e-mocni:

DBAM O SWOJE BEZPIECZEŃSTWO W INTERNECIE - UNIKAM ZAGROŻEŃ

Poziom podstawowy

Relacje z bliskimi. Scenariusz nr 14a


e-Mocni
CYFROWE UMIEJĘTNOŚCI,
REALNE KORZYŚCI

E-MOCNI:
CYFROWE UMIEJĘTNOŚCI,
REALNE KORZYŚCI

Fundusze Europejskie Polska Cyfrowa

e-Mocni

Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Fundacja Aktywizacja

FRSI FUNDACJA ROZWOJU SPOŁECZEŃSTWA INFORMACYJNEGO

PARTNERZY

FiRR FUNDACJA INSTYTUT ROZWOJU REGIONALNEGO

Polski Związek Głuchych PZG Oddział Łódzki

PROGRAM SZKOLENIA

1. Zagrożenia w internecie

2. Dekalog bezpiecznego internetu

3. Oszustwa w serwisach aukcyjnych i wiadomości nieznanego pochodzenia

4. Wirusy na Facebooku i w Messengerze

CELE SZKOLENIA

Uczestnik/ uczestniczka dowie się:

- jakie zagrożenia czyhają na nich w internecie,
- czym charakteryzują się oszustwa internetowe,
- czym są wirusy na Facebooku i w Messengerze
- jak pozbyć się niechcianych reklam i wiadomości
- w jaki sposób dostosować przeglądarkę do filtrowania niechcianych treści.

SZCZEGÓŁOWE CELE DYDAKTYCZNE

W wyniku szkolenia uczestnik/uczestniczka:

Wiedza

- będzie wiedział/wiedziała, jakie są zagrożenia w internecie
- będzie znał/znała możliwości radzenia sobie z tymi zagrożeniami
- będzie wiedział/wiedziała, jak oddzielać informacje chciane od niechcianych

SZCZEGÓŁOWE CELE DYDAKTYCZNE

W wyniku szkolenia uczestnik/ uczestniczka:

Umiejętności

- będzie potrafił/potrafiła zidentyfikować wirusy na Facebooku i w Messengerze
- będzie potrafił/potrafiła rozpoznać próbę oszustwa w wiadomości e-mail lub na portalu aukcyjnym
- będzie potrafił/potrafiła ustawić od kogo, chce otrzymywać wiadomości na Facebooku i w Messengerze
- będzie potrafił/potrafiła zainstalować nakładkę blokującą niechciane treści w przeglądarce

SZCZEGÓŁOWE CELE DYDAKTYCZNE

Postawa

Uczestnik / uczestniczka:

- będzie miał/miała większą świadomość zagrożeń dla siebie i swojego dziecka, na jakie może natrafić w internecie
- będzie zdawał/zdawała sobie sprawę, w jaki sposób radzić sobie z tymi zagrożeniami
- będzie miał/miała większą gotowość do używania dodatkowych narzędzi instalowanych w przeglądarce.

POZNAJMY SIĘ

CZĘŚĆ 1

ZAGROŻENIA W INTERNECIE

Pytanie

- Jakie znacie zagrożenia w internecie, które dotyczą Was lub Waszych dzieci?

Odpowiedź

- Zagrożenia w internecie to obecnie jedne z najbardziej popularnych zagrożeń, czyhających na człowieka, które najczęściej nam zagrażają.

- Szacuje się, że ludzie wytworzyli w ciągu ostatnich kilku lat więcej informacji, niż przez wszystkie poprzednie lata istnienia naszej cywilizacji, a spora część tych informacji znajduje się właśnie w sieci.

Trojany i wirusy

- To jeden z największych problemów w sieci. Możesz zainfekować nimi komputer nawet przez przypadek – otwierając wiadomości e-mail nieznanego pochodzenia lub odwiedzając zainfekowane strony.

Ataki hakerskie

- Oglądając różne filmy z gwiazdorską obsadą, możesz sądzić, że hakerów nie zajmuje "przeciętny Kowalski". To błąd. W obecnych czasach dane są warte bardzo dużo (są niezwykle cenne!) i to właśnie loginy, hasła, dane osobowe chcą zdobyć cyberprzestępcy.

Phishing

- To wyłudzanie danych. Phisher (osoba odpowiedzialna za oszustwo) przeważnie wysyła wiadomości e-mail, podobne do tych, które wysyłają banki, serwisy aukcyjne lub inne instytucje, często państwowe. Odpowiednio spreparowane wiadomości mają na celu wyłudzenia danych do logowania, czy numerów kart bankowych i kredytowych.

Pharming

- Jest to najbardziej niebezpieczny rodzaj phishingu, polegający na tym, że wpisując albo prawidłowy adres e-mail lub adres zawierający literówkę zostajemy przekierowani na stronę wyglądająco tak samo, jak strona np. naszego banku internetowego; podając później na nich swoje dane przekazujemy je przestępcom.

Czynnik ludzki

- Sami również często udostępniamy nasze dane, które mogą posłużyć nieuczciwym osobom. Musimy uważać na to, co publikujemy i komu przesyłamy zdjęcia, które zawierają nasze dane osobowe, numery kart kredytowych, numery konta, loginy, czy hasła.

Ochrona dzieci i młodzieży

- Przestępcy często wykorzystują naiwność najmłodszych użytkowników internetu, dlatego konieczna jest odpowiednia kontrola i ograniczenie możliwości przeglądania a także publikowania niektórych treści.
- Szczególnie niebezpieczne dla dzieci mogą być treści takie jak pornografia, kontakty z nieznajomymi, którzy podają się za osoby w ich wieku, cyberprzemoc (obraźliwe zdjęcia, uwagi, komentarze), czy popularny wśród młodzieży seksting – wiadomości tekstowe i zdjęciowe związane z erotyką.

