Kupuj i płać bezpiecznie w Internecie

Materiał pomocniczy dla nauczycieli opracowany na podstawie prezentacji i wykładu wygłoszonego przez Bartosza Wyżykowskiego, Radcę Prawnego z Biura Rzecznika Finansowego w Rzeszowie 17 stycznia 2018 roku.

Zagadnienia omówione w prezentacji

Rzecznik Finansowy
www.rf.gov.pl

1. Kompetencje Rzecznika Finansowego.
2. Kradzież pieniędzy z rachunków płatniczych (ataki *phishingowe*)
3. Jak się chronić się przed atakami phishingowymi?
4. Regulacje prawne – ustawa o usługach płatniczych.
5. Wykonanie przelewu z podaniem nieprawidłowego numeru rachunku odbiorcy.

Kompetencje Rzecznika Finansowego

Rzecznik Finansowy
www.rf.gov.pl

- Instytucja Rzecznika Finansowego funkcjonuje od 11.10.2015 r.
- Rzecznik Finansowy jest następcą prawnym Rzecznika Ubezpieczonych.
- Jego zadaniem jest **ochrona klientów** (osób fizycznych) **podmiotów rynku finansowego** (np. banku, zakładu ubezpieczeń, instytucji pożyczkowej, instytucji finansowej, SKOK-ów, firm i funduszy inwestycyjnych).
- Podstawowym prawem klienta jest **prawo do złożenia reklamacji**.
- Obowiązkiem podmiotu rynku finansowego jest **rozpatrzenie reklamacji i udzielenie odpowiedzi.**

W przypadku negatywnego rozpatrzenia reklamacji każdy klient ma prawo do złożenia wniosku do Rzecznika Finansowego.

Jak działa Rzecznik Finansowy?

Rzecznik Finansowy
www.rf.gov.pl

DZIAŁANIA SYSTEMOWE
jeśli dostrzegamy problem, który powtarza się i dotyczy wielu osób

WNIOSKI O UCHWAŁĘ SĄDU NAJWYŻSZEGO
w razie dostrzeżenia istotnych rozbieżności w orzecznictwie.

ISTOTNE POGLĄDY
na etapie postępowania sądowego

PORADNICTWO
„pierwsza pomoc" dla klientów - telefoniczne, mailowe, na Facebooku

POREKLAMACYJNE POSTĘPOWANIA INTERWENCYJNE
stajemy po stronie klienta po odrzuceniu reklamacji przez podmiot rynku finansowego.

POREKLAMACYJNE POSTĘPOWANIA POLUBOWNE prowadzone przez bezstronnych i niezależnych ekspertów z zachowaniem poufności.

Transakcje płatnicze – zasięg i ryzyko

Rzecznik Finansowy
www.rf.gov.pl

- Współczesny obrót gospodarczy coraz częściej opiera się na **transakcjach bezgotówkowych.**
- **Liczba** konsumentów korzystających z **rachunków płatniczych** stale rośnie.

Nowelizacja ustawy o usługach płatniczych wprowadzająca dostęp do rachunku podstawowego w celu zapewnienie bezpłatnego dostępu do najważniejszych usług płatniczych (tj. płatności internetowych, mobilnych itd.)

- Upowszechnienie transakcji bezgotówkowych zwiększa ryzyko popełnienia błędu lub stania się ofiarą przestępstwa finansowego (ataki *phishingowe*, wyłudzenia danych przy pomocy złośliwego oprogramowania).

*Głównym motywem przestępstw internetowych w 2016 r. była chęć kradzieży środków pieniężnych należących do użytkowników Internetu – phishing oraz wzrost liczby prób oszustwa wobec klientów bankowości mobilnej.**

* Źródło: Raport roczny z działalności CERT Polska, https://www.cert.pl/PDF/Raport_CP_2016.pdf [dostęp 0.05.2018]

Rzecznik Finansowy
www.rf.gov.pl

KRADZIEŻ PIENIĘDZY Z RACHUNKÓW PŁATNICZYCH – PRAWA KLIENTÓW

Kradzież pieniędzy z rachunków płatniczych 1/4

Rzecznik Finansowy
www.rf.gov.pl

Co to jest 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.

