



AUTOR: **Łukasz Tomczyk**

TYTUŁ: **Czy moje pieniądze są bezpieczne w sieci?**

CZAS TRWANIA: **90 minut**

OBSZAR TEMATYCZNY: **Przestrzeganie prawa i zasad bezpieczeństwa;
Instytucje finansowe**

PRZEDMIOT: **podstawy przedsiębiorczości, informatyka,**

ETAP EDUKACYJNY: **szkoła ponadpodstawowa**

CELE ZAJĘĆ

Celami ogólnymi zajęć są:

- rozwinięcie u uczniów i uczennic kompetencji cyfrowych niezbędnych do bezpiecznego poruszania się w sieci, zwłaszcza podczas wykonywania transakcji finansowych on-line;
- zaznajomienie się z prawami klientów w razie sporu z bankiem na związanym np. z nieautoryzowanym dostępem do konta czy karty kredytowej;
- wskazanie instytucji pomagających ofiarom wybranych przestępstw o charakterze finansowym w sieci.

CELE SZCZEGÓŁOWE

Po zajęciach uczeń/uczennica:

- będzie umiał/a wskazać kompetencje oraz obszary działania Rzecznika Finansowego;
- będzie potrafił/a wskazać przestępstwa o charakterze finansowym z wykorzystaniem technologii informatyczno-komunikacyjnych (ICT) oraz podać ich przyczyny;
- będzie umiał/a wyróżnić metody kradzieży on-line oraz wskazać skuteczne sposoby ochrony przed nimi;
- będzie potrafił/a wskazać i wyjaśnić regulacje prawne dotyczące bezpieczeństwa transakcji finansowych;
- będzie potrafił/a wyjaśnić - na podstawie konkretnych sytuacji - sposoby postępowania w sytuacji wykonania przelewu z podaniem nieprawidłowego numeru rachunku odbiorcy;
- będzie umiał/a współpracować i argumentować własne stanowisko w grupie.



METODY I FORMY PRACY

- miniwykład
- gry dydaktyczne
- praca z wykorzystaniem aplikacji internetowych
- debata
- rozmowa nauczająca
- praca w grupach, praca indywidualna

KLUCZOWE POJĘCIA

- Rzecznik Finansowy
- bezpieczeństwo cyfrowe
- transakcje finansowe
- oszustwo internetowe
- phishing

MATERIAŁY POMOCNICZE

- Załącznik nr 1. Quiz Kahoot
- Załącznik nr 2. Konferencja prasowa - opisy przypadków
- Załącznik nr 3. Atak phishingowy – tekst rozszerzony dla nauczyciela; dla uczniów infografika dostępna jest oddzielnie jako pdf-y oraz do wykorzystania w wersji online w aplikacji Piktochart
<https://create.piktochart.com/output/29727058-od-niebezpiecznego-zalacznika-do-utracy-naszyc-pieniedzy>;
<https://create.piktochart.com/output/29657494-atak-phishingowy>
- Załącznik nr 4. Bezpieczeństwo transakcji płatniczych wykonywanych w internecie - prezentacja autorstwa Bartosza Wyżykowskiego (materiał dla nauczyciela)
- Załącznik nr 5. Infografika dotycząca ścieżki postępowania w przypadku omyłkowego przelewu
- Infografika dotycząca działalności RF - https://rf.gov.pl/pdf/RzF_OnePage1_Jak-pomaga.pdf [dostęp 12.04.2018]
- smartfony,
- flamastry, flipchart
- aplikacja Kahoot
- rzutnik, komputer, dostęp do internetu



POWIĄZANIE Z PODSTAWĄ PROGRAMOWĄ¹

Szkoła ponadpodstawowa

Informatyka

V. Przestrzeganie prawa i zasad bezpieczeństwa. Respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych.

Uczeń: 1) postępuje zgodnie z zasadami netykiety oraz regulacjami prawnymi dotyczącymi: ochrony danych osobowych, ochrony informacji oraz prawa autorskiego i ochrony własności intelektualnej w dostępie do informacji; jest świadomy konsekwencji łamania tych zasad.; 2) rozumie rolę szyfrowania, technik uwierzytelniania, kryptografii i podpisu elektronicznego w ochronie i dostępie do informacji; stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego; 3) potrafi opisać szkody, jakie mogą spowodować działania pirackie w sieci, w odniesieniu do indywidualnych osób, wybranych instytucji i całego społeczeństwa.

Podstawy przedsiębiorczości

II. Rynek finansowy: pieniądź i jego obieg, instytucje rynku finansowego, formy inwestowania, bank centralny i polityka pieniężna, bankowość komercyjna i spółdzielcza, podatki, ubezpieczenia, umowy bankowe i ubezpieczeniowe, ochrona klienta usług finansowych, etyka w finansach.

Uczeń: 1) omawia funkcje i formy pieniądza oraz jego obieg w gospodarce;

2) charakteryzuje instytucje rynku finansowego w Polsce: (...) Rzecznik Finansowy, oraz objaśnia ich znaczenie w funkcjonowaniu gospodarki narodowej, przedsiębiorstw i życiu człowieka; (...) 16) jest świadomy, że należy korzystać z różnorodnych i wiarygodnych źródeł informacji przed podjęciem decyzji finansowych.

