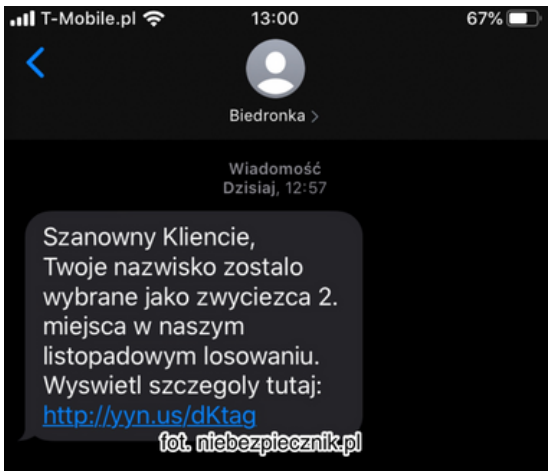




fot. niebezpiecznik.pl



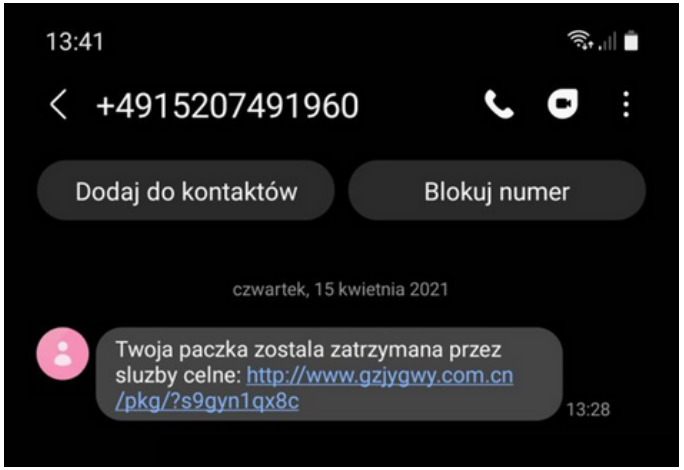


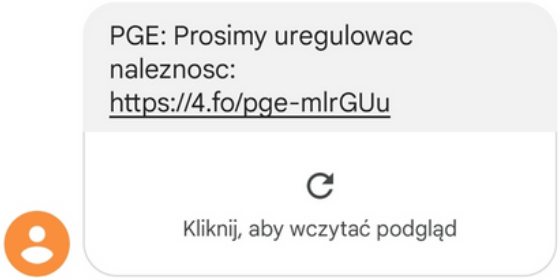


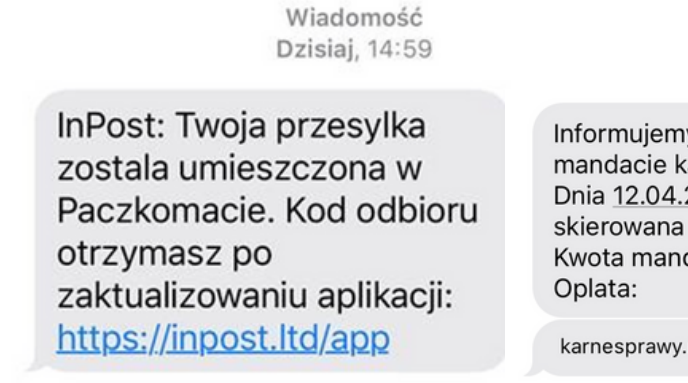
fot. niebezpiecznik.pl

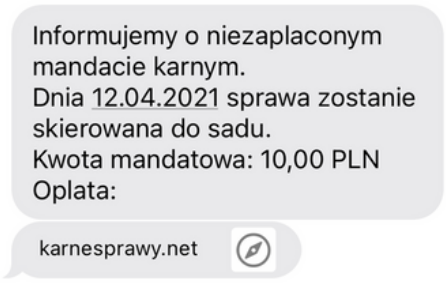
Materiały źródłowe

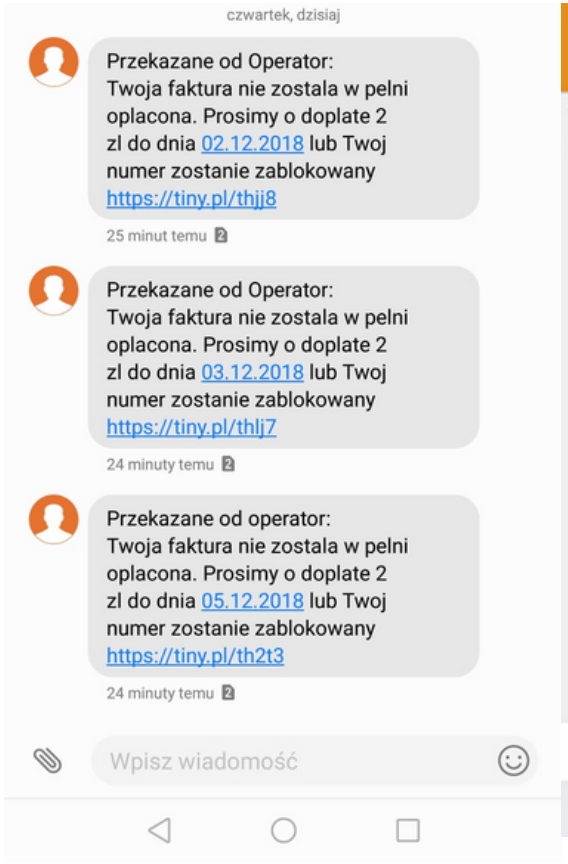
https://niebezpiecznik.pl/post/uwaga-na-sms-y-od-biedronki-i-lidla-informujace-o-wygranej/
https://www.sirt.pl/radio-zet-phishing/
https://biuroprasowe.orange.pl/blog/phishing-na-falszywa-aplikacje-inpost/
https://avlab.pl/ktos-podszywa-sie-pod-play-i-rozsyla-falszywe-wiadomosci-sms/
https://kwestiabezpieczenstwa.pl/phishing/
https://www.telepolis.pl/wiadomosci/bezpieczenstwo/nowa-fala-phishingowych-atakow-sms-udajacych-wiadomosci-od-pge-i-inpost

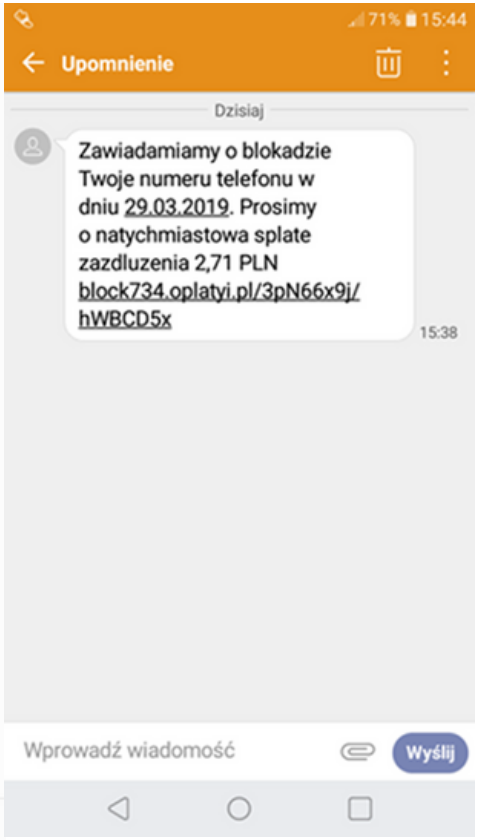


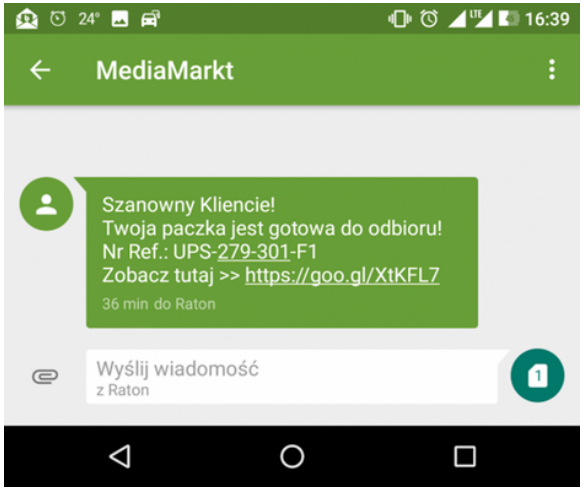


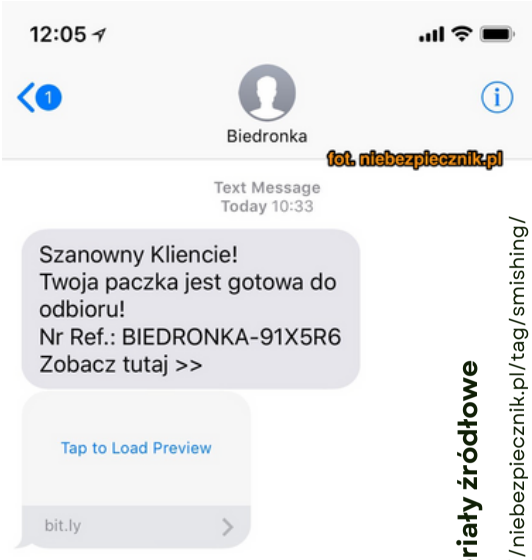












Materiały źródłowe

https://niebezpiecznik.pl/tag/smishing/
https://www.sirt.pl/wygrales-1000-zl-w-loterii-narodowego-programu-szczepien-to-kolejne-oszustwo/
https://niebezpiecznik.pl/post/mediamarkt-sms-iphone-scam/
https://www.nowytydzien.pl/sms-o-wygranej-to-sciema/
https://niebezpiecznik.pl/post/uwaga-na-sms-y-od-biedronki-i-rossmana/
https://kapitanhack.pl/2019/03/11/socjo/phishing-sms-dlaczego-jest-tak-skuteczny/

MODUŁ 3
JAK SIĘ BRONIĆ PRZED CYBER ZAGROŻENIAMI?
ĆWICZENIA I PRZYKŁADY

Ćwiczenie nr 1

PRACA SAMODZIELNA. Udostępnij tabelkę uczestnikom kursu. Niech zadecydują, które hasła są silne i chronią użytkownika, a które słabe i możne je łatwo odgadnąć? Po wykonaniu zadania uczestnicy mogą porównać swoje odpowiedzi i przedyskutować różnice.