CZĘŚĆ 2

DEKALOG BEZPIECZNEGO INTERNETU

Pytanie

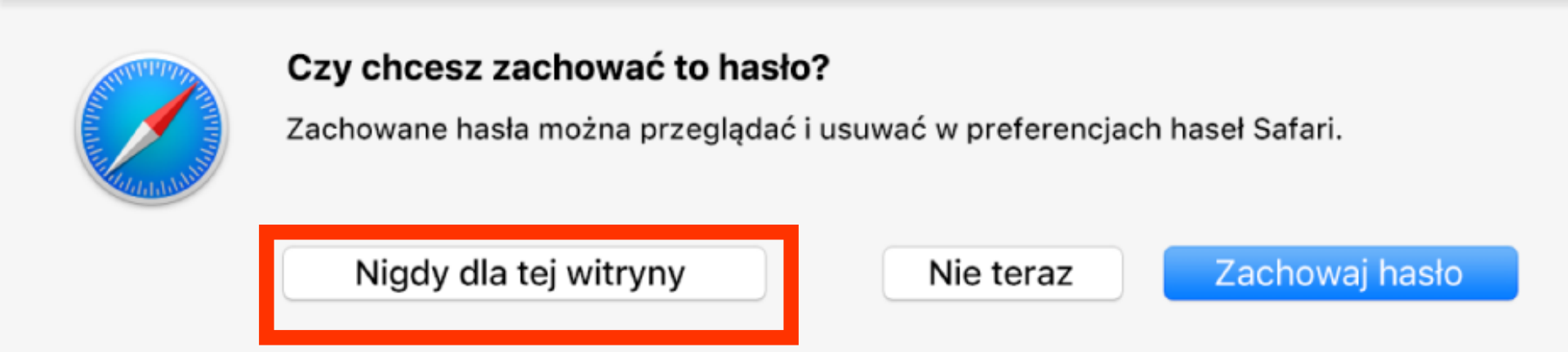
- Jakie zasady bezpiecznego korzystania znacie?

→ Postarajcie się wypisać przynajmniej 10.

10 przykazań bezpiecznego internetu

1. Szyfruj transmisję danych, a w szczególności wiadomości e-mail.
W innym przypadku zawsze będzie istniało ryzyko, że dane, które przesyłasz zostaną przechwycone i wykorzystane przez osoby postronne

10 przykazań bezpiecznego internetu



2. Nie zapisuj haseł na komputerze.
Kiedy będziesz musiał oddać komputer do naprawy, możesz przypadkiem ujawnić cenne dla Ciebie dane.

10 przykazań bezpiecznego internetu

3. Systematycznie zmieniaj hasła. Obecnie bardzo łatwo przechwycić hasło do naszej sieci bezprzewodowej, wykorzystując do tego specjalne oprogramowanie. Dlatego warto co jakiś czas zmieniać do niej hasło.

10 przykazań bezpiecznego internetu

4. Ustawiaj trudne hasła. Jeżeli jakiś serwis prosi nas o podanie daty urodzenia lub numeru telefonu warto podać fałszywe informacje. Pamiętaj, żeby podawać prawdziwe informacje w bankach czy innych instytucjach.