Metody

1. **Wyłudzenie danych 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.

Przykładowy atak phishingowy 2/4

Rzecznik Finansowy
www.rf.gov.pl

From: Ryszard Nowicki [mailto:securitycheck@supportbdfrance.com]
Sent: Tuesday, May 31, 2016 10:10 PM
Subject: IPKO zostanie zablokowany w ciagu 2 dni: 390

Bank Polski

Dzień dobry.

Nasz system bezpieczeństwa wykrył podejrzaną aktywność na Państwa koncie. W celu uniknięcia zablokowania konta, prosimy o potwierdzenie swoich danych. Proszę nie wykonywać procedury powtórnie, jeżeli konto już zostało potwierdzone. Jeśli dostali Państwo tą wiadomość i nie podjęliście działań, konto zostanie zablokowane.

Przepraszamy za niedogodności.

Weryfikacja

Lukasz Szydlowski

Źródło:
https://www.pkobp.pl/

Kradzież pieniędzy z rachunków płatniczych 3/4

Rzecznik Finansowy
www.rf.gov.pl

2. Wyłudzenie danych przy pomocy złośliwego oprogramowania

Najczęściej instaluje się ono po otwarciu załączników do fałszywych e-maili (smsów lub wiadomości) albo np. w związku z pobraniem aplikacji mobilnej.

Na zainfekowanym komputerze użytkownikowi wyświetla się komunikat namawiający go do instalacji aplikacji (rzekomo pochodzącej z banku) w celu dodatkowej ochrony telefonu i bankowości elektronicznej. Informację o konieczności zainstalowania aplikacji użytkownik może również otrzymać w e-mailu.

W komunikacie lub e-mailu znajduje się pole do wpisania numeru telefonu, na który SMS-em wysyłany jest link do pobrania złośliwej aplikacji.

Zainstalowanie na telefonie złośliwego oprogramowania pozwala na uzyskanie „kontroli" nad telefonem (np. możliwość przekierowywania wiadomości SMS z kodami jednorazowymi, czy podsłuchiwania rozmów za pomocą mikrofonu w telefonie).

Kradzież pieniędzy z rachunków płatniczych 4/4

Rzecznik Finansowy
www.rf.gov.pl

3. Podmiana strony bankowej na fałszywą, dodanie do strony dodatkowych pól, treści i komunikatów.

Bezpośrednio po zalogowaniu się na fałszywą stronę użytkownik może zostać poproszony o podanie kodu jednorazowego z narzędzia autoryzacyjnego. Podany kod może następnie zostać wykorzystany przez przestępców (w sposób niewidoczny dla klienta) do realizacji przelewu lub zdefiniowania nowego szablonu odbiorcy płatności na wskazany rachunek docelowy. Od tej pory przestępcy mogą zlecać przelewy bez podawania kolejnych kodów autoryzacyjnych.

5. Podmiana prawdziwego numeru rachunku bankowego użytkownika na fałszywy.

6. Nowa metoda z wykorzystaniem Facebook'a.

Przestępca podszywa się pod konto FB znajomego i prosi o wspomożenie przez dot-pay czy Przelewy 24.

Jak się chronić przed atakami phisingowymi?

Rzecznik Finansowy
www.rf.gov.pl

- Korzystaj z **legalnego oprogramowania** i regularnie je **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 wskazanych w e-mailach lub komunikatach.**
- Regularnie **zmieniaj 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.**

Jak chronić klientów przed atakami phisingowymi?