Lp.	Hasło	Silne	Słabe
1.	Krysia1234		
2.	Kry$!A0012		
3.	F0ToL@b2!*		
4.	wrzesień2023		
5.	Faceb2024		
6.	Kotki2!zWarszawy		
7.	Rysiek1965		
8.	Wr0C!ooV%&!12		
9.	M!s!#K2020		
10.	S!lneH@sł0		

Ćwiczenie nr 2

PRACA SAMODZIELNA. Udostępnij tabelę uczestnikom kursu. Uczestnicy powinni samodzielnie ją wypełnić, a nawet dodać własne inne aplikacje i programy.

Lp.	Program	Aktualizuje je regularnie? Tak/Nie	Ostatnia aktualizacja: ostatni tydzień/miesiąc/rok
1.	Microsoft Word/Excel itp.		
2.	Microsoft Windows		
3.	Messenger Facebook		
4.	WhatsApp/ Signal		
5.	Aplikacja bankowa		
6.	Antywirus na komputerze		
7.	Antywirus na telefonie		

MODUŁ 3
JAK SIĘ BRONIĆ PRZED CYBER ZAGROŻENIAMI?
ĆWICZENIA I PRZYKŁADY

Ćwiczenie nr 3

PRACA SAMODZIELNA/PRACA W GRUPIE. Udostępnij materiały uczestnikom kursu i podziel ich na mniejsze grupy. Niech wspólnie przeanalizują poniższego fałszywego maila. Jak wiele "czerwonych flag" uczestnicy są w stanie znaleźć? Co ich zaniepokoiło, co zwróciło ich uwagę?

Temat: Informujemy, iż w systemie mbank24 zarejestrowane zostało zlecenie przelewu.
Data: Wed, 01 Aug 2018 09:26:14 +0200
Nadawca: Mbank Polska <mbank24@zoho.eu>
Adresat: mbank24 <mbank24@zoho.eu>

mBank

Drogi Użytkowniku.

Informujemy, iż w systemie mbank24 zarejestrowane zostało zlecenie przelewu, z potwierdzeniem E-mail na odbiorcę.

Tytułem : *NR 0013210/18 - Przelew Krajowy.*

Typ : *Z potwierdzeniem email na odbiorcę.*

W związku ze zrealizowaniem zlecenia, wydane zostało certyfikowane potwierdzenie przelewu.
*Potwierdzenie przelewu zgodne z nową ustawą "RODO", możliwe do otworzenia tylko na komputerach z systemem Microsoft Windows.
Zobacz potwierdzenie.
Potwierdzenie dostępne również w załączeniu (.pdf)

Więcej informacji na temat szczegółów przelewu uzyskasz w swoim "*Certyfikowanym potwierdzeniu przelewu*".

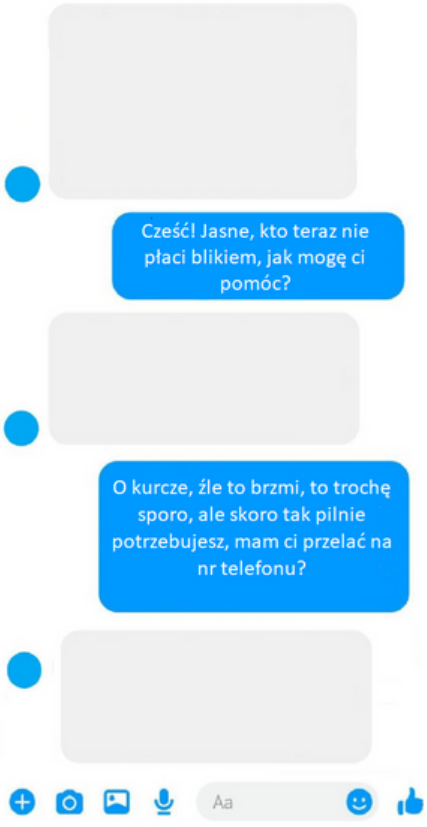
Więcej informacji na temat "*Certyfikowanego potwierdzenia przelewu*" możesz znaleźć na stronie www.mbank.pl.

Pozdrawiamy
Zespół Mbank.

Wiadomość wygenerowana automatycznie przez system Mbank24.pl. Nie odpowiadaj na te wiadomość. W celu uzyskania informacji prosimy o wysłanie nowego emaila pod adres: kontakt@mbank24.pl

Ćwiczenie nr 4

PRACA SAMODZIELNA. Udostępnij uczestnikom poniższe zadanie. Niech seniorzy wyobrażą sobie, że są cyber przestępcami i przejęli konto z Jana Kowalskiego. Wysyłają prośbę o pieniądze do jego przyjaciół. Niech wypełnią puste okienka odpowiedziami, które podałby prawdziwy przestępca.



MODUŁ 3
JAK SIĘ BRONIĆ PRZED CYBER ZAGROŻENIAMI?
ĆWICZENIA I PRZYKŁADY

Ćwiczenie nr 5

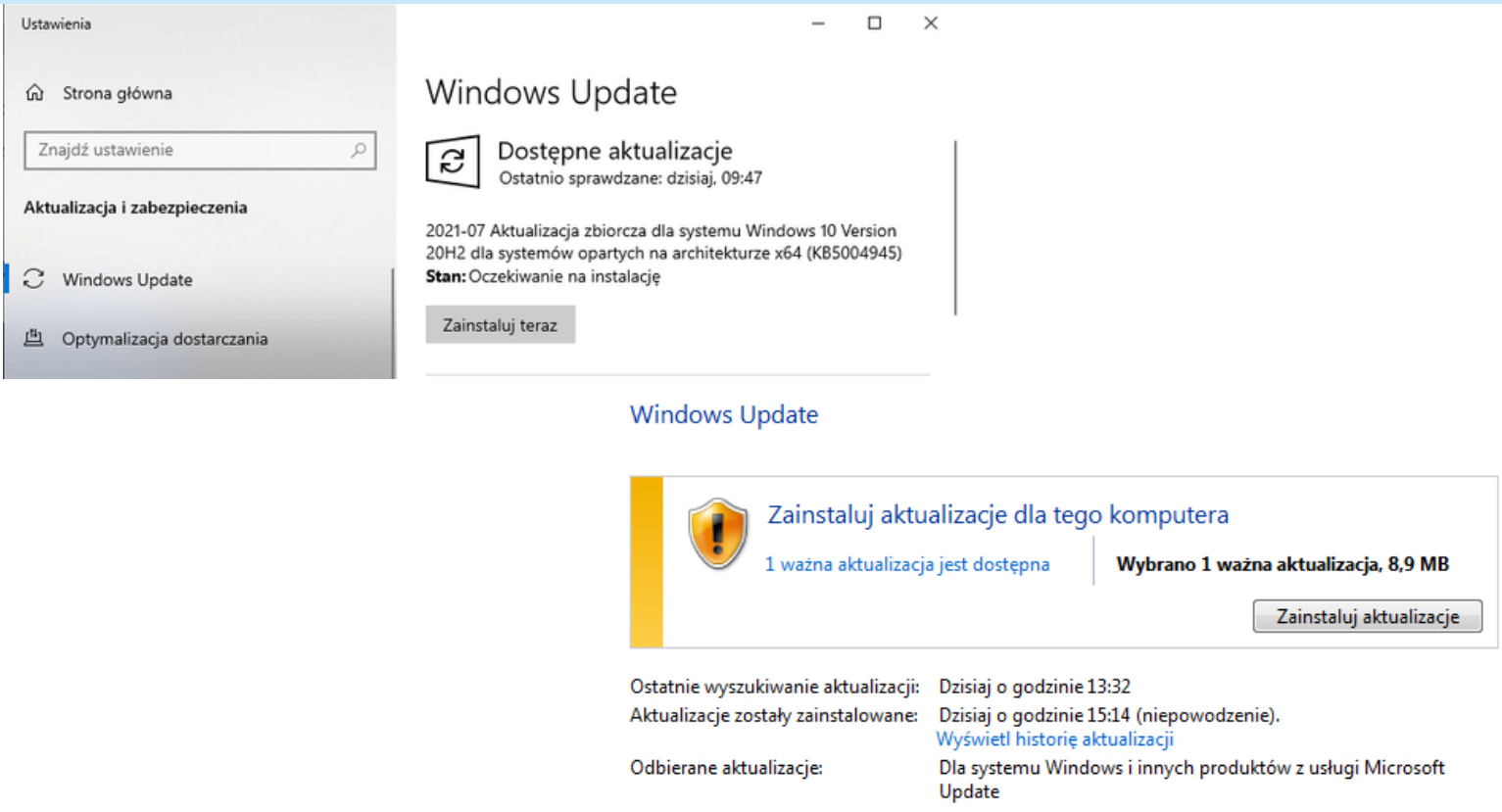
DYSKUSJA. Zaproś uczestników kursu do dyskusji: "Przyjaciel stał się ofiarą cyberprzestępstwa. Czuje się winny/winna". Niech uczestnicy zastanowią się jak odpowiedzieli by na przykładowe stwierdzenia przyjaciela/przyjaciółki.