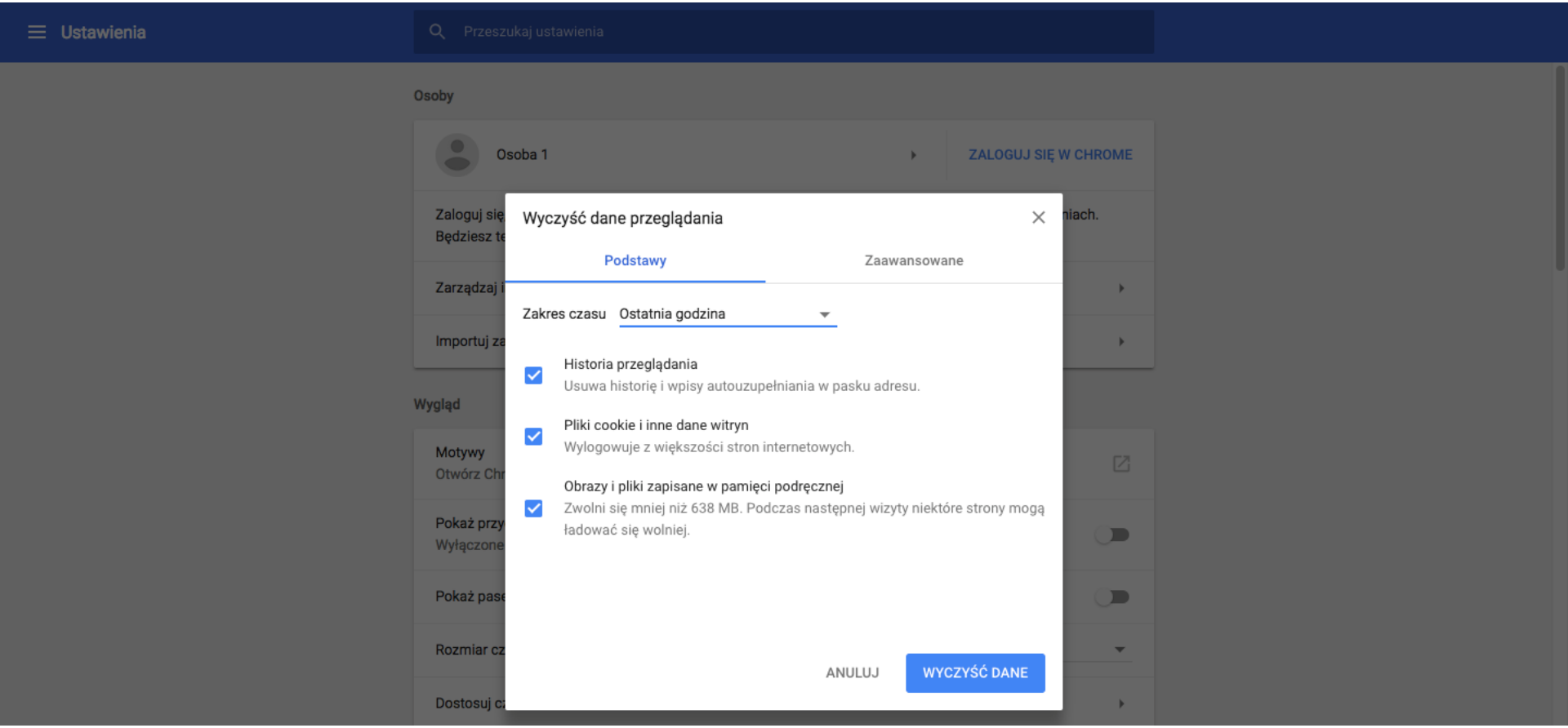
10 przykazań bezpiecznego internetu

5. Zainstaluj porządne oprogramowanie antywirusowe i firewall, np. Kasperski Lab https://www.kaspersky.pl/do-pobrania

10 przykazań bezpiecznego internetu

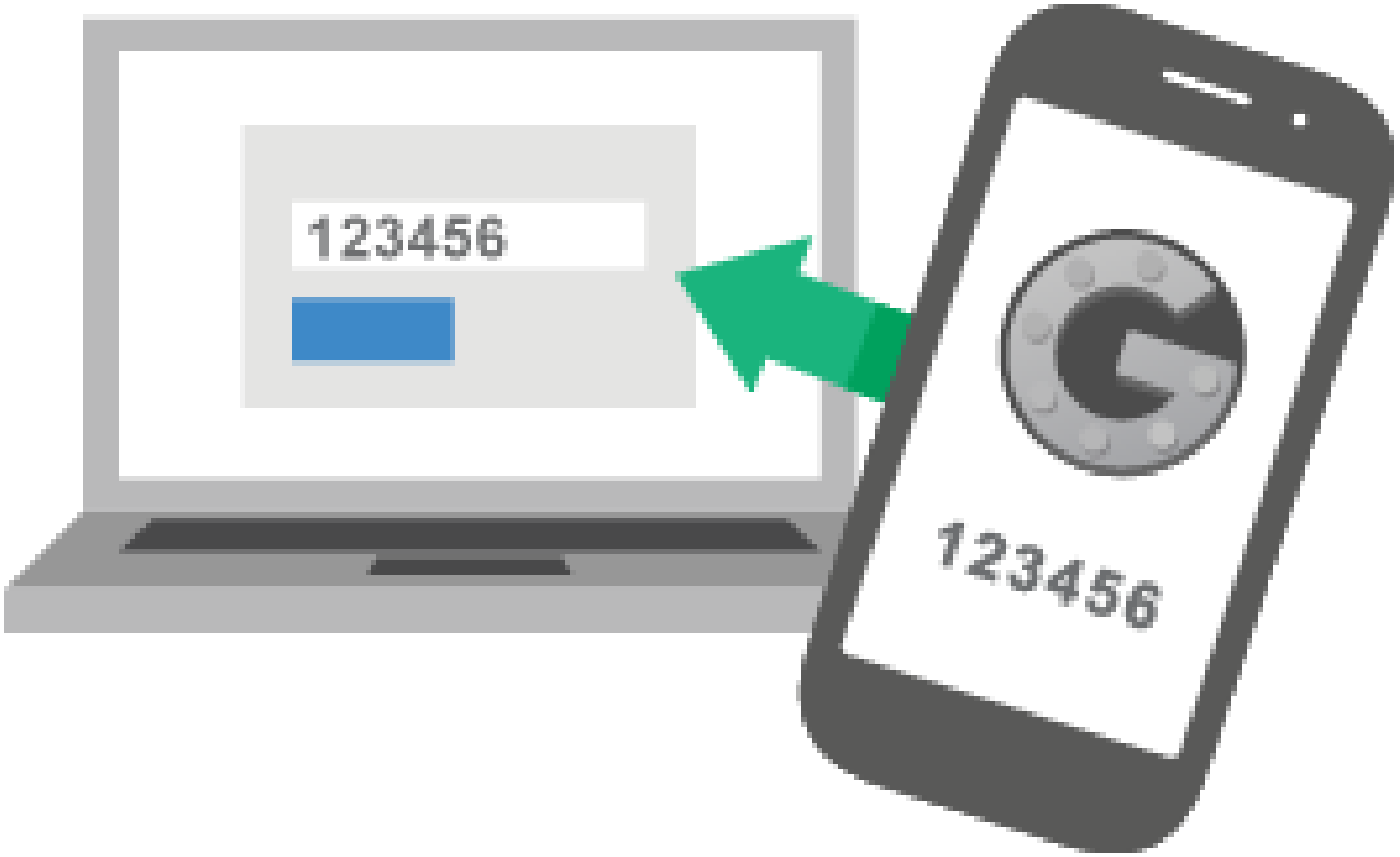
6. Pamiętaj, że bezpieczeństwo w sieci dotyczy także tabletów i smartfonów. Wyłącz Wi-Fi i Bluetooth, kiedy z nich nie korzystasz.

10 przykazań bezpiecznego internetu



7. Przeglądarki internetowe często zbierają informacje o stronach, które przeglądamy, ale też zapisują nasze loginy i hasła, dlatego warto od czasu do czasu usuwać historię przeglądania.