¹ Rozporządzenie Ministra Edukacji Narodowej z dnia 30 stycznia 2018 r. w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia (Dz.U z 2018 r., poz. 467), <http://www.dziennikustaw.gov.pl> [dostęp 12.04.2018].



UWAGI METODYCZNE

Wymienione powyżej wymagania szczegółowe podstawy programowej podstaw przedsiębiorczości wskazują na znaczenie tak wiedzy na temat finansów, jak i umiejętności związanych ze świadomym funkcjonowaniem na rynku finansowym konsumenta. Podczas realizacji tego rodzaju tematyki szczególnie ważne jest, by uczeń na realnych przykładach dokonywał oceny oraz podejmował dojrzałe decyzje, rozumiejąc ich rozmaite konsekwencje.

Przed lekcją prowadzący zajęcia powinien zapoznać się z prezentacją multimedialną pt. *Bezpieczeństwo transakcji płatniczych wykonywanych w internecie* przygotowaną przez Bartosza Wyżykowskiego, Zastępcę Dyrektora Wydziału Klienta Rynku Bankowo-Kapitałowego Biura Rzecznika Finansowego (dołączonej do scenariusza zajęć).

Specjalistycznym źródłem wiedzy w omawianej tematyce powinna być również strona internetowa Rzecznika Finansowego – www.rf.gov.pl z umieszczonymi tam infografikami oraz opisami bieżących spraw, którymi zajmuje się Rzecznik.

MOŻLIWOŚĆ KONTYNUACJI ZAJĘĆ W POSTACI PROJEKTU EDUKACYJNEGO

Można zachęcić młodzież, by przeprowadziła z osobami dorosłymi (np. rodzicami, dziadkami, rodzeństwem, nauczycielami) wywiady na temat bezpieczeństwa transakcji finansowych wykonywanych za pośrednictwem internetu. Ich celem powinno być uzyskanie odpowiedzi na przykładowe pytania dot. wiedzy na temat bezpieczeństwa wykonywanych powszechnie finansowych transakcji w internecie:

- *W jaki sposób najczęściej można być okradzionym w sieci?*
- *Na co należy uważać przy zakupach internetowych?*
- *Jakie środki ostrożności należy podjąć wykonując przelew internetowy?*
- *Czy transakcje internetowe są regulowane prawnie?*
- *Jakie prawa ma osoba robiąca zakupy i przelewy w internecie?*
- *Co należy zrobić jeśli wpisało się błędny numer konta internetowego i wykonało przelew?*



Wywiady uczniowie mogą nagrywać na smartfonach. Kluczowe wnioski z przeprowadzonych wywiadów każdy z uczniów prezentuje na forum klasowym. Prezentację uczniowie mogą przygotować z użyciem bezpłatnych aplikacji (np. CANVA - www.canva.com lub Thinglink www.thinglink.com). Rolą nauczyciela jest podsumowanie zaprezentowanych wniosków w postaci mapy myśli.

Można też zachęcić uczniów, by kluczowe informacje dotyczące podstawowych zasad bezpieczeństwa transakcji finansowych dokonywanych w sieci przedstawili w postaci infografik i umieścili je na szkolnej stronie internetowej lub FB a także – wydrukowane - na ściennych gazetkach. Wcześniej przygotowane ulotki można rozdawać rodzicom podczas dni otwartych szkoły lub wywiadówek.

PRZEBIEG ZAJĘĆ

Wprowadzenie

1. Rola Rzecznika Finansowego – quiz Kahoot (10 minut)

Tytułem wprowadzenia nauczyciel wyjaśnia, że istnieją w Polsce oraz innych krajach instytucje państwowe dbające o prawa różnych osób i grup, wspierające słabszą stronę, czyli obywateli w sporach z przedsiębiorcami czy instytucjami. Może poprosić uczniów/uczennice, by podali przykłady takich instytucji lub sam je wskazać, zachęcając uczniów, by spróbowali wyjaśnić jakich obszarów/osób może dotyczyć ich ochrona (np. Rzecznik Praw Dziecka, Rzecznik Praw Obywatelskich, Rzecznik Funduszy Europejskich, Społeczny Rzecznik Praw Osób Starszych).

Następnie pyta uczniów/uczennice, czy słyszeli o Rzeczniku Finansowym oraz zbiera od uczniów propozycje, jakie obszary może obejmować jego działalność. Na zakończenie weryfikuje podawane przez uczniów informacje, wyjaśniając, że Rzecznik Finansowy w Polsce funkcjonuje już od 2015 r. Wyświetla infografikę dotyczącą działalności RF (dostępną na stronie: https://rf.gov.pl/pdf/RzF_OnePage1_Jak-pomaga.pdf [dostęp 12.04.2018] lub **Załącznik 1a**) i prosi uczniów, by zapamiętali jak najwięcej informacji. Prosi następnie uczniów aby zalogowali się na stronę internetową (a pomocą smartfonów): www.play.kahoot.it ², gdzie wcześniej powinien zostać umieszczony quiz zaproponowany w

² Strona dla administratora quizu to <https://kahoot.com/>



Załączniku nr 1 (nauczyciel może też rozwinąć zaproponowany test dodając inne, ważne z jego punktu widzenia, pytania).

Po wypełnieniu przez uczniów/uczennice testu prowadzący wspólnie z nimi podsumowuje wyniki. Zachęca też młodzież do odwiedzenia strony RF (może razem z rodzicami) oraz profilu na FB, gdzie mogą znaleźć więcej informacji (także w postaci infografik) dotyczących bieżącej działalności Rzecznika.