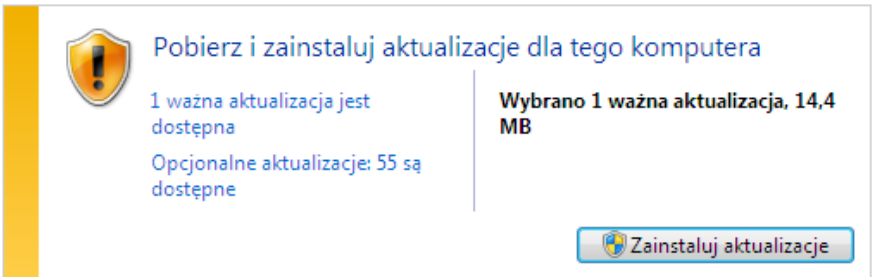
1. Jestem taki/taka głupi/a;
2. Nie powinienem/powinnam już używać maila;
3. Internet nie jest dla mnie;
4. Usunę wszystkie konta na mediach społecznościowych;
5. Policjanci mnie wyśmieją;
6. Nie zgłoszę tego, bank/policja mi nie pomogą.

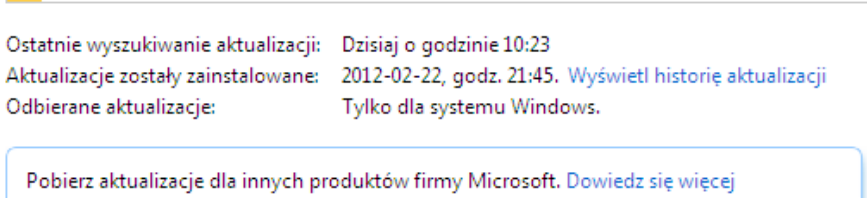
Przykład nr 1

DYSKUSJA. Udostępnij uczestnikom poniższe przykłady powiadomień aktualizacyjnych. Zapytaj uczestników kursu:

1. Ile razy ignorowałeś/ignorowałaś aktualizacje?
2. Ile razy myślałeś/myślałaś, że aktualizacje nie są potrzebne? Może te powiadomienia cię denerwowały, że potrzebują się aktualizować więcej niż raz, w ciągu krótkiego okresu?







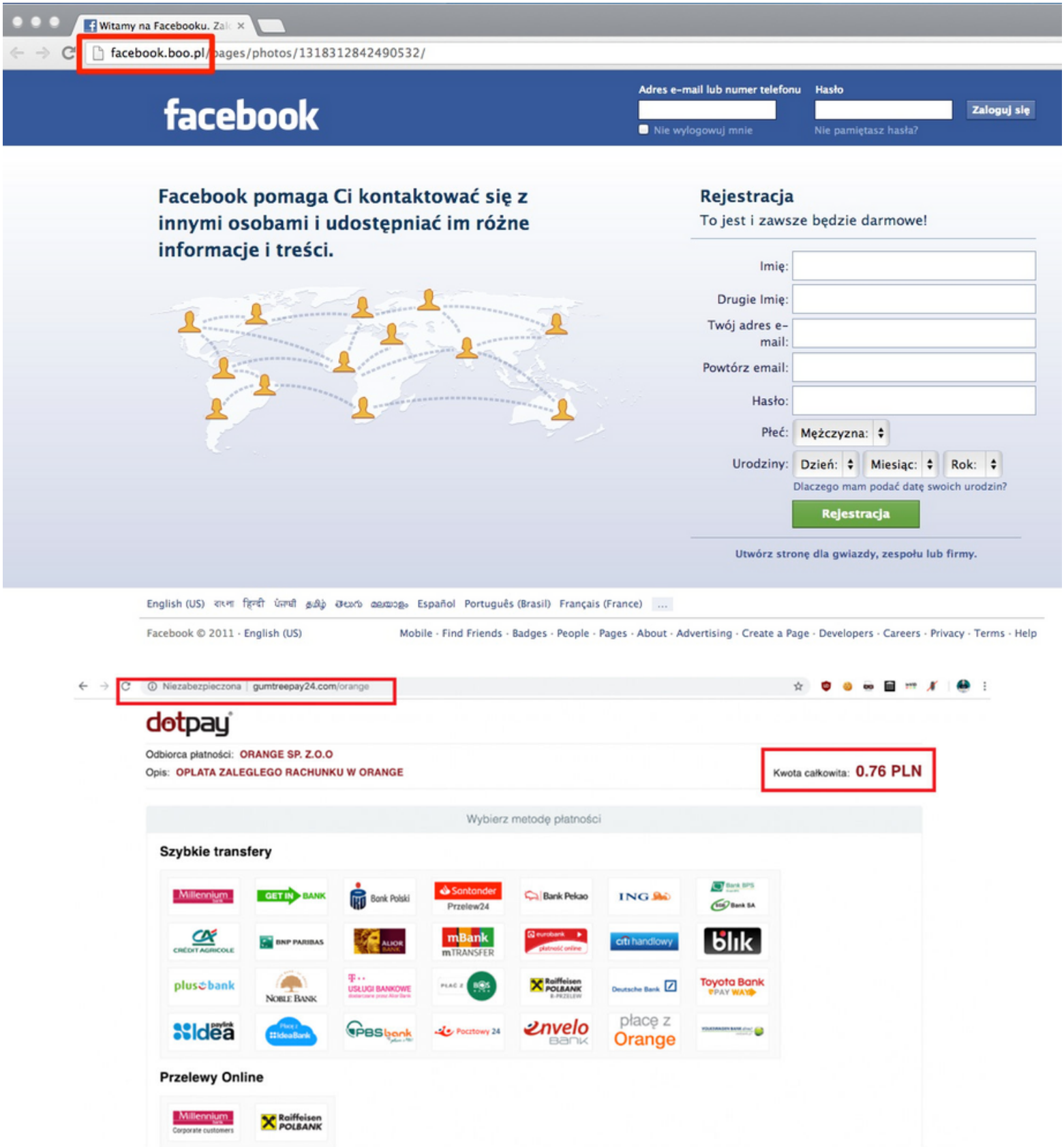
Materiały źródłowe

https://traxter-online.net/aktualizowanie-systemu-poprzez-windows-update-oraz-wsus-offline-update/
https://www.pcworld.pl/news/Musisz-zainstalowac-aktualizacje-KB5004945-natychmiast,429493.html
https://www.elektroda.pl/rtvforum/topic3259556.htm

Przykład nr 2

DYSKUSJA. Udostępnij poniższą fałszywą stronę uczestnikom kursu i rozpocznij dyskusję pytaniami: Czy pamiętasz:

