Rozprawy Ubezpieczeniowe. Konsument na rynku usług finansowych nr 31 (1/2019): 17-32
Journal of Insurance, Financial Markets and Consumer Protection No. 31 (1/2019): 17-32
DOI: 10.32078/JOIN.31.02

Postrzeganie bezpieczeństwa korzystania z usług bankowych w segmencie osób młodych

Mateusz FILIPIAK[1]
Uniwersytet Ekonomiczny w Poznaniu

Złożono: 12 kwietnia 2018; Zaakceptowano do druku: 12 maja 2019; Opublikowano: 28 czerwca 2019

Streszczenie. Otoczenie technologiczne instytucji finansowych zmienia się w bardzo szybkim tempie, co zarazem związane jest z pojawieniem się nowych zagrożeń, m.in. terroryzmu, cyberprzestępstw czy wirusów komputerowych. Klienci banków wymagają nie tylko prywatności oraz komfortu użytkowania, ale przede wszystkim chcą mieć pewność, że ich oszczędności chronione są według najwyższych standardów. Celem artykułu jest ocena znajomości i przestrzegania zasad bezpiecznego korzystania z wybranych usług bankowych przez studentów. W publikacji wykorzystano wyniki badań własnych przeprowadzonych w 2017 r. wśród 274 studentów publicznych szkół wyższych w Poznaniu. Scharakteryzowano czynniki, na które zwracają uwagę klienci podczas korzystania z usług bankowych, tak by ich fundusze były bezpieczne, a także postawy wobec biometrii i innych sposobów zabezpieczeń.

Słowa kluczowe: bankowość mobilna, bankowość internetowa, ochrona konsumenta.
Kody JEL: G210, D18.

1. Wstęp

Nowoczesne technologie stają się niezbędne do rozwoju i unowocześniania instytucji bankowych, a także innych przedsiębiorstw. Rynek urządzeń typu smartfon rośnie w bardzo szybkim tempie. Wymogi i oczekiwania formułowane wobec urządzeń mobilnych znajdują odzwierciedlenie w pragnieniach i wymaganiach klientów banków żywionych względem usług świadczonych przez instytucje depozytowo-kredytowe. Należy jednak pamiętać, że rozwój nowoczesnych technologii powiązany jest ściśle z zagrożeniami, głównie zaś z cyberprzestępczością. Zatem na pierwszy plan wysuwają się nie wygoda związana z szybkimi płatnościami, a bezpieczeństwo transakcji. Klienci banków pragną, aby ich pieniądze były chronione zgodnie z najwyższymi standardami, przy zachowaniu prywatności oraz komfortu użytkowania.

[1] Kontakt z autorem: Mateusz Filipiak, e-mail: mateuszfilipiak@onet.pl.

Celem artykułu jest ocena znajomości i przestrzegania zasad bezpiecznego korzystania z wybranych usług bankowych przez studentów. W publikacji wykorzystane zostały wyniki badań własnych przeprowadzonych w 2017 r. wśród 274 studentów publicznych szkół wyższych w Poznaniu. Scharakteryzowane zostały czynniki, na które zwracają uwagę klienci podczas korzystania z innowacyjnych usług bankowych, tak by ich fundusze były bezpieczne, a także postawy wobec biometrii i innych sposobów zabezpieczeń.

2. Bezpieczeństwo podczas korzystania z usług bankowych

2.1. Potrzeba bezpieczeństwa finansowego

W potocznym rozumieniu bezpieczeństwo jest utożsamiane ze stanem zapewniającym pewność istnienia i przetrwania. *Słownik współczesnego języka polskiego* definiuje to słowo jako „poczucie pewności; przeciwieństwo zagrożenia" [Dunaj *et al.* 1999, s. 50]. Natomiast najogólniej i najtrafniej określić należy bezpieczeństwo jako „zaspokajanie takich potrzeb jak: istnienie, przetrwanie, całość, tożsamość, niezależność, spokój, posiadanie i pewność rozwoju" [Zięba 1999, s. 27]. Warto dodać, że Światowe Forum Ekonomiczne zdefiniowało zagrożenia bezpieczeństwa w pięciu kategoriach: ryzyko gospodarcze, ryzyko geopolityczne, ryzyko dla środowiska, ryzyko społeczne, ryzyko technologiczne [Schwab 2011]. W niniejszym opracowaniu zostaną omówione głównie ryzyko ekonomiczne (w szczególności finansowe) oraz ryzyko technologiczne.