Rzecznik Finansowy
www.rf.gov.pl

Konieczne zmiany – rekomendacje dla dostawców usług bankowych

- Dostawcy usług bankowych powinni wprowadzić – zwłaszcza na prośbę klienta – autoryzacji tzw. przelewów wewnętrznych
- Sugeruje się wprowadzenie dodatkowego mechanizmu wymuszania cyklicznego hasła.
- Konieczny jest lepszy monitoring nietypowych transakcji i systemowa weryfikacja, czy transakcja rzeczywiście była autoryzowana przez użytkownika

Regulacje prawne – ustawa o usługach płatniczych (UUP) 1/4

Rzecznik Finansowy
www.rf.gov.pl

PRZYKŁAD 1. Czy w sytuacji, w której transakcja dokonywana jest na podstawie działań podjętych przez inne niż płatnik osoby (np. gdy dane uwierzytelniające i autoryzujące uzyskane zostały w wyniku działań o charakterze przestępczym – co prowadzi do inicjacji transakcji płatniczej przez osoby trzecie wbrew woli lub bez wiedzy płatnika) w ogóle można mówić o zgodzie płatnika na jej przeprowadzenie?

Art. 40, ust. 1: *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. 45:

1) *Ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika.*

2) Wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana.

Regulacje prawne – ustawa o usługach płatniczych (UUP) 2/4

Rzecznik Finansowy
www.rf.gov.pl

PRZYKŁAD 2. Jak kształtują się zasady odpowiedzialności jeśli mamy do czynienia z nieautoryzowaną transakcją?

Dostawcy usług bankowych najczęściej argumentują, że to płatnik naruszył obowiązki wynikające z art. 42 ustawy i w konsekwencji - na podstawie art. 46 ust. 3 - rażąco niedbałe zachowanie klienta skutkuje jego pełną odpowiedzialnością za nieautoryzowaną transakcję.

Sugeruje to, że sami dostawcy uznają, że nie doszło do autoryzacji transakcji.

Regulacje prawne – ustawa o usługach płatniczych (UUP) 3/4

Rzecznik Finansowy
www.rf.gov.pl

Art. 46 ust. 3: *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. 42 ust. 1 UUP: 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.

Regulacje prawne – ustawa o usługach płatniczych (UUP) 4/4

Rzecznik Finansowy
www.rf.gov.pl

Aby uznać pełną odpowiedzialność płatnika nie wystarczy zarzucić mu rażące niedbalstwo, lecz trzeba dowieść, że naruszył on co najmniej jeden z obowiązków, o których mowa w art. 42 ustawy (na poprzednim slajdzie).

Ponadto treść artykułu 46 ust. 1 ustawy podkreśla, że 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 przed nieautoryzowaną transakcją płatniczą.

Mimo, iż we wskazanych w ustawie okolicznościach odpowiedzialność za nieautoryzowaną transakcję ponosi płatnik (art. 46 ust. 2 i 3), to żaden przepis ustawy nie uchyla obowiązku wynikającego z art. 46 ust. 1.

Jedyny wyjątek w tym zakresie stanowi art. 44 ust. 2. mówiący o niedopełnieniu przez płatnika obowiązku poinformowania o nieprawidłowościach w terminie 13 miesięcy od obciążenia rachunku.

Co mówi orzecznictwo? 1/3

Rzecznik Finansowy
www.rf.gov.pl

Wyrok Sądu Najwyższego z 18.01.2018 (sygn. akt. V CSK 141/17)

- Potwierdza linię prezentowaną przez Rzecznika Finansowego w sporach dotyczących nieautoryzowanych transakcji płatniczych
- Zgodnie z przepisami ustawy o usługach płatniczych - w uproszczeniu - konsument odpowiada za nieautoryzowaną transakcję płatniczą w pełnej wysokości tylko jeżeli doprowadził do niej umyślnie albo nie dopełnił obowiązków wynikających ze wspomnianej ustawy umyślnie lub w wyniku rażącego niedbalstwa.
- Przypomina, że ciężar dowodu w tym zakresie – również wówczas, gdy doszło do kradzieży środków z rachunku w wyniku działania przestępczego – spoczywa na dostawcy usług płatniczych (np. banku).
- W takich wypadkach bank obowiązany jest niezwłocznie zwrócić konsumentowi kwotę nieautoryzowanej transakcji płatniczej. Odpowiedzialność konsumenta ogranicza się co najwyżej do równowartości kwoty 150 euro.