Może też przygotować dla każdego ucznia wydruk wskazanej wyżej infografiki i po omówieniu roli Rzecznika poprosić uczniów o wklejenie jej do zeszytów.

Wyjaśnia też, czym będą zajmowali się na zajęciach – podaje cele lekcji oraz sposób pracy.

Rozwinięcie

2. Czy moje zakupy i przelewy internetowe są bezpieczne – minidebata oksfordzka? (15 minut)

Nauczyciel dzieli klasę na trzy grupy. Podziału może dokonać poprzez odliczenie do trzech (lub z wykorzystaniem innego, używanego przez siebie, sprawdzonego sposobu).

Pierwsza grupa uczniów będzie wcielała się w rolę obrońców tezy, że użytkownicy internetu nie mają się czego obawiać przy wykonywaniu zakupów i płatności w sieci, ponieważ obecnie internet jest bardzo bezpieczny.

Druga grupa uczniów będzie oponentem tej tezy twierząc, że w przestrzeni online czeka na każdego wiele zagrożeń, na które należy uważać przy wykonywaniu nawet najprostszych czynności, gdzie pojawiają się dane poufne.

Trzecia grupa uczniów będzie obserwatorem, którego zadaniem jest ocena argumentów dwóch pierwszych grup. Nauczyciel jest moderatorem dyskusji oraz podsumowuje pojawiające się argumenty. Oceny obu stanowisk może zostać dokonana poprzez tajne głosowanie lub poprzez przechodzenie obserwatorów na wybraną stronę (tezy lub kontrtezy). Swoje przewidziane stanowisko mogą zabrać także członkowie grupy pierwszej i drugiej.

W związku z tym, że jest to minidebata można poprosić grupy o przygotowanie od 3 do 5 argumentów przemawiających za bronionym



stanowiskiem. Argumenty „zwycięskiej grupy” wszyscy uczniowie zapisują w zeszytach w postaci notatki.

3. Elektroniczne zagrożenia – gry w TABU (10 minut)

Nauczyciel dzieli klasę ponownie na 5 grup. Przedstawiciel każdej z nich losuje jedną z przygotowanych wcześniej karteczek z nazwami elektronicznego zagrożenia, rzutującego na bezpieczeństwo finansowe użytkowników urządzeń elektronicznych. Wśród tych zagrożeń są:

- brak oprogramowania antywirusowego,
- pobranie „pirackiego oprogramowania”, które ma w sobie program szpiegujący (zbierający dane o loginach i hasłach tzw. keylogger),
- atak phishingowy*,
- korzystanie z bankowości elektronicznej poprzez ogólnodostępne wi-fi (otwartą sieć),
- posiadanie jednego hasła do wszystkich serwisów (poczty, banku, sklepu internetowego, portalu społecznościowego)

Zadaniem uczniów (każdej z grup) będzie opisanie danego zjawiska z wykorzystaniem przekazu werbalnego (bez użycia słów kluczowych), niewerbalnego lub za pomocą rysunków.

Uwaga! Grupa, której zadaniem jest przedstawienie hasła „atak phishingowy” powinna dostać krótki opis tego przestępstwa – możliwe że po raz pierwszy styka się z tym pojęciem, a zatem by je przekazać innym uczniom, musi się zapoznać z podstawowymi informacjami na ten temat. Nauczyciel informację tę może przygotować na podstawie slajdów z prezentacji stanowiącej **Załącznik nr 4** do tego scenariusza. Materiał ten może wyglądać następująco:

Atak phishingowy (smishingowy) to metoda „oszustwa”, w której osoba trzecia podszywa się pod inny podmiot w celu wyłudzenia informacji (danych), które umożliwią zalogowanie się do bankowości elektronicznej (uwierzytelnienie) i zlecenia oraz autoryzowania transakcji płatniczej (najczęściej przelewu). Wyłudzenie danych odbywa się przy pomocy różnego rodzaju socjotechnik (np. osoby w kontakcie telefonicznym podają się za pracowników banku, kancelarii prawnej lub firmy współpracującej z bankiem, i – powołując się na potrzebę zwiększenia bezpieczeństwa – proszą o podanie poufnych informacji; przy pomocy



złośliwego oprogramowania (najczęściej instaluje się po otwarciu załączników do fałszywych e-maili (smsów lub wiadomości) albo np. w związku z pobraniem aplikacji mobilnej; poprzez podmianę prawdziwego numeru rachunku bankowego użytkownika na fałszywy; poprzez podszywanie się pod konto znajomego i prośbę o wspomóżenie przez dot-pay czy przelewy 24.

W trakcie prezentacji haseł wszyscy uczniowie koncentrują się na odganięciu prezentowanego zagrożenia. Nauczyciel podsumowuje poszczególne prezentacje, natomiast po odgadnięciu przez klasę zjawiska phishingu wyświetla na rzutniku infografiki (**Załącznik nr 3 w wersji online**) dotyczącą ataku tego typu, omawiając jego mechanizm, przyczyny i skutki. Infografiki te można rozdać uczniom w szkole oraz rodzicom podczas wywiadówek. Zachęcamy do „osadzenia” na stronie internetowej szkoły ich wersji on-line.