Bezpieczeństwo finansowe jest określane jako „stan osób, gospodarstw domowych oraz społeczności, które są w stanie pokryć swoje podstawowe potrzeby i nieuniknione wydatki w sposób zrównoważony, biorąc pod uwagę wymagania fizjologiczne, środowiska i obowiązujące normy kulturowe" [Raczkowski 2012, s. 299–300]. Jest o zarazem pojęcie wielowymiarowe, dotyczy bowiem wszystkich podmiotów działających na rynkach finansowych – od instytucji państwowych zaczynając, poprzez pośredników finansowych, kończąc na klientach indywidualnych i instytucjonalnych.

Na bezpieczeństwo finansowe jednostki wpływa jej zachowanie. Niepodważalnym faktem jest, że wraz ze wzrostem wiedzy ekonomicznej, poznaniem podstawowych pojęć i umiejętnością ich wykorzystywania zwiększa się poczucie bezpieczeństwa [Raczkowski 2012, s. 300]. Poczucie bezpieczeństwa finansowego jednostki zależne jest również od stabilności rynków finansowych, koniunktury gospodarki danego kraju czy też od wiedzy oraz umiejętności menedżerów i polityków. Trudno sobie wyobrazić, by klienci banków, pomimo swoich wysokich dochodów, czuli się bezpiecznie, gdyby panował światowy kryzys, a politycy i prezesi banków byli osobami niekompetentnymi. Ograniczanie ryzyka finansowego możliwe jest dzięki działaniom prewencyjnym. Odpowiednie przepisy zawarte w aktach prawnych, między innymi o adekwatności kapitałowej banków, czy też tworzenie instytucji odpowiedzialnych za kontrolę rynku finansowego, takiej jak na przykład Komisja

Nadzoru Finansowego, powodują podwyższenie poczucia bezpieczeństwa finansowego jednostki.

Rozwijający się rynek nowoczesnych technologii przyczynia się do wprowadzania innowacji na rynku usług bankowych. Klienci banków niechętnie przekonują się do korzystania z nowinek technicznych, nie darzą ich zaufaniem, ponieważ obawiają się o bezpieczeństwo swoich pieniędzy. Jak wynika z raportu Fundacji Kronenberga zaledwie 52% badanych deklaruje zaufanie do nowoczesnych kanałów obsługi w banku. Usługi takie jak bankowość mobilna i internetowa największym zaufaniem cieszą się wśród osób z wyższym wykształceniem (72%), najmniejszym zaś u osób z wykształceniem podstawowym (32%). Warto zwrócić uwagę na to, że poczucie bezpieczeństwa wobec nowoczesnych usług bankowych jest tym większe, im wyższe wykształcenie posiada klient banku [Fundacja Kronenberga 2015]. Jednak wyniki podobnych badań na przestrzeni lat ulegają zmianom, a działania podejmowane przez banki w zakresie ochrony konsumentów przynoszą wymierne korzyści. Według najnowszego raportu Związku Banków Polskich aż 91% Polaków czuje się bezpiecznie podczas korzystania z bankowości mobilnej i internetowej [Barbrich, Minkina, Polak 2018, s. 7].

To, że klienci banków przykładają dużą wagę do kwestii bezpieczeństwa, potwierdza również systematyczne badanie bankowców przez „Monitor Bankowy". Wynika z niego, iż w latach 2014–2016 zwiększył się odsetek bankowców twierdzących, że klientów gotowych na korzystanie z bankowości mobilnej jest więcej niż 40%, ale główną barierą rozwoju e-gospodarki są obawy konsumentów o bezpieczeństwo – na tę przeszkodę wskazało 43% osób [Minkina 2016].

2.2. Rodzaje zabezpieczeń stosowanych przez banki

Instytucje depozytowo-kredytowe starają się każdego dnia ulepszać system zabezpieczeń danych swoich klientów. Świadczenie usług poprzez różne kanały dystrybucji (stacjonarny, internetowy i mobilny) stwarza wiele możliwości dla potencjalnych oszustów, dlatego banki starają się przewidzieć, w jaki sposób konsument może zostać okradziony. Wiedza zdobyta dzięki profesjonalnym oddziałom IT, które nieustannie analizują to ryzyko, przyczynia się do udoskonalenia bezpieczeństwa klientów korzystających z usług w oddziale banku oraz z możliwości bankowości internetowej i mobilnej.

Konsumenci narażeni są na: niekontrolowane udostępnienie ich danych osobowych z zasobów banku, włamanie się na internetowy rachunek bankowy, kradzież danych z karty płatniczej, kradzież tożsamości czy też oszustwa podczas płatności elektronicznych. Bankowcy uważają, że ich systemy dobrze chronią przed tego typu zagrożeniami. Najwyżej oceniają bezpieczeństwo w zakresie ochrony danych osobowych w placówkach banków (96%) oraz zapobieganie włamaniom na internetowe konta bankowe (94%). W ich opinii instytucje depozytowo-kredytowe mają jednak jeszcze dużo do zrobienia w zakresie czasowych awarii w bankowości elektronicznej oraz kradzieży danych karty płatniczej [Barbrich, Minkina, Polak 2018, s. 16].