Co mówi orzecznictwo? 2/3

Rzecznik Finansowy
www.rf.gov.pl

Wyroki Sądu Okręgowego w Łodzi: z 15.01.2016 (sygn. akt. I C 307/15); z 8.02.2016 (sygn. I C 1908/14):

- *Komputer powódki posiadał zainstalowane oprogramowanie antywirusowe. W ocenie Sądu skorzystanie przez powódkę z wyświetlonego podczas logowania na stronę Banku komunikatu zachęcającego użytkowników do „dodatkowego zabezpieczenia telefonu", które spowodowało w dalszej kolejności zainfekowanie szkodliwym oprogramowaniem aparatu komórkowego oraz komputera powódki nie nosi cech rażącego niedbalstwa.*
- *Powódka miała prawo pozostawać w przekonaniu, że komunikat wyświetlający się podczas logowania na stronę Banku pochodzi właśnie od Banku i służy uzyskaniu lepszych zabezpieczeń.*
- *Bank nie ostrzegał w dacie zdarzenia swoich klientów przed tego rodzaju komunikatami, nie informował, iż skorzystanie z nich może nieść za sobą negatywne skutki.*

Co mówi orzecznictwo? 3/3

Rzecznik Finansowy
www.rf.gov.pl

Wyroki Sądu Okręgowego w Łodzi: z 15.01.2016 (sygn. akt. I C 307/15); z 8.02.2016 (sygn. I C 1908/14) – ciąg dalszy:

- *Należy podkreślić, że powódka nie przekazała swojego loginu ani hasła do konta bankowego, a jedynie numer telefonu, nie naruszyła więc obowiązku wskazanego w art. 42 ust. 2 ustawy o usługach płatniczych.*
- *Należy dodać, iż powódka spełniła wynikający z art. 42 ust. 1 pkt. 2 ustawy o usługach płatniczych obowiązek niezwłocznego zawiadomienia o zaistnieniu nieautoryzowanej transakcji płatniczej.*
- *Powódka nie naruszyła obowiązków, o których mowa w art. 42 ustawy o usługach płatniczych. Bezzasadne jest tym samym twierdzenie pozwanego, że powódka przyczyniła się do powstania szkody.*
- *W związku z powyższym, zgodnie z art. 46 ust. 1 ustawy o usługach płatniczych, pozwany jest zobowiązany niezwłocznie zwrócić powódce kwotę nieautoryzowanej transakcji płatniczej.*

Rzecznik Finansowy
www.rf.gov.pl

WYKONANIE PRZELEWU Z PODANIEM NIEPRAWIDŁOWEGO NUMERU RACHUNKU

Przelew z podaniem nieprawidłowego numeru rachunku 1/3

Rzecznik Finansowy
www.rf.gov.pl

Jakie dane podajemy zlecając przelew?

- Numer rachunku, imię i nazwisko odbiorcy, tytuł przelewu, inne dane, które mają służyć identyfikacji odbiorcy lub oznaczeniu produktu lub usługi z jaką związany jest przelew.

Które z tych danych są istotne dla wykonania przelewu?

- **Numer rachunku** (unikatowy identyfikator)
- **Cel:** skrócenie czasu realizacji transakcji.
- **Negatywny skutek uboczny:** zmniejszenie bezpieczeństwa transakcji.

Sytuację tę umożliwiły zapisy ustawy o usługach płatniczych, która wprowadziła m.in. zasadę, zgodnie z którą transakcja płatnicza powinna zostać zrealizowana najpóźniej w następnym dniu roboczym po jej zleceniu.

Przelew z podaniem nieprawidłowego numeru rachunku 2/3

Rzecznik Finansowy
www.rf.gov.pl

Co to oznacza w praktyce?