10 przykazań bezpiecznego internetu

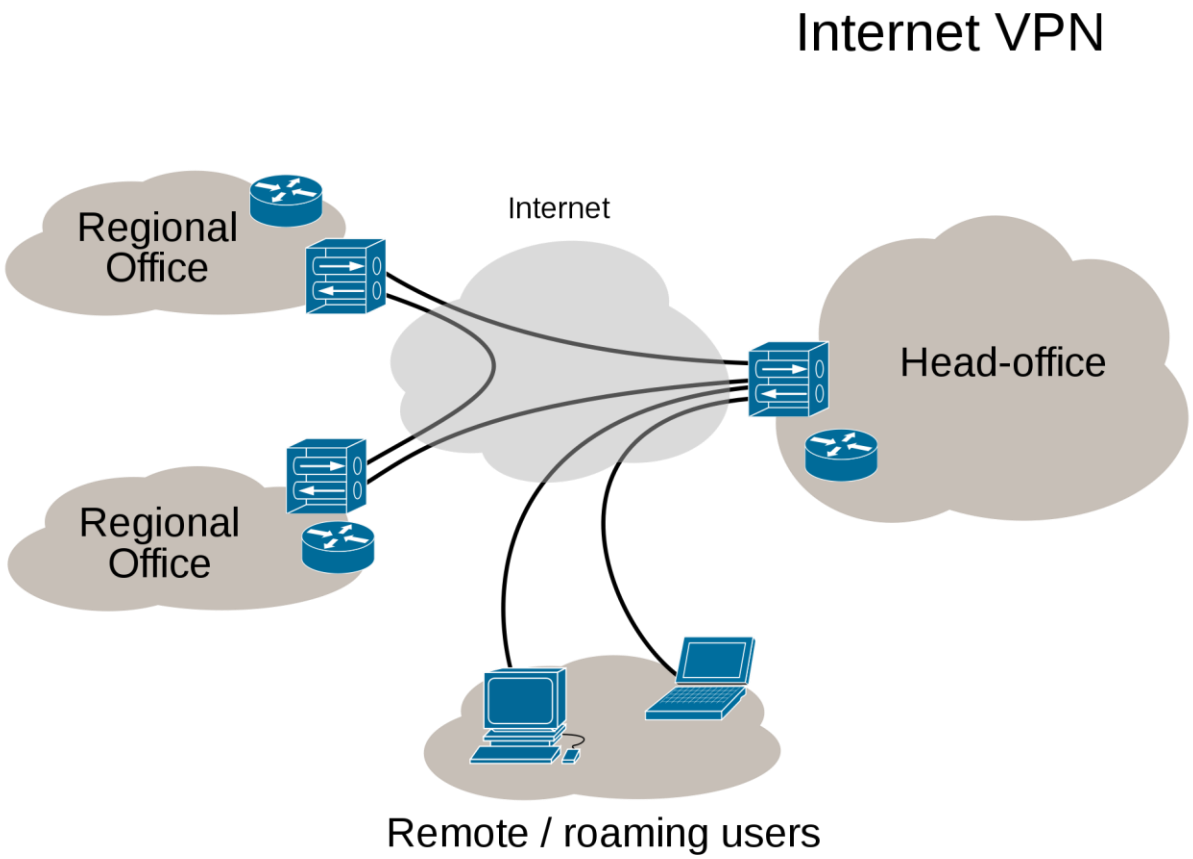


8. Weryfikacja dwuetapowa. Podwójna weryfikacja pozwoli nam zablokować dostęp do naszych serwisów nawet wtedy, kiedy ktoś pozna nasze hasło. Często wykorzystuje się do tego potwierdzenie kodem smsowym.

10 przykazań bezpiecznego internetu

9. Rób kopie zapasowe. Możesz robić je w chmurze, ale pamiętaj, że nie zawsze są one odpowiednio zabezpieczone, dlatego najlepiej trzymać kopie ważnych dokumentów i plików na osobnym dysku.

10 przykazań bezpiecznego internetu



10. VPN – wirtualna sieć prywatna. Jeżeli możesz zainwestuj w VPN. W ten sposób wszystkie Twoje dane przesyłane w tunelu są odpowiednio szyfrowane. Nawet, kiedy trafią w niepowołane ręce - nie będą mogły być w żaden sposób wykorzystane.

CZĘŚĆ 3

OSZUSTWA W SERWISACH AUKCYJNYCH I WIADOMOŚCI NIEZNANEGO POCHODZENIA

Oszustwa w serwisach aukcyjnych

- Czasami na popularnych serwisach aukcyjnych można znaleźć wymarzone oferty – nieprawdopodobne rabaty,
  a często darmowe produkty, do których wystarczy opłacić tylko przesyłkę.
- Należy uważać nie tylko na takie oferty, ale również z pewną dozą ostrożności podchodzić do każdej aukcji,
  w każdym serwisie.
- Jeśli można - bezpieczniej zamówić przesyłkę za pobraniem, niż płatną przelewem. Jest to, co prawda droższe, ale bezpieczniejsze.

OLX – Dotpay, Przelewy24.pl

a. Po złożeniu zamówienia otrzymujemy e-mail z potwierdzeniem, że kurier został zamówiony; pozostaje nam tylko kwestia dokonania odpowiedniej płatności.
b. Sprzedający przesyła nam link do dokonania przelewu w popularnych, zaufanych serwisach takich jak Dotpay, czy Przelewy24.pl.
c. Następnie zostajemy przekierowani na stronę łudząco podobną do oryginalnej, klikamy w odpowiednią ikonę naszego banku.
d. Oszustwo odbywa się w czasie rzeczywistym – to oznacza, że przestępca widzi nasze dane i tymi danymi loguje się do naszego konta w prawdziwej witrynie banku.
   Następnie definiuje przelew zaufany, a całość zostaje potwierdzona przez oszukaną osobę kodem sms, która myśli, że potwierdza smsem przelew za paczkę.

W ten sposób możemy być okradani na niskie kwoty przez długi czas.

Podszywanie się oszusta pod bank

- Oszuści często podszywają się pod godne zaufania instytucje, jakimi są banki, np. klienci PKO otrzymywali maila, w którym informowano o otrzymaniu nowej wiadomości dostępnej w serwisie internetowym banku.
- Po kliknięciu w link, przekierowywano ich na łudząco podobną stronę; należało podać numer klienta, hasło oraz jednorazowy kod dostępu. Dzięki temu oszust miał dostęp do naszego konta.