4. Jak pomóc oszukanym w internecie - konferencja prasowa (35 minut)

W tej części zajęć nauczyciel wciela się w postać „rzecznika prasowego” osób, które zostały oszukane w sieci lub za pomocą internetu wykonały działania, które naraziły ich na straty finansowe lub też inne kłopoty. Zanim zacznie się konferencja uczniowie otrzymują kartki z poszczególnymi historiami (jeden uczeń – jedna historia). Zapoznają się z nimi indywidualnie, zastanawiając się, o co chcieliby zapytać „rzecznika prasowego”, by lepiej zrozumieć, co i dlaczego się w danym przypadku wydarzyło oraz co można zrobić, by poprawić/naprawić sytuację ofiary opisywanego zdarzenia. Ważne jest, by uczniowie przygotowali też pytania o możliwe sposoby zabezpieczenia się przed opisywanymi przypadkami w przyszłości. Na zapoznanie się z historią i przygotowanie pytań powinni mieć co najmniej 10 minut – mogą zebrać się w grupy analizujące ten sam przypadek i wspólnie ustalić zestaw pytań.

Uwaga! Ważnym elementem w trakcie wyjaśnienia danych sytuacji powinno być odwoływanie się przez „rzecznika prasowego” – nauczyciela do ustawy o usługach płatniczych – najważniejsze uregulowania przedstawione zostały w prezentacji stanowiącej załącznik do scenariusza)³. Zaprezentowanie prawnego zakotwiczenia

³ Ustawa z dnia 19 sierpnia 2011 o usługach płatniczych (Dz.U. 2011 Nr 199, poz. 1175).



danych sytuacji pozwoli na pełniejsze zrozumienie zagrożeń oraz mechanizmów ochronnych dotyczących popularnych usług sieciowo-finansowych. Prowadzący podkreśla też na zakończenie konferencji, jak ważne jest systematyczne zapoznawanie się z ostrzeżeniami banku (np. na stronie internetowej, komunikatach e-mailowych, czy też w systemie bankowym).

Proponujemy, by konferencja przebiegała według następującego porządku: 1) odczytanie na głos przez moderatora konferencji lub wyświetlenie na rzutniku pojedynczej historii 2) czas na zadanie 2-3 pytań „rzecznikowi prasowemu” 3) czas na odpowiedzi „rzecznika prasowego” 4) odwołanie się do kontekstu prawnego (z wykorzystaniem prezentacji załączonej do scenariusza) opisanej sytuacji.

Aby „konferencja prasowa” przebiegła sprawnie można poprosić jednego z uczniów, by ją moderował, pilnując kolejności zadawanych pytań, ich długości oraz czasu odpowiedzi.

Poszczególne historie do wykorzystania w tym ćwiczeniu znajdują się w **Załączniku nr 2**. Pod każdą historią znajduje się odniesienie do zapisów ustawy o usługach płatniczych⁴, którymi warto każdą rundę pytań i odpowiedzi podsumować. Zachęcamy prowadzącego do przygotowania prezentacji porządkującej ten materiał.

5. Każdy może się pomylić – rozmowa nauczająca (10 minut)

Na początku nauczyciel zadaje pytanie uczniom:

- *Kto z was płacił przez internet za: bilet, zamówiony towar, jakiś cyfrowy produkt (np. e-book), opłacał rachunki lub pomagał w realizacji takiej opłaty?*

Kontynuując rozmowę nauczyciel zadaje kolejne pytanie:

- *Na jakie elementy zwiększające bezpieczeństwo zwracaliście wtedy uwagę?*

⁴ Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. 2011, Nr 199, poz. 1175; Ustawa z dnia 22 marca 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (Dz.U. 2018, poz. 864).



Pod dyskusję zostają w trakcie rozmowy poddane kwestie protokołu przesyłania danych (http i https, wirusy zmieniające numery konta – przy wykonywaniu czynności kopiuj-wklej czy też popularne przez pewien czas „nigeryjskie szwindle”). Następnie prowadzący prosi uczniów, by spróbowali odpowiedzieć na trzecie pytanie:

- *Który z wymienionych wyżej elementów jest – waszym zdaniem - najistotniejszy w trakcie realizacji przelewu internetowego?*

W trakcie rozmowy należy podkreślić istotę numeru rachunku - unikatowego identyfikatora (art. 143 ust. 1 ustawy o usługach płatniczych), wyjaśniając, że autoryzacja przelewu z błędnym numerem konta w zleceniu płatniczym powoduje wyłączenie odpowiedzialności dostawcy usługi, nawet jeśli płatnik (np. właściciel konta) miał jako intencję wskazanie innego, prawidłowego konta.

Nauczyciel zadaje następnie kolejne pytanie:

- *Czy płatnik może dochodzić roszczeń np. w banku, jeśli poprzez roztargnienie pomyli cyfry w zleceniu przelewu?*

Pytając uczniów o rozwiązania dla powyższej sytuacji nauczyciel rozpatruje realność poszczególnych wskazań z uwzględnieniem nowelizacji ustawy o usługach płatniczych (której inicjatorem był Rzecznik Finansowy), wyświetlając infografikę z Załącznika nr 5.