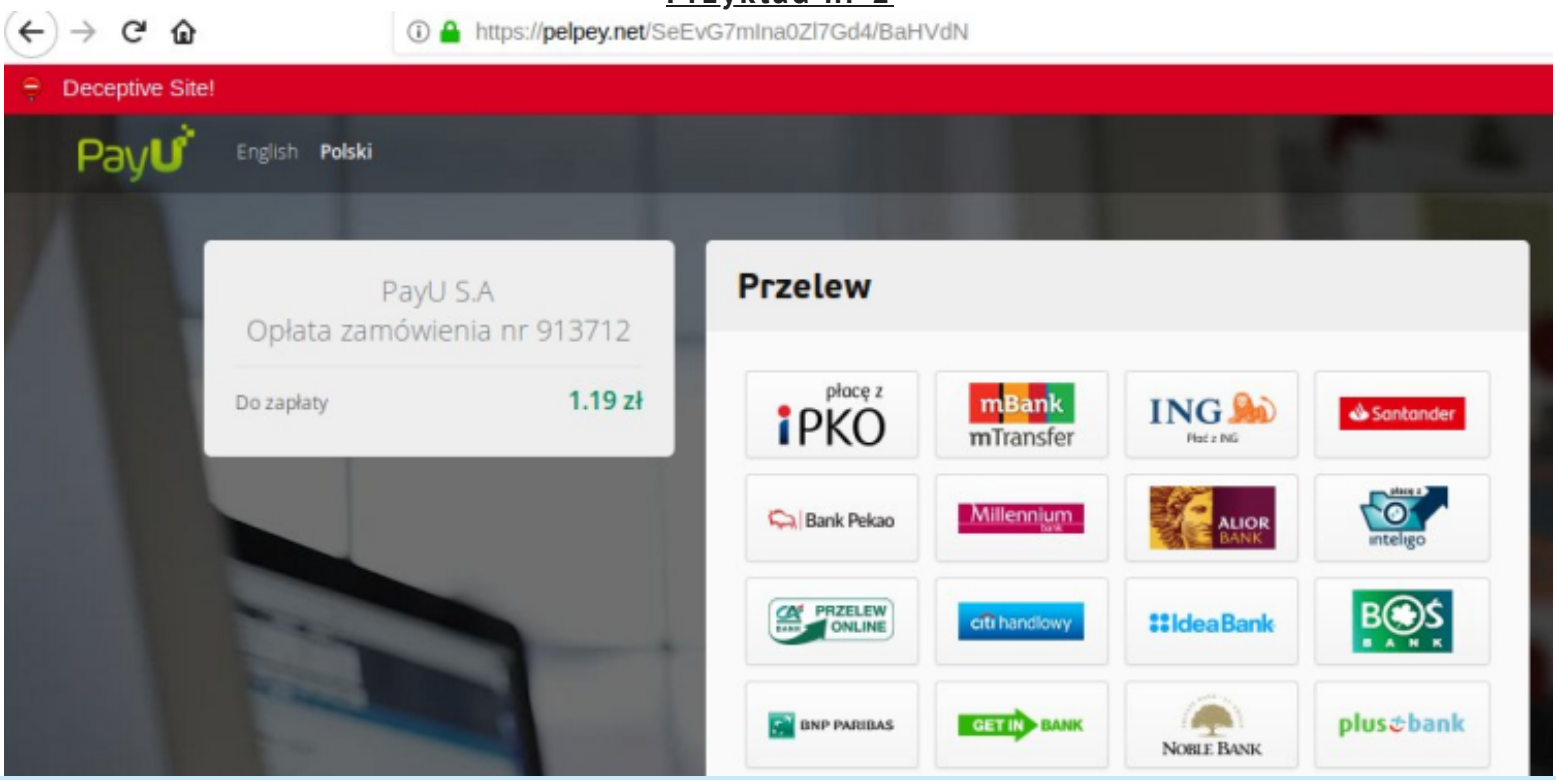
1. Abyś widział/widziała kiedyś takie fałszywe adresy internetowe?
2. Abyś próbował/próbowała zalogować się na takich fałszywych stronach?



Materiały źródłowe

https://niebezpiecznik.pl/post/fanpage-gazeta-pl-przejety/
https://poland.payu.com/blog/jak-sie-bronic-przed-oszustwem-internetowym/

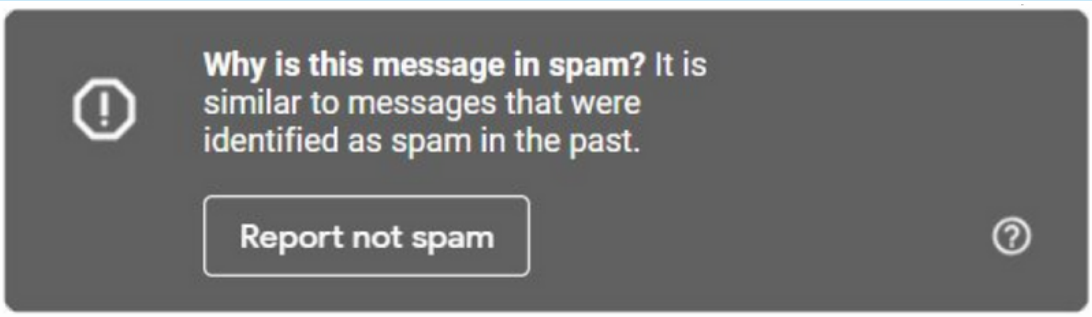
Przykład nr 2



Przykład nr 3

DYSKUSJA. Udostępnij przykład uczestnikom i rozpocznij dyskusję pytaniem: Czy pamiętasz:

1. Czy widziałeś/widziałaś takie powiadomienia na swoim koncie mailowym? Co z nimi zrobiłeś/łaś?



Przykład nr 4

DYSKUSJA. Udostępnij przykład uczestnikom i rozpocznij dyskusję pytaniem: Czy pamiętasz:

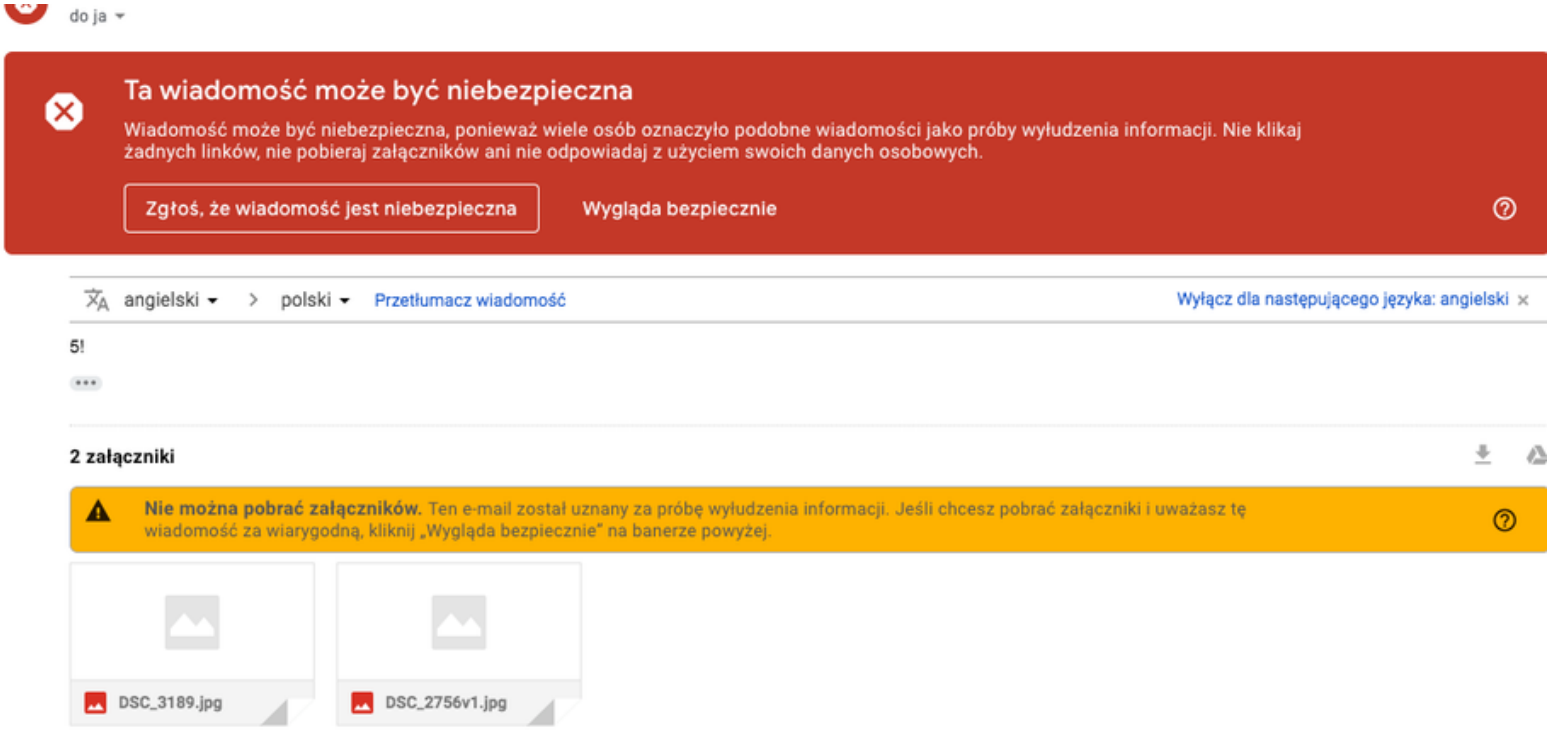
1. Abyś otrzymał/otrzymała wiadomość z nieznanego adresu? Co wtedy zrobiłeś/zrobiłaś?