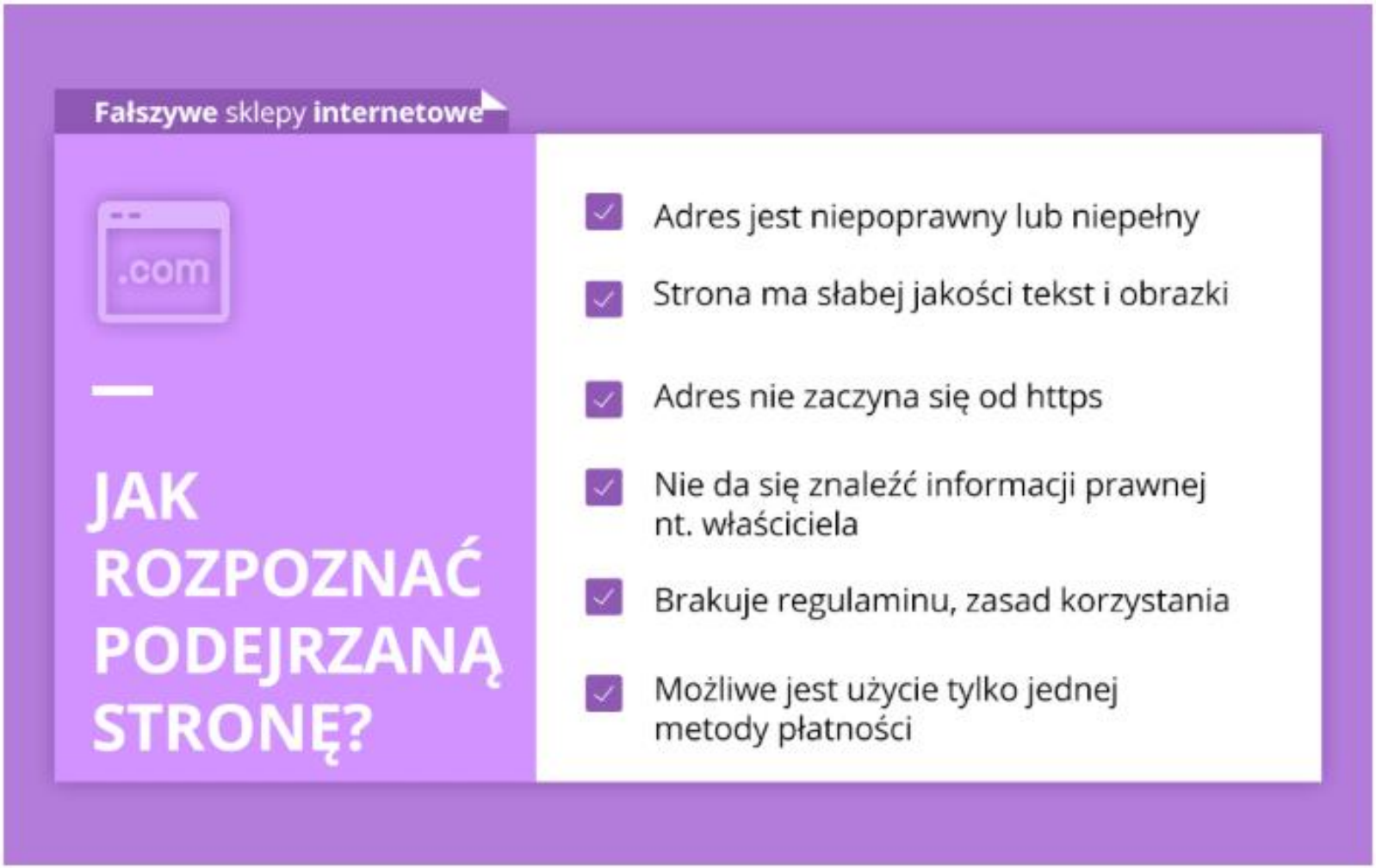
Podejrzane wiadomości - oznaki

- Adres e-mail lub numer telefonu nadawcy nie jest zgodny z nazwą firmy, za której pracownika podaje się dana osoba.
- Twój adres e-mail jest inny niż ten, który podano danej firmie.
- Wiadomość rozpoczyna się od bezosobowego zwrotu, np. „Szanowny kliencie”.
- Wiadomość różni się znacząco od innych, otrzymywanych od tej firmy.
- Wiadomość zawiera prośbę o podanie informacji osobistych, takich jak numer karty kredytowej lub hasło do konta.
- Wiadomość nie była zamawiana i zawiera załącznik.

Podejrzana strona internetowa

Spróbujcie teraz ustalić, co może zawierać podejrzana strona internetowa?

Podejrzana strona internetowa?

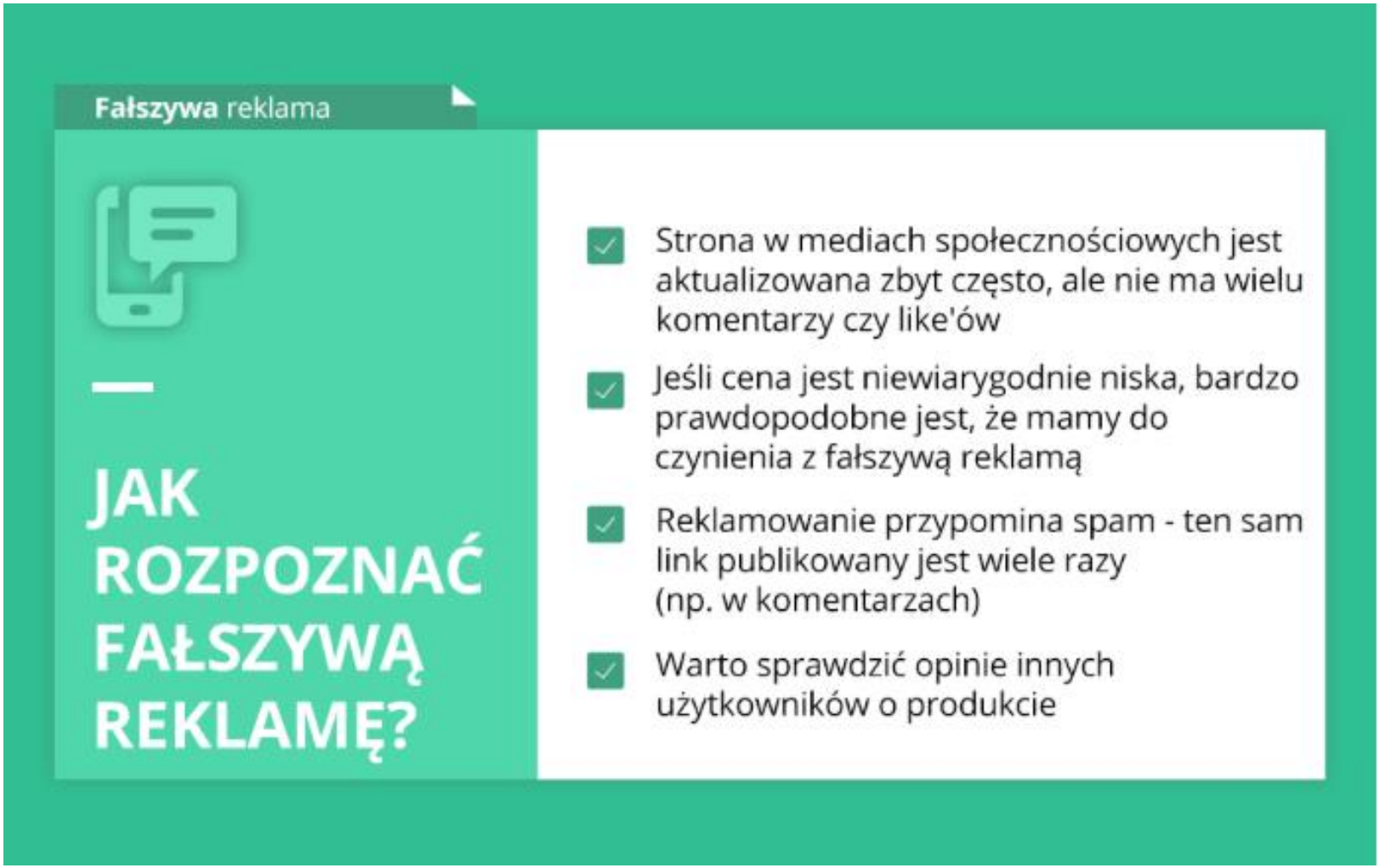


Źródło: http://krknews.pl/sa-najpopularniejsze-oszustwa-internecie-sie-nimi-chronic/

Fałszywa reklama?