„Jeżeli procedura nie doprowadzi do odzyskania mylnie przelanej kwoty w terminie miesiąca od zgłoszenia zdarzenia przez płatnika swojemu dostawcy, płatnik będzie miał prawo zwrócić się do dostawcy o udostępnienie danych odbiorcy i je otrzyma w celu umożliwienia skutecznego dochodzenia roszczeń na drodze sądowej”⁵.

W podsumowaniu warto zaznaczyć, że choć wszystkie pozostałe elementy zwiększające bezpieczeństwo wydają się na tym tle mało istotne dla wykonania danej transakcji, nie oznacza to jednak, że należy te elementy pomijać.

Podsumowanie

6. Bezpieczne finanse w sieci – mapa myśli (10 minut)

⁵ Ustawa z dnia 22 marca 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (Dz.U. 2018, poz. 864) oraz prezentacja załączona do scenariusza.



Nauczyciel prosi uczniów, aby dokonali podsumowania zajęć poprzez wykonanie mapy myśli dotyczącej bezpieczeństwa cyfrowego w kontekście finansowym przy użyciu aplikacji Coggle.it lub innego podobnego oprogramowania.

Mapa myśli powinna uwzględniać czynniki chroniące użytkowników przed pomyłkami, oszustwami, kradzieżami oraz zawierające elementy: techniczne, ludzkie, manipulacyjne, krytycznego odbioru informacji. Link do mapy myśli uczniowie mogą przestać e-mailowo na konto nauczyciela.

Tytułem podsumowania nauczyciel wyświetla również kilka stron internetowych, gdzie uczniowie lub ich rodzice, dziadkowie, znajomi mogą uzyskać pomoc w przypadku wystąpienia naruszenia bezpieczeństwa cyfrowego:

- Naruszenia bezpieczeństwa finansowego - <https://rf.gov.pl/>
- DyżurNet (SaferInternet) - <https://dyzurnet.pl/>
- Projekt CyfrowoBezpieczni - <https://www.cyfrowobezpieczni.pl/centrum-pomocy>
- Projekt Cybernauci - <https://cybernauci.edu.pl>



Załącznik nr 1. Quiz Kahoot (przykładowe pytania)

Pytanie nr 1. Rzecznik Finansowy zajmuje się wspieraniem klientów w sporach z podmiotami rynku finansowego (np. bankami, ubezpieczycielami)

a) TAK⁶

b) TAK, ale tylko dla firm

c) NIE

Pytanie nr 2. Rzecznik Finansowy ma możliwość wnioskowania do właściwych organów o podjęcie inicjatywy ustawodawczej lub zmianę prawa w zakresie:

a) reklamacji kupna sprzedaży produktów elektronicznych

b) ochrony klientów podmiotów rynku finansowego

c) żadnym z powyższych.

Pytanie nr 3. Rzecznik Finansowy ma możliwość rozwiązania sporu klienta z podmiotem rynku finansowego poprzez:

a) osobiste wizyty w danej instytucji i rozwiązywanie problemów klientów

b) postępowanie polubowne

c) zawiadomienie policji.

Nauczyciel powinien dodać po tym pytaniu, że podejmowanie postępowania polubownego to stosunkowo nowa kompetencja Rzecznika Finansowego. Jej dodanie wynika rosnącej popularności pozasądowych form rozwiązywania sporów..

Podmioty rynku finansowego mają obowiązek przystąpić do tego postępowania, co uzasadniono „potrzebą zapewnienia wysokiego poziomu ochrony klientów podmiotów rynku finansowego”. Postępowanie polubowne jest prowadzone na wniosek klienta (opłata 50 zł na rachunek Rzecznika Finansowego). Trzeba w nim określić jakiego rodzaju działań klient oczekuje. Prowadzący postępowanie może najpierw spróbować doprowadzić do zbliżenia stanowisk stron sporu, wykorzystując techniki mediacyjne. Jeśli to nie przyniesie efektu może przedstawić stronom swoją propozycję rozwiązania sporu, jak w typowej

⁶ Prawidłowe odpowiedzi zostały pogrubione.



**Rzecznik
Finansowy**

www.rf.gov.pl

CEO
CENTRUM EDUKACJI
OBYWATELSKIEJ

koncyliacji. Klient może wybrać obydwie tryby lub tylko jeden (<https://rf.gov.pl/polubowne/#top-5-pytan>)

Pytanie nr 4. Który z obszarów działań dotyczy działalności Rzecznika Finansowego?

a) edukacyjno-informacyjne (np. skierowane do konsumentów)

b) kontrola wypłacalności banków

c) nakładanie kar na instytucje wprowadzające w błąd klientów.

Pytanie nr 5. Czy Rzecznik Finansowy może udzielać wsparcia osobom prywatnym poszukującym pomocy np. w sporze z bankiem?

a) TAK

b) NIE

c) TAK, ale tylko gdy wpłacą odpowiednią kwotę za pomoc.



Załącznik nr 2. Konferencja prasowa - opisy przypadków

Historia nr 1

Pan Iksiński zalogował się na własne konto bankowe. Okazało się, że ktoś autoryzował przelew na kilkaset złotych z jego konta za zakupy w znanym portalu aukcyjnym. Pan Iksiński czuje się oszukany i nie wie kogo zawiadomić w pierwszej kolejności, jakie podjąć działania aby odzyskać pieniądze oraz czy to nie jest jego wina, ponieważ ma nieaktualny program antywirusowy.