Materiały źródłowe

https://biuroprasowe.orange.pl/blog/falszywe-bramki-platnosci-jak-to-dziala/
https://storage.googleapis.com/support-forums-api/attachment/thread-145329321-7389783455480387387.png

MODUŁ 3
JAK SIĘ BRONIĆ PRZED CYBER ZAGROŻENIAMI?
ĆWICZENIA I PRZYKŁADY

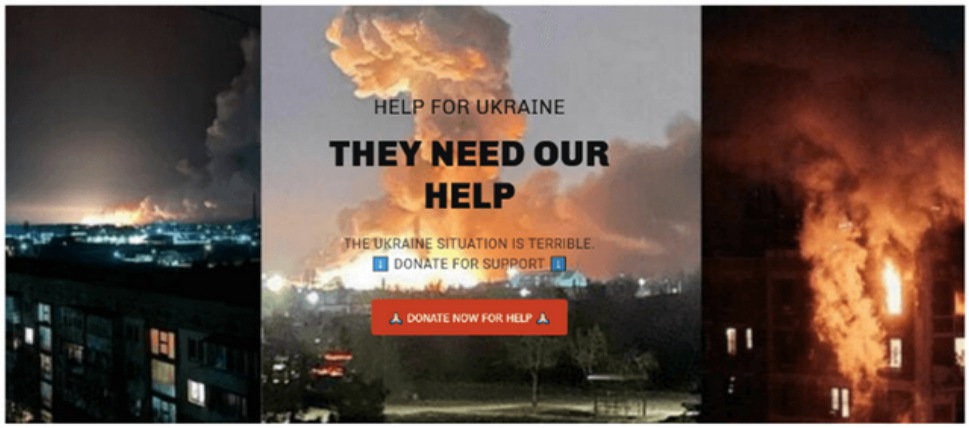
Przykład nr 4

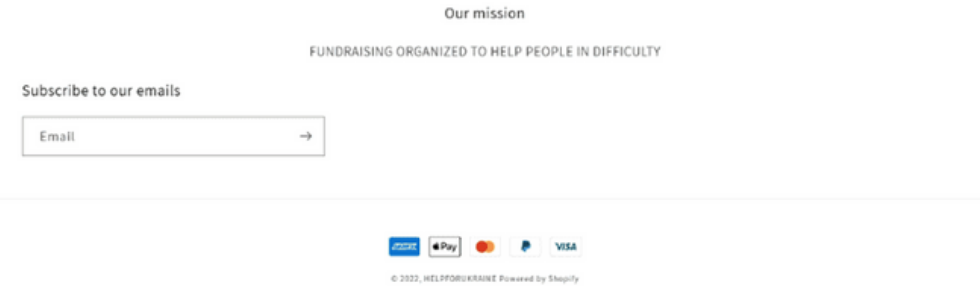


Przykład nr 5

DYSKUSJA. Udostępnij przykład uczestnikom i rozpocznij dyskusję pytaniem: Czy pamiętasz:

1. Abyś widział/widziała wiadomości/strony jak poniżej? Czy na nią odpowiedziałeś/aś? Czy sprawdziłeś/aś tą informację zanim ją udostępniłeś/aś, pokazałeś rodzinie, znajomym?





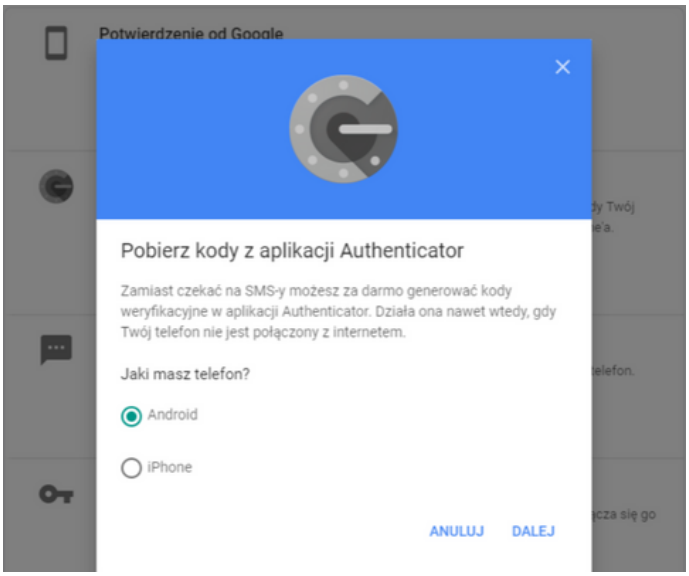
Materiały źródłowe

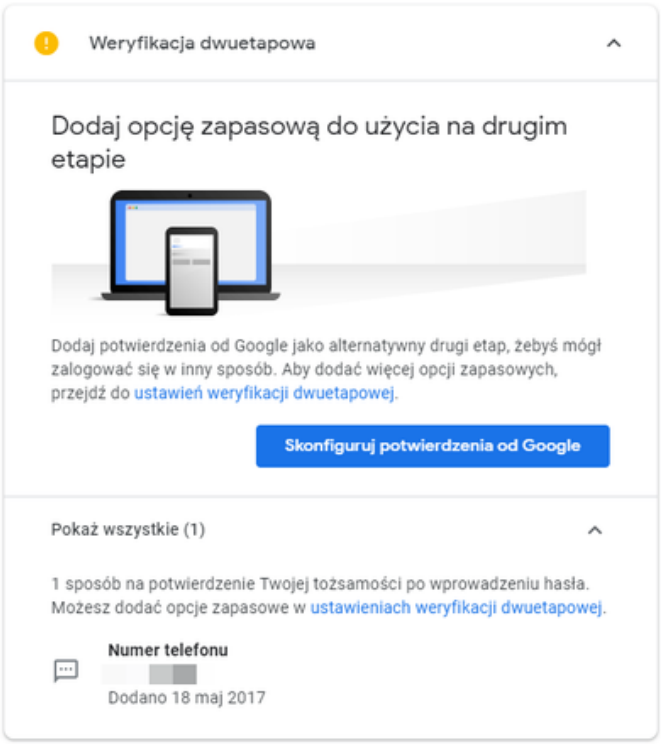
https://support.google.com/mail/thread/4799366/m%C3%B3j-e-mail-zosta%C5%82-b%C5%82%C4%99dnie-oznaczony-jako-pr%C3%B3ba-wy%C5%82udzenia-informacji-co-zrobi%C4%87?hl=pl
https://infoludek.pl/wp-content/uploads/2022/03/ESET_Oszustwa_wplaty_dla_Ukrainy_1.png

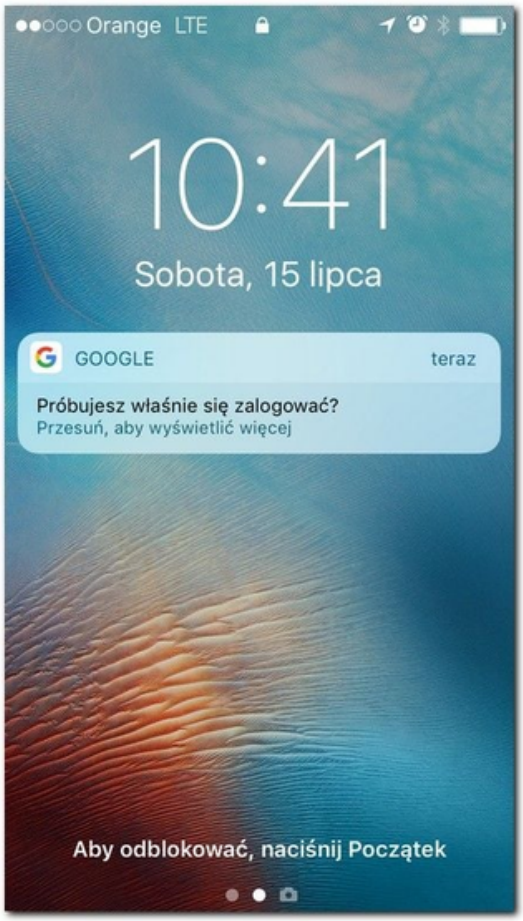
Przykład nr 6

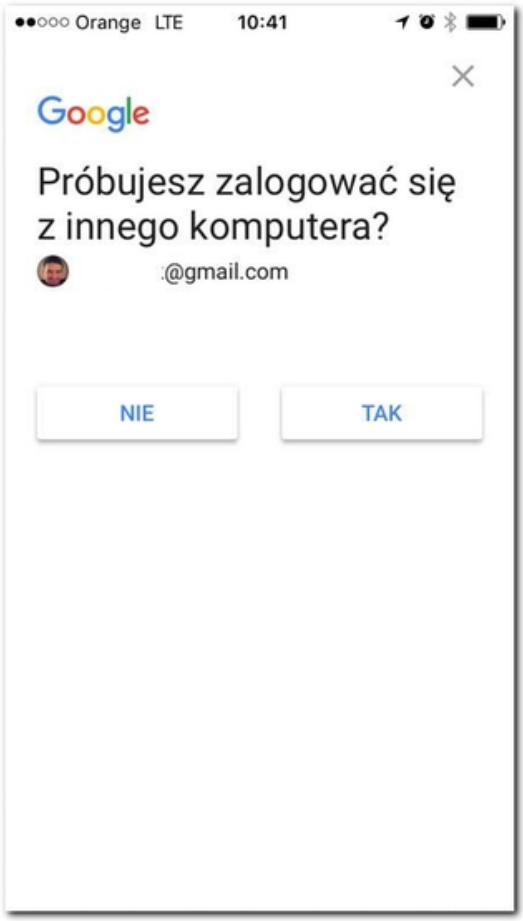
DYSKUSJA. Udostępnij przykład uczestnikom i rozpocznij dyskusję pytaniem: Czy pamiętasz:

1. Abyś miał/miała podwójną weryfikację?
2. Abyś używał/używała takiej veryfikacji na innych swoich kontach, np. bankowym?