- Dla wykonania danej transakcji bez znaczenia pozostają wszelkie – poza unikatowym identyfikatorem – dane identyfikujące odbiorcę (nawet jeżeli zostały wskazane przez płatnika w zleceniu płatniczym).
- Częstym błędem jest podanie nieprawidłowego unikatowego identyfikatora odbiorcy, czyli **wskazanie nieprawidłowego numeru rachunku płatniczego odbiorcy**.
- **Autoryzacja** takiego przelewu doprowadzi do uznania rachunku odbiorcy do którego przypisany jest numer wskazany w zleceniu płatniczym.
- Źródła błędu:

- płatnik

- pomyłka/działanie odbiorcy lub osoby trzeciej (nie chodzi o działania przestępcze).

Przelew z podaniem nieprawidłowego numeru rachunku 3/3

Rzecznik Finansowy
www.rf.gov.pl

- W przypadku autoryzacji zlecenia i wykonania na rachunek odbiorcy zgodnie z wskazanym w zleceniu identyfikatorem **odpowiedzialność dostawcy jest wyłączona**.
- Dzieje się tak nawet, jeżeli intencją płatnika było wskazanie innego numeru (mówi o tym art. 143 ust. 2 ustawy).
- **Dla płatnika oznacza to w zasadzie brak możliwości dochodzenia roszczeń od dostawcy.**

Nowelizacja ustawy o usługach płatniczych

Rzecznik Finansowy
www.rf.gov.pl

W związku z pojawiającymi się nowymi zagrożeniami z inicjatywy Rzecznika Finansowego podjęte zostały prace nad nowelizacją ustawy o usługach płatniczych. Ustawa została już podpisana i opublikowana w Dzienniku Ustaw 10 maja 2018 r. (Dz.U. 2018, poz. 864).

Celami zmian było:

1. Wprowadzenie szczegółowej procedury, określającej jakie działania powinni podjąć dostawcy w przypadku **transakcji wykonanej z użyciem nieprawidłowego unikatowego identyfikatora**.
2. Doprecyzowanie, że działania w celu odzyskania kwoty transakcji płatniczej wykonanej obowiązani są **zarówno dostawca płatnika, jak również dostawca odbiorcy.**
3. 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.**

OMYŁKOWY PRZELEW NA ZŁE KONTO?

Zobacz jak wygląda procedura zwrotu pieniędzy.

Rzecznik Finansowy
www.rf.gov.pl

KLIENT (PŁATNIK) ZGŁASZA → wykonanie omyłkowego przelewu do swojego banku lub SKOK-u (tzw. dostawcy płatnika)

3 dni – tyle czasu od otrzymania informacji ma bank lub SKOK prowadzący rachunek odbiorcy na poinformowanie odbiorcy o błędzie i konsekwencjach braku zwrotu w ciągu 30 dni.

*Jeśli poinformowana instytucja **nie prowadzi** rachunku odbiorcy informuje bank lub SKOK odbiorcy. Ten podejmuje analogiczne działania.*

ODBIORCA ZWRACA PIENIĄDZE

NA SPECJALNY RACHUNEK TECHNICZNY.
MA ZAPEWNIONĄ PEŁNĄ ANONIMOWOŚĆ!

PŁATNIK OTRZYMUJE ZWROT ŚRODKÓW
W CIĄGU 1 - 2 DNI ROBOCZYCH.

BRAK ZWROTU W CIĄGU 30 DNI

BANK LUB SKOK JEST ZOBOWIĄZANY DO
PRZEKAZANIA PŁATNIKOWI DANYCH ODBIORCY.

PŁATNIK MA MOŻLIWOŚĆ ZŁOŻENIA POZWU W SĄDZIE
POWOŁUJĄC SIĘ NA **BEZPODSTAWNE WZBOGACENIE ODBIORCY.**

Odbiorca omyłkowego przelewu zwracający pieniądze nigdy nie poniesie żadnych kosztów. Płatnik, który zlecił przelew, może być obciążony kosztami całej operacji.

Rzecznik Finansowy
www.rf.gov.pl

Dziękuję za uwagę!

www.rf.gov.pl
biuro@rf.gov.pl
facebook.com/@RzecznikFinansowy