Po serii pytań uczniów rolę nauczyciela jest wyjaśnienie, że jeśli dane do logowania i autoryzacji przelewu zostały użyte przez inne osoby bez woli i zgody płatnika wtedy pan Iksiński jest chroniony - mówi o tym art. 40 ust. 1 ustawy o usługach płatniczych. Wyświetla slajd o następującej treści:

Transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą (Art. 40, ust. 1).

Ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika. Wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana (Art. 45, ust. 1, 2).

Historia nr 2

Pan Iksiński złożył reklamację w banku, jednakże instytucja finansowa odmówiła uznania reklamacji zastaniając się błędami klienta. Dane do logowania oraz dostęp uwierzytliwiający przez SMS był odpowiednio chroniony przez pana Iksińskiego.

Nauczyciel w trakcie odpowiadania na pytania dziennikarzy - uczniów nawiązuje do ustawy o usługach płatniczych - Art. 46 ust. 3 oraz Art. 42 ust. 1. Ważnym elementem rozmowy jest uświadomienie uczniom kwestii



zapisanych w umowie z bankiem dotyczących należitych środków ochronnych. Po udzieleniu odpowiedzi zostają wyświetlone następujące zapisy z ustawy o usługach płatniczych, a następnie omówione przez prowadzącego w kontekście analizowanego przypadku.

Płatnik odpowiada za nieautoryzowane transakcje płatnicze w pełnej wysokości, jeżeli doprowadził do nich umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 (Art. 46 ust. 3).

1. Użytkownik uprawniony do korzystania z instrumentu płatniczego jest obowiązany:

*1) korzystać z instrumentu płatniczego zgodnie z umową ramową oraz
2) zgłaszać niezwłocznie dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu.*

2. W celu spełnienia obowiązku, o którym mowa w ust. 1 pkt 1, użytkownik, z chwilą otrzymania instrumentu płatniczego, podejmuje niezbędne środki służące zapobieżeniu naruszeniu indywidualnych zabezpieczeń tego instrumentu, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym (Art. 42 ust. 1, 2)

Historia 3

Pan Iksiński otrzymał odmowę uznania reklamacji z banku, jednak przeczytał w Internecie, że jego działań, nie można uznać za rażące niedbalstwo. Nie naruszały też art. 42 ustawy o usługach płatniczych. Czy istnieje zatem jakieś rozwiązanie zawarte w ustawie pozwalające na dalszą argumentację w sporze z bankiem?

Nauczyciel prezentuje na kolejnym slajdzie dalsze informacje:

W przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika jest obowiązany niezwłocznie zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej, a w przypadku gdy płatnik korzysta z rachunku płatniczego, przywrócić obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza (Art. 46 ust. 1).



Zwraca jednak uczniom uwagę na fakt, że zacytowany wyżej przepis ma znaczenie porządkowe – opisuje, co się ma wydarzyć, jeśli już wiadomo, że doszło do „nieautoryzowanej” transakcji płatniczej.

Jeśli bank odrzuca reklamację i wskazuje własne argumenty, to osoba poszkodowana może:

- 1) można udać się do Rzecznika Finansowego, żeby jego eksperci spojrzeli na przypadek i zgromadzoną argumentację, szczególnie, że kwestia definicji rażącego niedbalstwa jest kwestią typowo prawną;
- 2) jeśli nie uda się rozwiązać sprawy przy pomocy Rzecznika Finansowego (czy to w trybie polubownym czy interwencyjnym), to pozostaje droga sądowa. Wtedy, jak podkreślono to przy pierwszej historii, obowiązek zgromadzenia i przedstawienia dowodu leży po stronie banku

Historia 4

Kolega pana Iksińskiego pan Adamski gdy dowiedział się o przejściach swojego przyjaciela opowiedział mu własną historię, która przydarzyła się niedawno. Pan Adamski miał zainstalowany program antymalware, posiadał aktualny antywirus, miał wykupione dodatkowe zabezpieczenia w postaci firewalla. System operacyjny miał również wyposażony w nowe aktualizacje. Pewnego dnia otrzymał od banku informację, że musi również zaktualizować oprogramowanie na Androida łączące się z bankiem przy wykorzystaniu telefonu komórkowego. Tak też zrobił. Następnego dnia okazało się, że z konta pana Adamskiego zniknęła pewna znacząca kwota. Przyjaciel pana Iksińskiego złożył reklamację do banku.

Nauczyciel zadaje pytanie, na jakie argumenty mógł się powołać przy tworzeniu reklamacji pan Adamski? Omawia wskazane przez uczniów propozycje i wyświetla następujący slajd:

Pan Adamski nie przekazał nikomu loginów i haseł, nie autoryzował przelewu, zatem, nie naruszył obowiązku wskazanego w art. 42 ust. 2 ustawy o usługach płatniczych. Ponadto wskazana osoba niezwłocznie zawiadomiła o zaistnieniu nieautoryzowanej transakcji, więc spełniła obowiązek wynikający z art. 42 ust. 1 pkt. 2 ustawy o usługach płatniczych.



Załącznik nr 3. Atak phishingowy⁷

Wersje graficzne i online dostępne pod linkami (można je udostępniać za pomocą portali społecznościowych oraz osadzać na stronie. Można też pobrać pdf i wydrukować wersję papierową).