Spróbujcie teraz ustalić, co może zawierać fałszywa reklama?

Fałszywa reklama

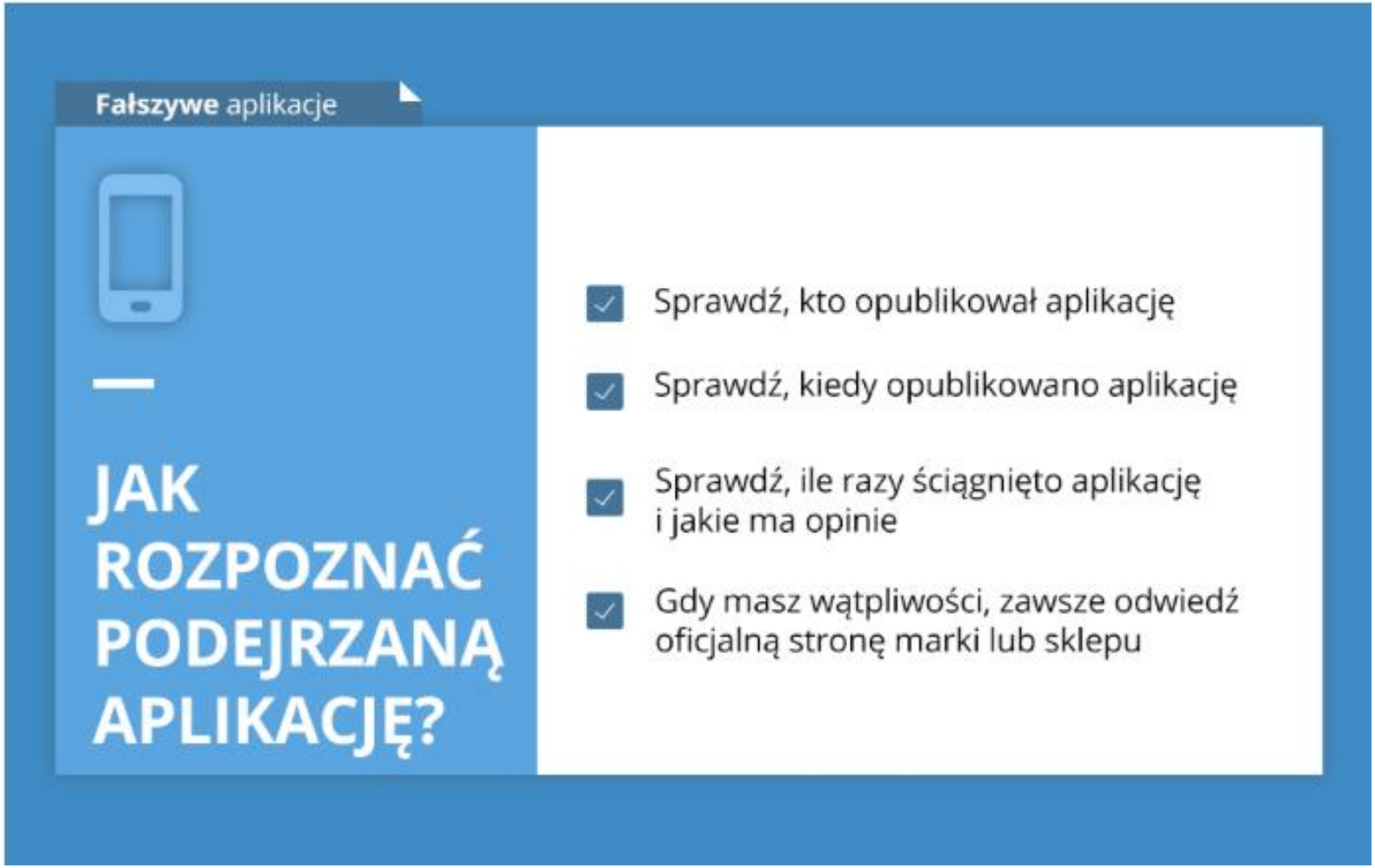


- Źródło: http://krknews.pl/sa-najpopularniejsze-oszustwa-internecie-sie-nimi-chronic/

Podejrzana aplikacja?

Spróbujcie teraz ustalić, co może zawierać podejrzana aplikacja?

Podejrzana aplikacja?



- Źródło:http://krknews.pl/sa-najpopularniejsze-oszustwa-internecie-sie-nimi-chronic/

CZĘŚĆ 4

WIRUSY NA FACEBOOKU I W MESSENGERZE

Wirusy na Facebooku (1)

- Nierozważne klikanie w linki wyświetlające się na Facebooku może w najlepszym przypadku skutkować zablokowaniem konta, a w najgorszym utratą danych osobowych.

Wirusy na Facebooku (2)

- Na Facebooku często można zobaczyć posty, typu „Nie uwierzysz, co zrobiła…”, sugerujące, że po kliknięciu w nie obejrzymy ciekawy filmik.
- Natomiast po kliknięciu często jesteśmy przekierowywani na stronę udającą serwis Youtube.com, na którym pojawia się informacja o braku możliwości obejrzenia filmu bez instalacji odpowiedniego oprogramowania.
- Po jego zainstalowaniu z naszego konta rozsyłane będą takie wiadomości do naszych znajomych, a oprogramowanie, czy rozszerzenie może zainfekować nasz komputer.

Wirusy na Facebooku (3)

- Innym sposobem są wiadomości rozsyłane przez naszych znajomych. Są to automatycznie generowane wiadomości, o których nasi znajomi często nie mają nawet pojęcia.
- Po kliknięciu w link możemy zostać przekierowani do podrobionego panelu logowania Facebooka z prośbą o ponowne logowanie – logując się przekazujemy nasze dane oszustom.
- W innym przypadku możemy być poproszeni o podanie numeru telefonu. Po otrzymaniu i wpisaniu kodu zapiszemy się do płatnej usługi SMS Premium, która może nas słono kosztować.

Jak reagować?

- Jeżeli Twój znajomy publikuje podejrzane linki lub wysyła nietypowe wiadomości powinieneś mu o tym powiedzieć.
- Powiedz mu to osobiście lub zadzwoń albo napisz sms. Wysyłając mu wiadomość przez Facebook istnieje bardzo duża szansa, że wiadomość zostanie automatycznie usunięta przez złośliwe oprogramowanie, a Twój znajomy nigdy jej nie otrzyma.