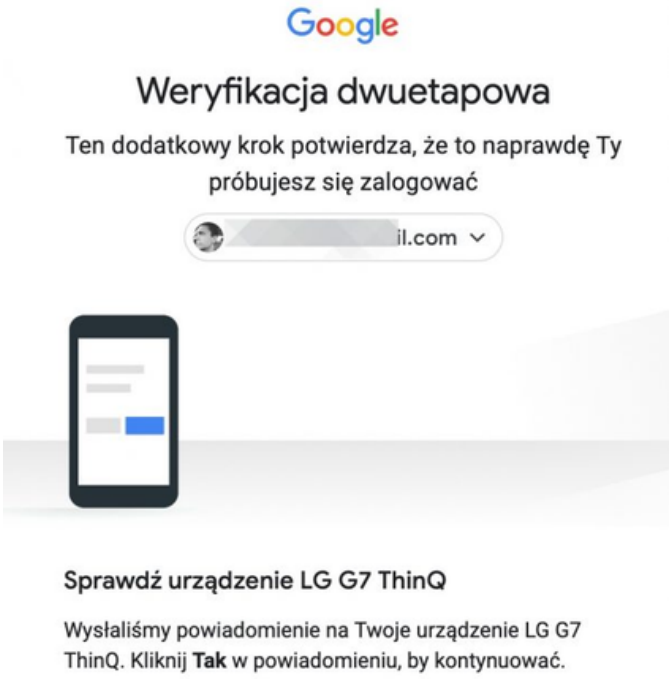


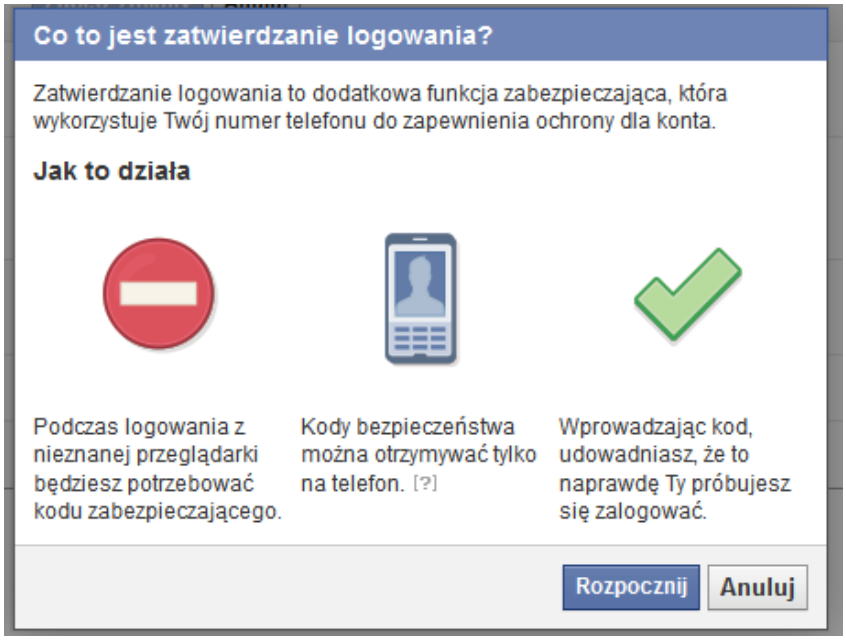


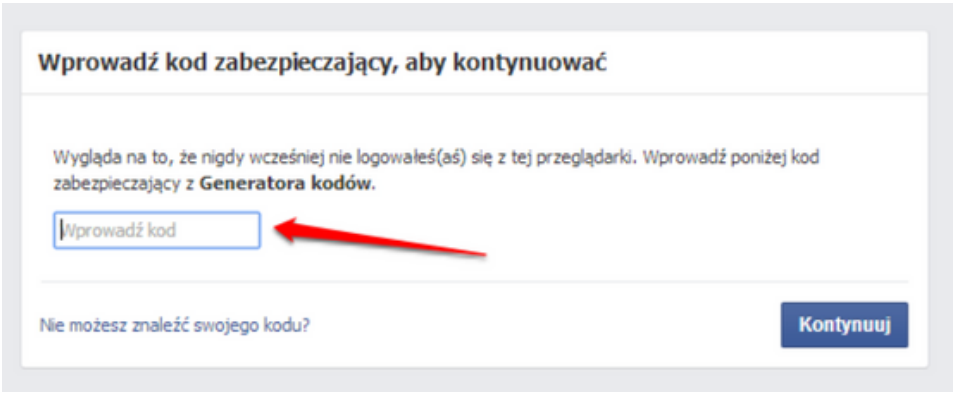
Materiały źródłowe

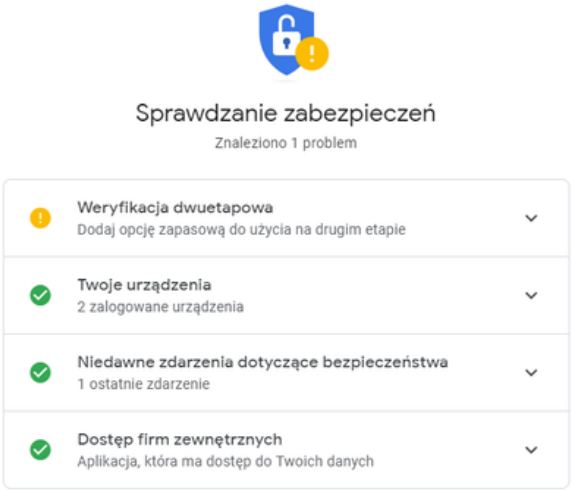
https://antyweb.pl/google-weryfikacja-dwuetapowa

Przykład nr 6









Materiały źródłowe

https://www.softonic.pl/artykuly/jak-wlaczyc-dwustopniowa-weryfikacje-na-facebooku-i-czy-warto-to-zrobic
https://www.tabletowo.pl/google-weryfikacja-dwuetapowa-domyslnie-wlaczona/

Przykład nr 1

.....
Miejscowość, data

.....
.....
.....
Imię i nazwisko konsumenta(-ów)
Adres konsumenta(-ów)

.....
.....

Nazwa i adres przedsiębiorcy

Oświadczenie
o odstąpieniu od umowy zawartej na odległość
lub poza lokalem przedsiębiorstwa

Ja/My (*).....niniejszym informuję/informujemy(*) o moim/naszym(*)
odstąpieniu od umowy sprzedaży następujących rzeczy(*) .....
umowy dostawy następujących rzeczy(*) .....
umowy o dzieło polegającej na wykonaniu następujących rzeczy/o świadczenie następującej usługi(*).....

Data zawarcia umowy[1]/odbioru[2](*).....

.....
Podpis konsumenta(-ów)

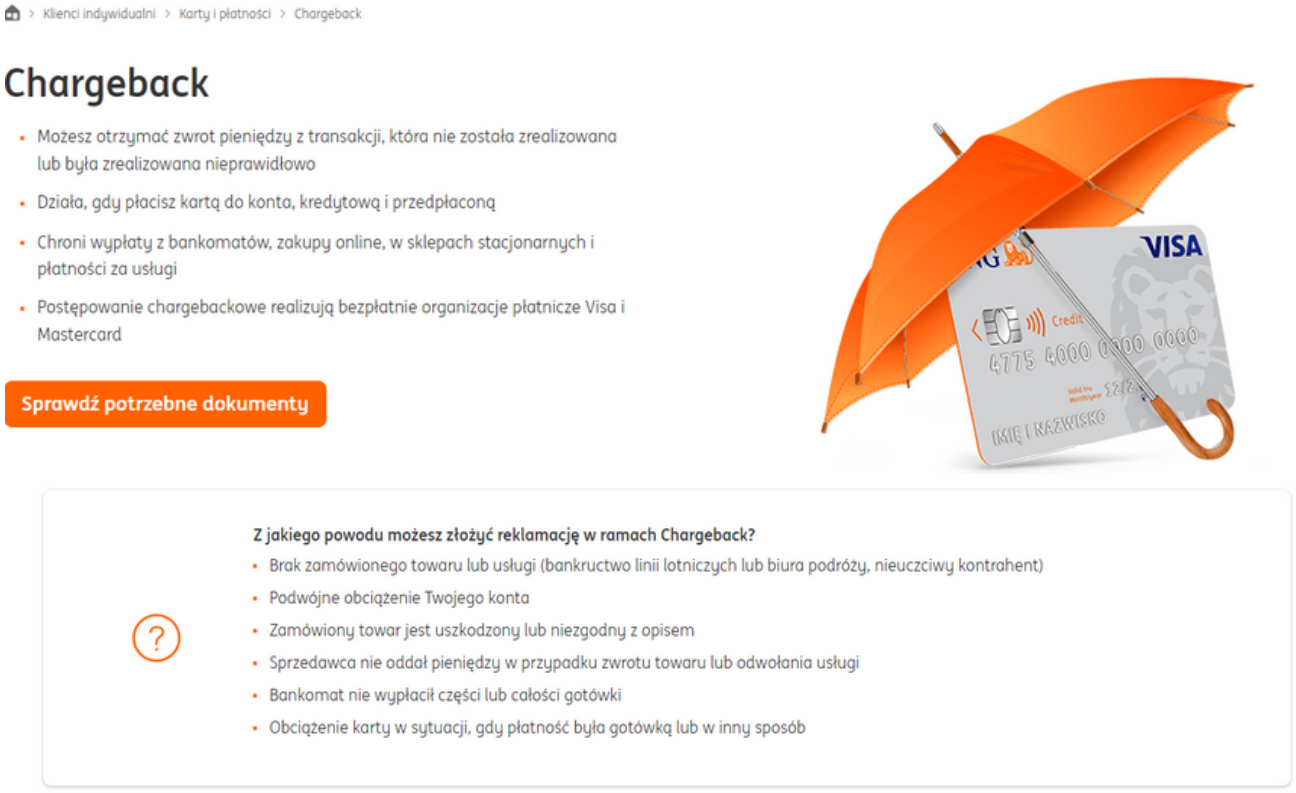
(*) Niepotrzebne skreślić
[1] podać, jeżeli umowa dotyczyła świadczenia usług
[2] podać, jeżeli umowa dotyczyła zakupu towaru