<https://create.piktochart.com/output/29727058-od-niebezpiecznego-zalacznika-do-utracy-naszyc-pieniedzy>

<https://create.piktochart.com/output/29657494-atak-phishingowy>

Pishing – co to takiego?

Atak phishingowy (smishingowy) to metoda oszustwa, w której osoba trzecia podszywa się pod inny podmiot w celu wyłudzenia informacji (danych), które umożliwią zalogowanie się do bankowości elektronicznej (uwierzytelnienie) i zlecenie oraz autoryzowanie transakcji płatniczej (najczęściej przelewu).

Jak wyłudzane są nasze dane?

Wyłudzenie danych odbywa się przy pomocy różnego rodzaju socjotechnik:

- osoby w kontakcie telefonicznym podają się za pracowników banku, kancelarii prawnej lub firmy współpracującej z bankiem, i – powołując się na potrzebę zwiększenia bezpieczeństwa – proszą o podanie poufnych informacji;
- przy pomocy złośliwego oprogramowania (najczęściej instaluje się ono po otwarciu załączników do fałszywych e-maili, smsów lub wiadomości albo w związku z pobraniem aplikacji mobilnej);
- poprzez podmianę prawdziwego numeru rachunku bankowego użytkownika na fałszywy;
- poprzez podszywanie się pod konto FB znajomego i prośbę o wspomoczenie przez dot-pay czy Przelewy 24.

⁷ Materiał powstał w oparciu o prezentację *Bezpieczeństwo transakcji płatniczych wykonywanych w internecie* autorstwa Bartosza Wyżkowskiego oraz materiały wypracowane w projekcie „Zagrożenia Cyberprzestrzeni” realizowanym przez WSP TWP w Warszawie - *Zjawisko phishingu oraz bankowość elektroniczna*, Zespół NASK: Marcin Bochenek, Piotr Bisalski, Anna Rywczyńska, Martyna Rożycka, Krzysztof Silicki, Agnieszka Wrońska, [w:] J. Lizut, *Zagrożenia Cyberprzestrzeni*, Wydawnictwo WSP TWP, Warszawa, 2015, s.239-240.

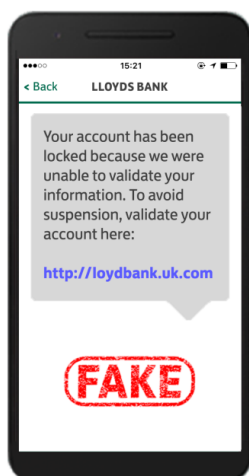
Jak się chronić?

- Zawsze korzystaj z legalnego oprogramowania i regularnie go aktualizuj.
- Stosuj programy antywirusowe oraz firewall.
- Nie wyszukuj stron internetowych banku przez przeglądarki.
- Nie otwieraj e-maili nieznanego pochodzenia, nie odpowiadaj na nie, a zwłaszcza nie otwieraj załączników lub linków w nich wskazanych.
- Zmieniaj regularnie hasło do konta.
- Nie kopiuj numerów rachunków ze „schowka”.
- Weryfikuj dane zawarte w SMS-ach autoryzacyjnych: rodzaj dyspozycji i dane transakcji w SMS-ie powinny się zgadzać się z tymi, które wyświetlają się na ekranie.
- Nie loguj się do banku z otwartych sieci WiFi.

Od niebezpiecznego załącznika do utraty pieniędzy

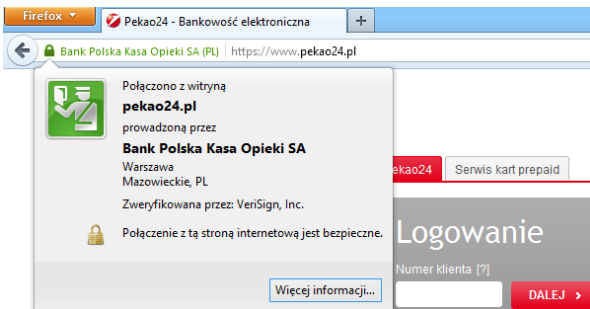


Atakujący wysyła spam, czyli dużą liczbę wiadomości przy pomocy poczty elektronicznej lub portali społecznościowych do wielu internautów, w celu skłonienia ich do odwiedzenia konkretnej strony internetowej lub podania osobistych danych (np. loginu i hasła do serwisu aukcyjnego czy konta bankowego).

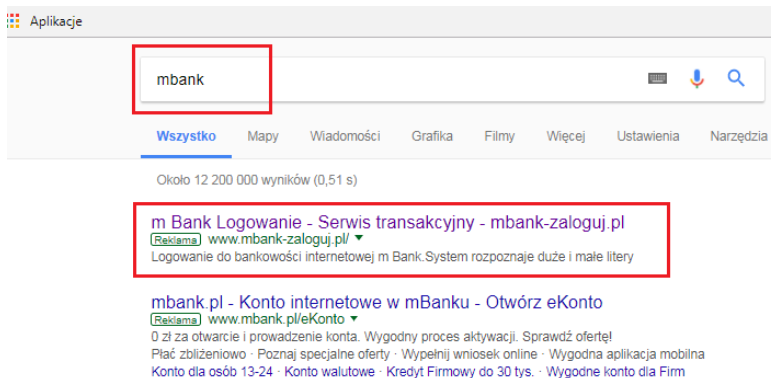


Spamer często podszywa się pod znaną instytucję (np. bank) i uzasadnia konieczność zweryfikowania danych do konta internetowego procedurami bankowymi lub zablokowaniem konta.