Objawy zainfekowania komputera

Jeżeli Twoje konto na Facebooku:

- publikuje spam i wysyła niepożądane wiadomości,
- w historii konta pojawiają się nietypowe miejsca logowania,
- widzisz wiadomości i posty, których nie wysyłałeś,

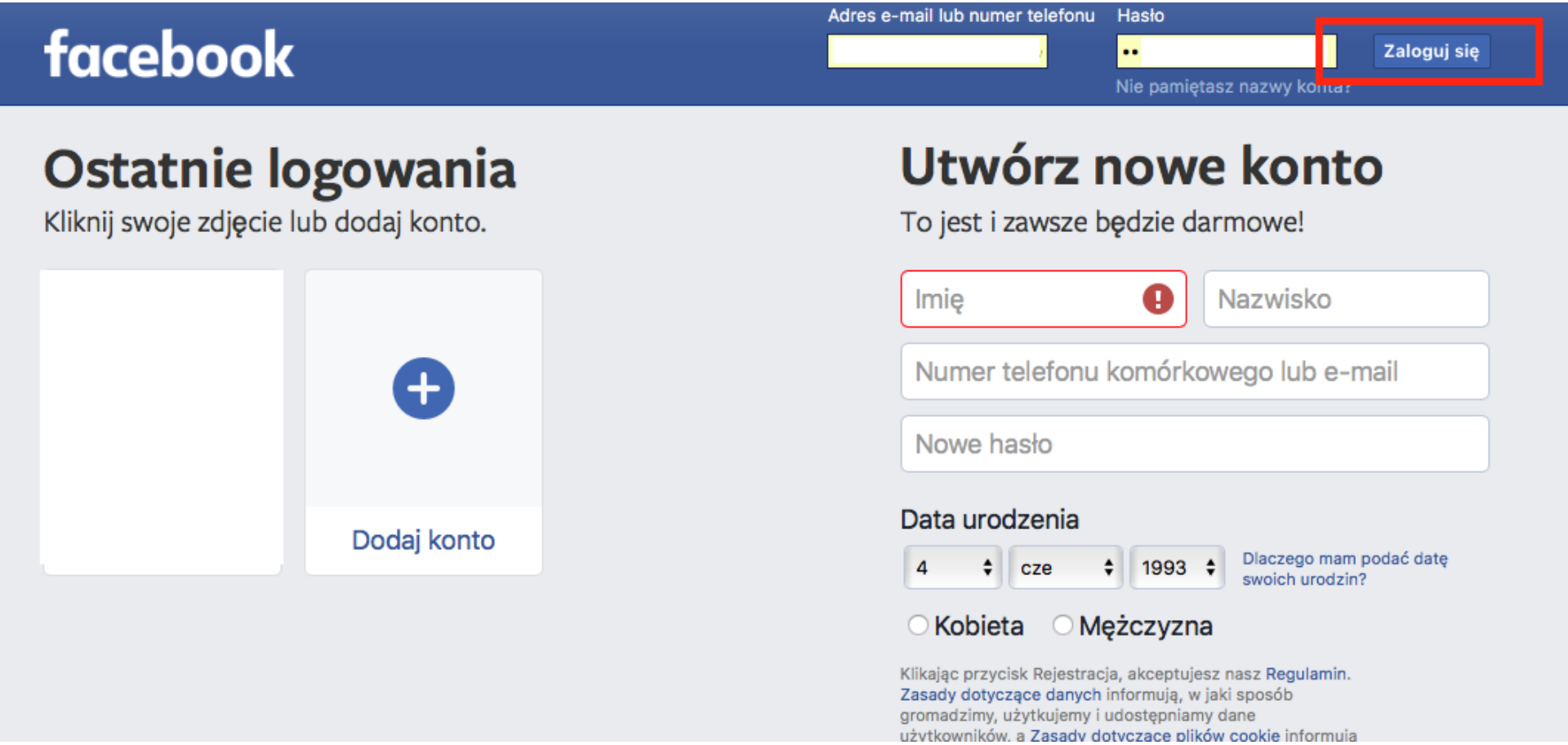
➢ Twoje konto zostało zainfekowane.

Wiadomości od nieznajomych

Czasem możesz również otrzymywać podejrzane wiadomości od nieznajomych osób.

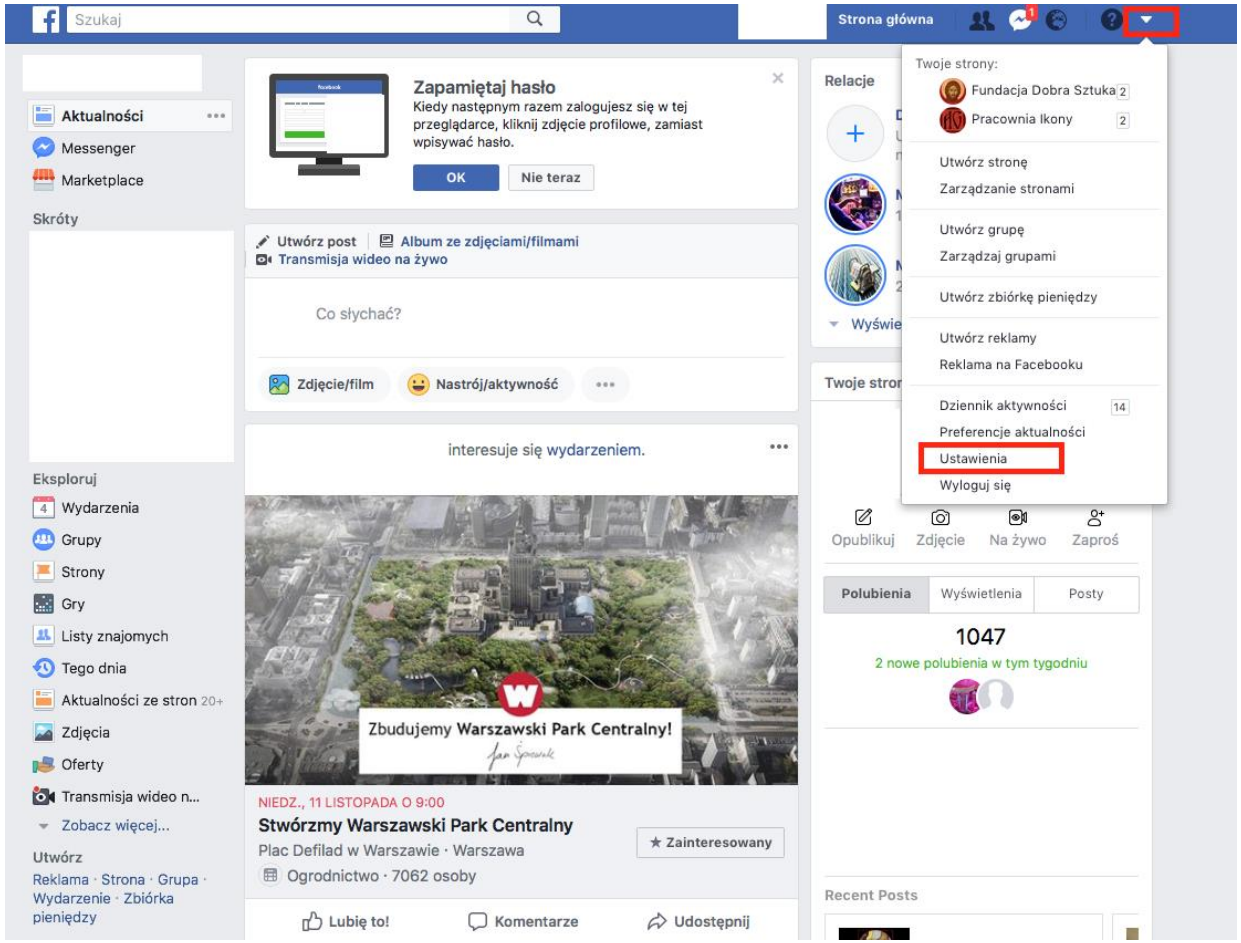
- Mogą to być zarówno wirusy, jak i wiadomości od osób, których nie znasz, albo nie chcesz ich otrzymywać.
- Możesz zmienić w ustawieniach Facebooka, kto może wysyłać do Ciebie wiadomości. W tym celu musisz zablokować osoby, od których nie chcesz otrzymywać wiadomości.