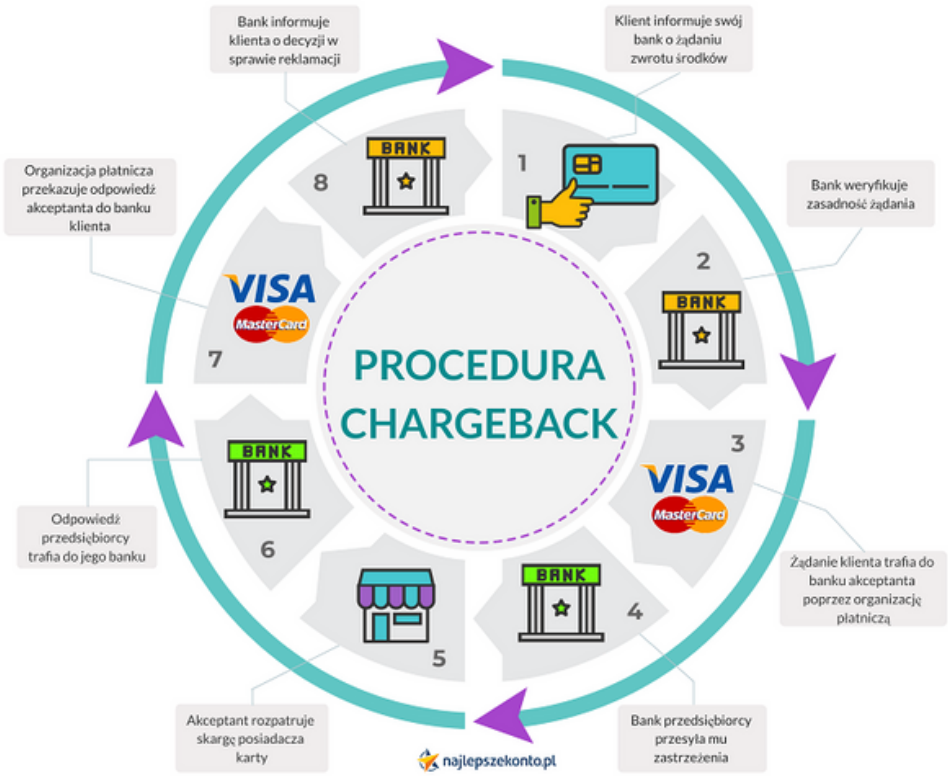
MODUŁ 4
OCHRONA DANYCH OSOBOWYCH I KONSUMENTA
PRZYKŁADY

Przykład nr 2

DYSKUSJA: Udostępnij przykład procedury chargeback, w jednym z banków, uczestnikom kursu i rozpocznij dyskusję pytaniami:

1. Czy coś cię zaskoczyło?
2. Czy wiedziałeś/łaś o procedurze chargeback?
3. Z jakiego powodu można rozpocząć procedurę chargeback?





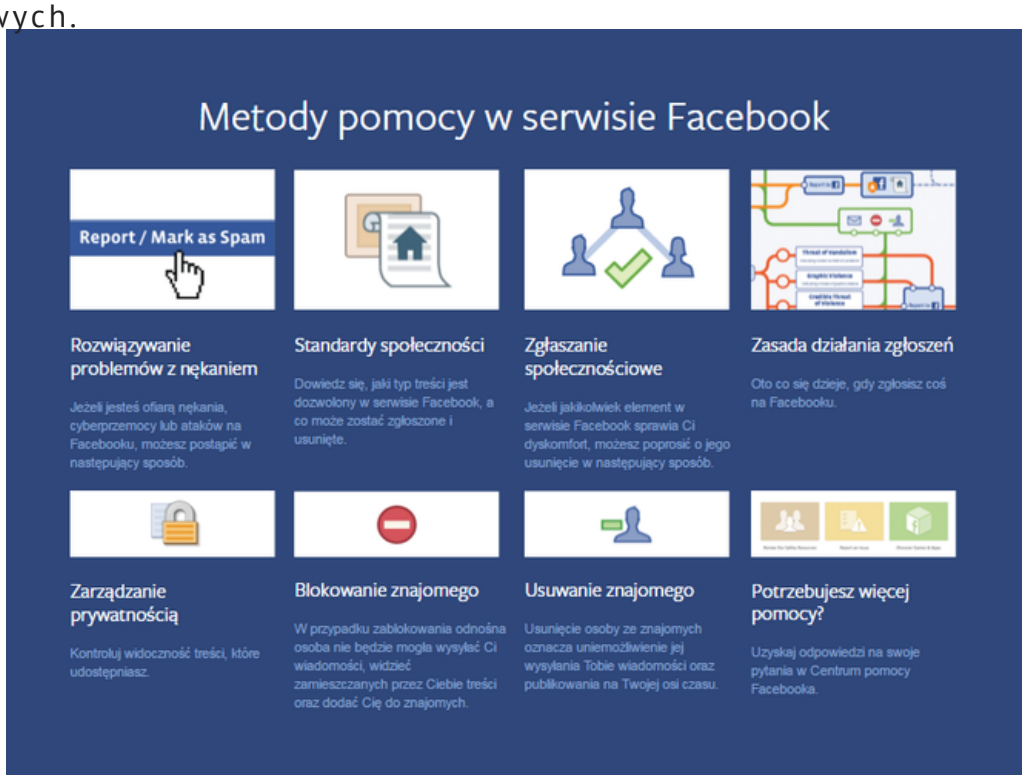
Materiały źródłowe

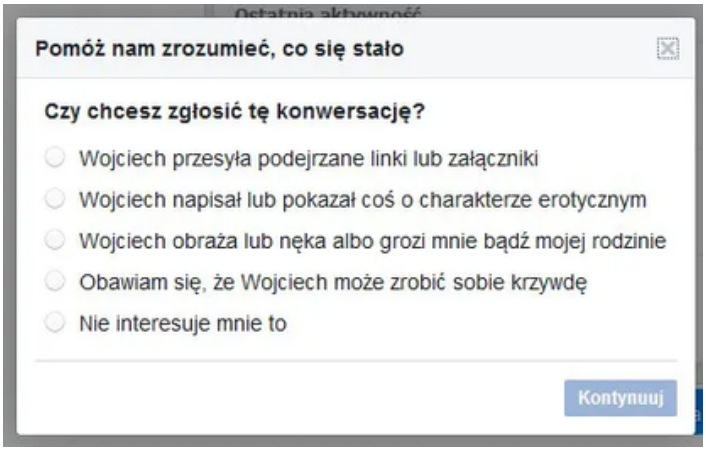
https://www.ing.pl/indywidualni/karty/chargeback
https://www.najlepszekonto.pl/procedura-chargeback-obciazenie-zwrotne-co-to-jest

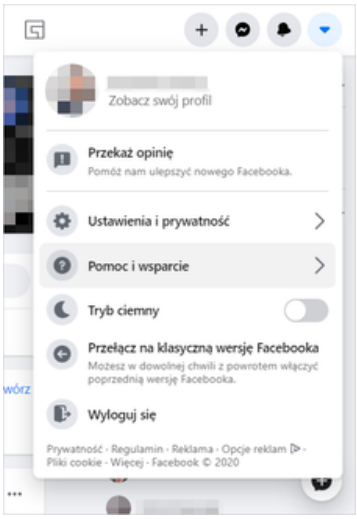
MODUŁ 5
JAK SPRAWIĆ, ABY NASZE OTOCZENIE BYŁO BEZPIECZNIEJSZE?
PRZYKŁADY

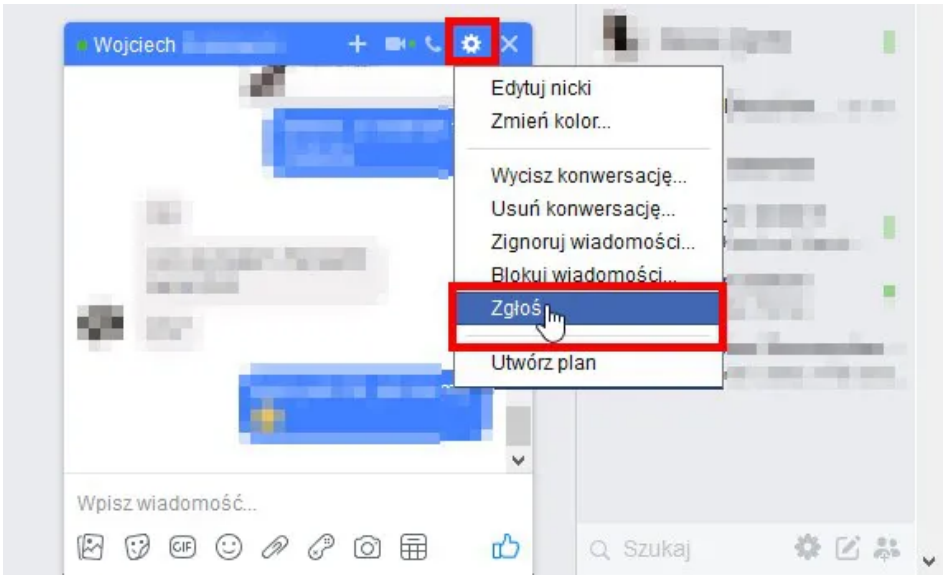
Przykład nr 1

PRACA SAMODZIELNA: Udostępnij uczestnikom kursu przykład jak wygląda możliwość zgłoszenia szkodliwych treści na jednym z najbardziej znanych portali społecznościowych.