Link do strony internetowej spamera bardzo przypomina adres http konkretnego banku.



Ofiara, w zależności od treści e-maila, podaje swoje poufne dane lub wchodzi na spreparowaną przez cyberprzestępcę stronę, która do złudzenia przypomina znaną mu witrynę.



Na spreparowanej stronie ofiara loguje się, myśląc, że ma do czynienia z autentyczną witryną swojego banku albo serwisu aukcyjnego i jej dane poufne zostają przechwycone przez przestępcę.

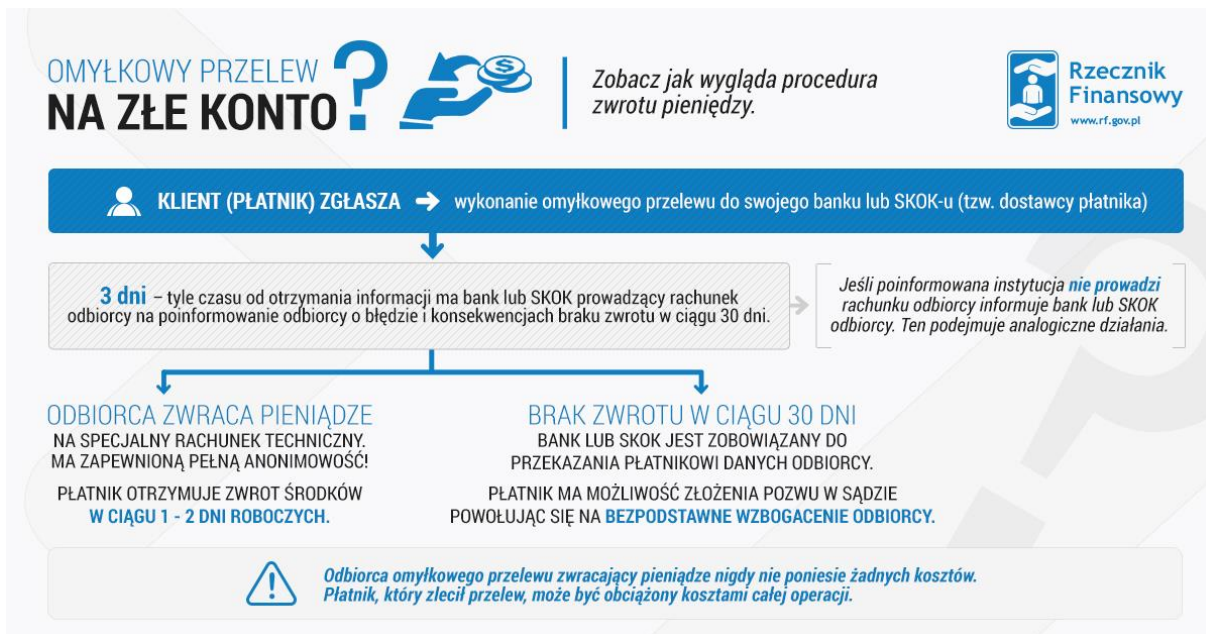
Komputer bądź smartfon użytkownika zostaje zarażony tzw. złośliwym oprogramowaniem (ang. *malware*), takim jak wirusy czy konie trojańskie i dołącza do komputerów na całym świecie, które są pod kontrolą podziemia internetowego (tzw. *botnety*).

Od tej pory przestępca jest w stanie kontrolować wszystko, co robi na komputerze jego właściciel, m.in. jest w stanie dokonywać nieuprawnionych transakcji w sposób niezauważalny dla użytkownika – co jest bezpośrednim zagrożeniem dla portfela internauty.





Załącznik nr 5. Infografika dotycząca ścieżki postępowania w przypadku omyłkowego przelewu



INFORMACJE O AUTORZE SCENARIUSZA

dr Łukasz Tomczyk - inżynier informatyki, doktor filozofii PhDr. (specjalność edukacja dorosłych; doktor nauk społecznych w zakresie pedagogiki Recenzent podręczników szkolnych w Ministerstwie Edukacji Narodowej w zakresie technologii informacyjnej (w tym e-podręczników), projektów edukacyjnych i badawczych w Ministerstwie Kultury i Dziedzictwa Narodowego w obszarze edukacji informatycznej i medialnej. Autor i współautor 3 monografii, 80 artykułów recenzowanych, współredaktor 13 monografii wydanych w Polsce i za granicą. Recenzent artykułów w czasopismach z listy filadelfijskiej oraz notowanych w bazie SCOPUS. Uczestniczył jako prelegent w ponad 60 konferencjach naukowych. Tematyka poruszanych badań i analiz dotyczy: pedagogiki mediów, andragogiki, geragogiki. Uczestniczył do tej pory w 14 projektach badawczych. Członek rady programowej projektu Bezpiecni+ realizowanego dla MEN. Stypendysta programu Mundus Penta (odbył miesięczny staż w Bośni i Hercegowinie na Uniwersytecie w Sarajewie, gdzie badał zjawisko FOMO). Zrealizował kilkaset godzin wykładów i szkoleń w zakresie profilaktyki zagrożeń elektronicznych w Polsce i zagranicą (Czechy, Słowacja, Macedonia, Bośnia i Hercegowina, Niemcy).