Ustawienia wiadomości Facebook (1)



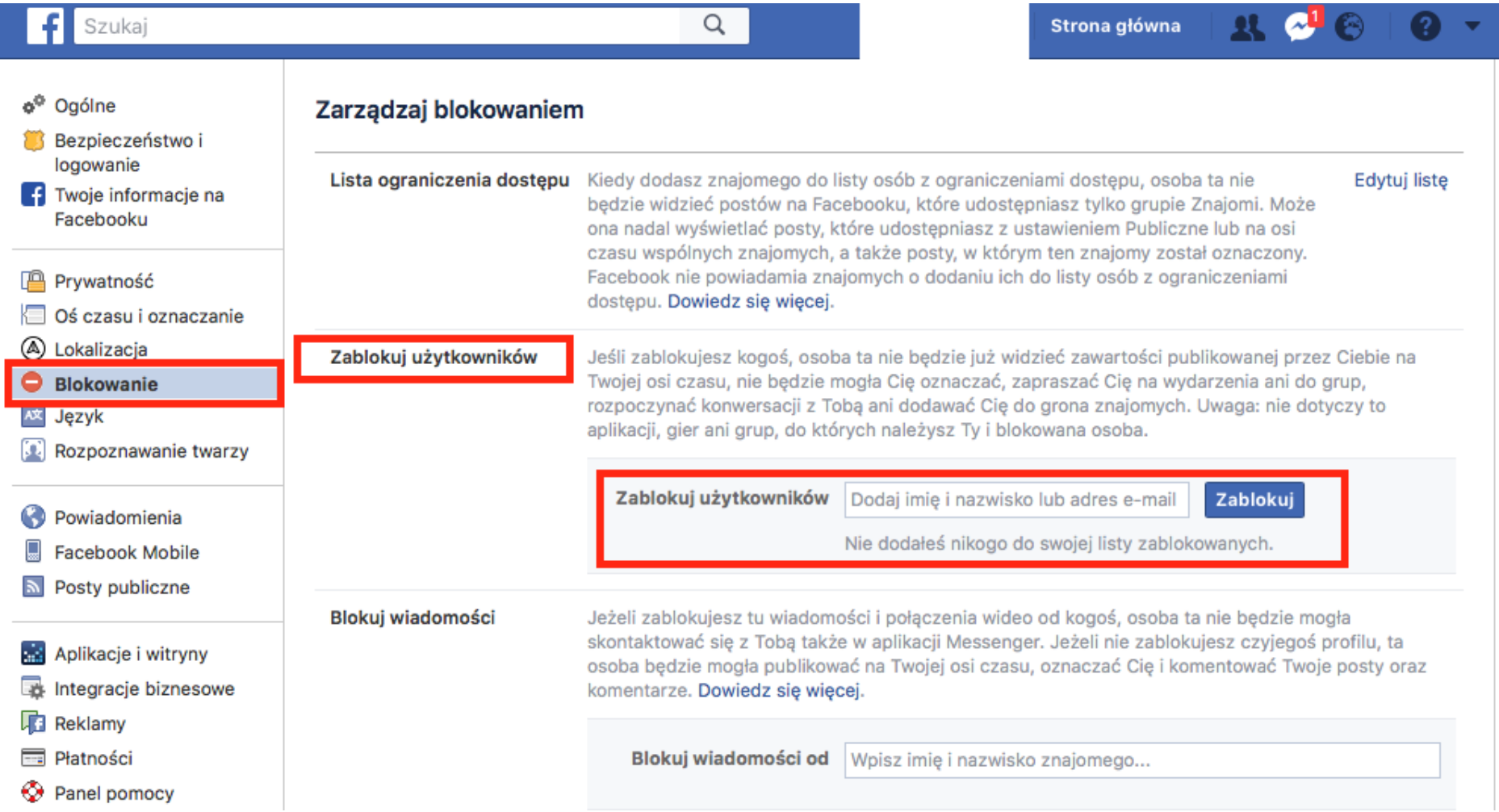
- Aby zmienić ustawienia otrzymywanych wiadomości zaloguj się na swój profil.

Ustawienia wiadomości Facebook (2)



- Kolejno wejdź w "Ustawienia".

Ustawienia wiadomości Facebook (3)



- Z menu bocznego wybierz „Blokowanie”, a w zakładce „Zablokuj użytkowników wybierz użytkowników, których chcesz zablokować.

WWW.E-MOCNI.ORG.PL