Materiały źródłowe

https://www.ing.pl/indywidualni/karty/chargeback
https://www.najlepszekonto.pl/procedura-chargeback-obciazenie-zwrotne-co-to-jest
https://uniwersytet.shoper.pl/social-media/jak-skontaktowac-sie-z-facebookiem/

MODUŁ 6
METODOLOGIA
ĆWICZENIA

Ćwiczenie nr 1

PRACA SAMODZIELNA/ DYSKUSJA: Udostępnij uczestnikom kursu poniższe ćwiczenia: "Połącz w pary stwierdzenia, tak by stanowiły prawdziwe wyrażenia". Po zakończeniu samodzielnej pracy - zaproponuj uczestnikom wspólne omówienie rezultatów.

Cyberoszuści często wykorzystują	... powinnam/powinienem od razu usuwać podejrzane e-maile
Aby uniknąć złośliwych oprogramowań	... pochodzić z legalnego źródła i być sprawdzony
Program antywirusowy, który wybrałem/am powinien ...	... oszustwa dotyczące fałszywych wygranych
Zapisywanie danych do logowania w przeglądarce, ...	... powinniśmy być krytyczni i nieufni co do tego co widzimy na ekranach
Aby uniknąć niewłaściwych treści w Internecie...	... nie jest zalecane

MODUŁ 6
METODOLOGIA
ĆWICZENIA

Ćwiczenie nr 3

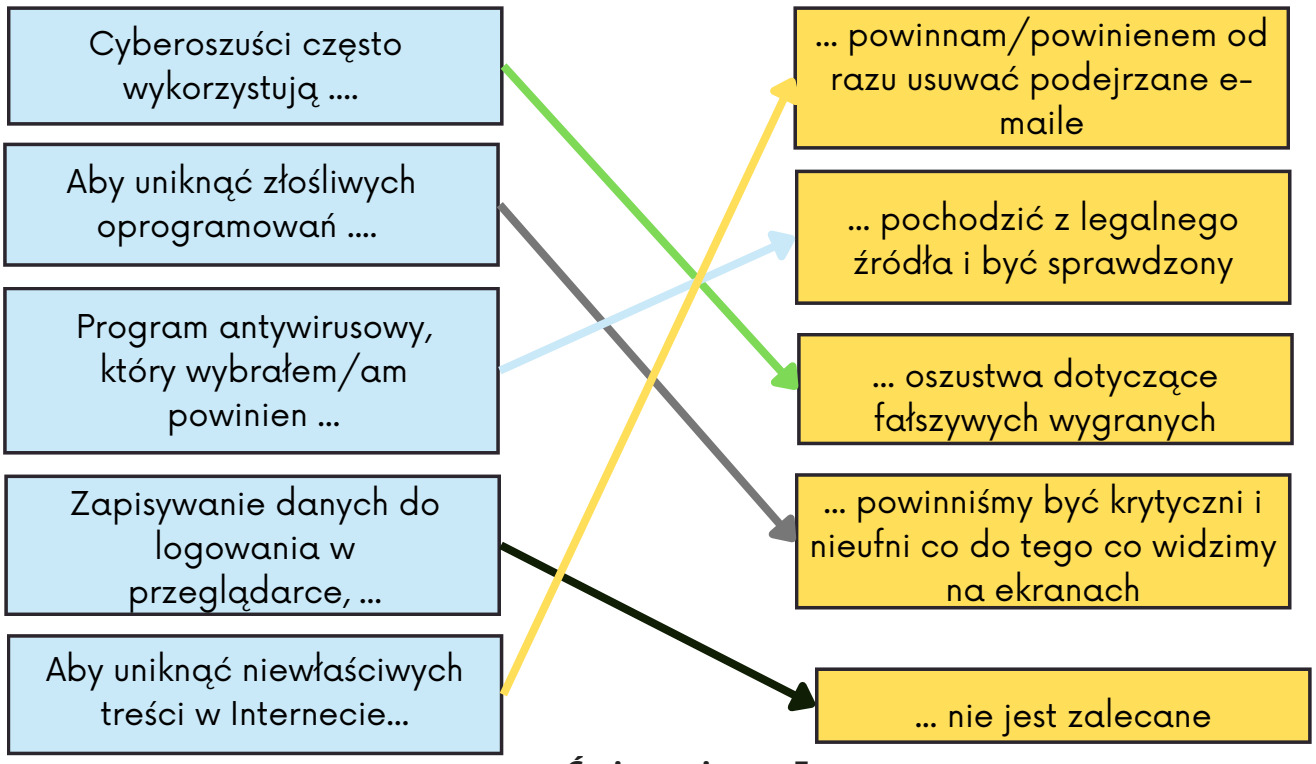
PRACA SAMODZIELNA/DYSKUSJA: Udostępnij poniższe ćwiczenie uczestnikom kursu wraz z poleceniem: "Zaznacz w odpowiednim okienku, które stwierdzenia wydają się być prawdziwe, a które fałszywe". Po wykonaniu ćwiczenia zaproponuj wspólne omówienie wyników ćwiczenia.

PRAWDA		FAŁSZ
☐	1.Podczas tworzenia hasła pamiętaj o uwzględnieniu symboli i cyfr, aby utrudnić jego złamanie.	☐
☐	2. Podczas pobierania programów z Internetu należy zawsze przeskanować komputer programem antywirusowym w celu wykrycia wirusów.	☐
☐	3. Zezwalaj przeglądarkom internetowym na zapamiętywanie nazwy użytkownika i hasła.	☐
☐	4. Przesyłaj dane osobowe w Internecie.	☐
☐	5. Podaj swoje hasło wszystkim i nigdy nie używaj tego samego hasła przez cały czas.	☐
☐	6. Otwieraj i pobieraj załączniki z nieznanego źródła, ponieważ mogą one zawierać ciekawe informacje.	☐
☐	7. Wypełniaj wszelkie ankiety internetowe, które proszą o podanie danych osobowych lub danych bankowych.	☐
☐	8. Twoje hasło może być takie samo jak nazwa użytkownika.	☐
☐	9. Korzystaj z oprogramowania antywirusowego i regularnie je aktualizuj.	☐
☐	10. Rejestruj wszystkie transakcje dokonywane online i regularnie sprawdzaj swoje konto bankowe.	☐

MODUŁ 6.
METODOLOGIA
ĆWICZENIA- KLUCZ ODPOWIEDZI

Ćwiczenie nr 1

Połącz wyrażenia, aby utworzyły poprawne stwierdzenia:



Ćwiczenie nr 3

Zaznacz w odpowiednim okienku, które stwierdzenia wydają się być prawdziwe, a które fałszywe

PRAWDA		FAŁSZ
☑	1.Podczas tworzenia hasła pamiętaj o uwzględnieniu symboli i cyfr, aby utrudnić jego złamanie.	☐
☑	2. Podczas pobierania programów z Internetu należy zawsze przeskanować komputer programem antywirusowym w celu wykrycia wirusów.	☐
☐	3. Zezwalaj przeglądarkom internetowym na zapamiętywanie nazwy użytkownika i hasła.	☑
☐	4. Prześlij dane osobowe w Internecie.	☑
☐	5. Podaj swoje hasło wszystkim i nigdy nie używaj tego samego hasła przez cały czas.	☑
☐	6. Otwieraj i pobieraj załączniki z nieznanego źródła, ponieważ mogą one zawierać wirusy.	☑
☐	7. Wypełniaj wszelkie ankiety internetowe, które proszą o podanie danych osobowych lub danych bankowych.	☑
☐	8. Twoje hasło może być takie samo jak nazwa użytkownika.	☑
☑	9. Korzystaj z oprogramowania antywirusowego i regularnie je aktualizuj.	☐
☑	10. Rejestruj wszystkie transakcje dokonywane online i regularnie sprawdzaj swoje konto bankowe.	☐

Kurs Seniorzy dla Seniorów

Dofinansowane przez
Unię Europejską

Kontakt:

www.goluchowski.edu.pl - Zakładka "Akademia"

seniorzy_edukatorzy@goluchowski.edu.pl

Akademia Nauk Stosowanych im. J. Gołuchowskiego, Rektorat
ul. Akademicka 12, Ostrowiec Świętokrzyski 27-400
z dopiskiem "Projekt Seniorzy dla Seniorów"