Tabela 1. Rodzaje zabezpieczeń stosowanych w usługach bankowych

Usługa bankowa	Sposób uwierzytelniania	Dodatkowe zabezpieczenia
Wypłaty w oddziale banku	dowód osobisty wzór podpisu dane osobowe (np. nazwisko panieńskie matki)	monitoring
Bankomat	PIN kod BLIK czytnik linii papilarnych[2]	montowanie plastikowych wypustek wokół otworu na kartę kamera moduł EMV[3] limity transakcji
Płatności kartą bankomatową	PIN	kod CVC2/CVV2[4] odpowiedzialność posiadacza karty do równowartości 150 euro limity transakcji
Bankowość internetowa	login hasło maskowane dwustopniowy model (dodatkowo kilka cyfr z numerem PESEL bądź dowodu osobistego)	szyfrowanie połączenia z bankiem certyfikat klucza publicznego[5] jednorazowe hasła SMS podczas płatności limity transakcji
Bankowość mobilna	login hasło maskowane dwustopniowy model (dodatkowo kilka cyfr z numerem PESEL bądź dowodu osobistego) skanowanie odcisku palca	jednorazowe hasła SMS podczas płatności uaktualnianie aplikacji mobilnej limity transakcji
Płatności telefonem przy użyciu systemu BLIK	dwustopniowy (jednorazowy kod oraz zaakceptowanie płatności przy użyciu aplikacji mobilnej)	aplikacja mobilna zabezpieczona loginem i hasłem lub też poprzez skanowanie odcisku palca

Źródło: opracowanie własne na podstawie m.in. [Górnisiewicz, Obczyński, Pstruś 2014].

Banki świadczą usługi tradycyjne, do których należy zaliczyć wpłaty i wypłaty w oddziale banku i bankomacie, ale także usługi nowoczesne, takie jak bankowość mobilna, bankowość internetowa, płatności zbliżeniowe kartą bankomatową oraz płatności telefonem, np. system BLIK. Tabela 1 prezentuje, w jaki sposób klienci chronieni są przed atakami oszustów, gdy korzystają z tych usług.

[2] Rozwiązanie to jest nadal w fazie testowej.

[3] Moduł EMV – standard opracowany przez zrzeszenie wydawców kart płatniczych Europay, MasterCard i Visa, definiujący zasady współpracy kart płatniczych wyposażonych w chip (tzw. chip EMV) z innymi urządzeniami, takimi jak terminale płatnicze i bankomaty [Górnisiewicz, Obczyński, Pstruś 2014, s. 7].

[4] Kod CVC2/CVV2 – kod zapisany na odwrocie karty płatniczej pozwalający – wraz z numerem karty, datą jej ważności oraz danymi posiadacza karty – na przeprowadzenie transakcji typu card-not-present [Górnisiewicz, Obczyński, Pstruś 2014, s. 7].

[5] Certyfikat klucza publicznego – zestaw informacji, które zasadniczo nie są możliwe do podrobienia i służą do weryfikacji tożsamości podmiotu w internecie [Górnisiewicz, Obczyński, Pstruś 2014, s. 7].

Wymienione zabezpieczenia stosowane przez banki ulegają ciągłej ewolucji. Wyjątkową pozycję wśród bankowych technologii zabezpieczeniowych zajmuje obecnie biometria. Technika opierająca się na indywidualnych cechach istot żywych jest wykorzystywana przez instytucje depozytowo-kredytowe już od kilkunastu lat. Technologie biometryczne używane są w siedzibach banków na różnych poziomach zabezpieczeń, będą to m.in.: skan tęczówki oka, geometria twarzy, geometria dłoni, odcisk palca, rejestracja głosu [Jasiński 2007, s. 81].

Identyfikację biometryczną banki starają się wprowadzić również na użytek komercyjny, aby klienci czuli się bezpiecznie. Jednak największą trudnością we wdrożeniu tej techniki jest brak bazy obejmującej wzorce biometryczne. Niektóre banki już świadczą tego typu usługi swoim klientom; głównie polegają one na logowaniu się do aplikacji mobilnej przy użyciu skanowania odcisku palca. Możliwość taką swoim klientom proponuje jedynie 10 banków w Polsce (stan na dzień 10 marca 2018 r.). Przykładowo potwierdzenie transakcji przy użyciu skanowania odcisku palca oferuje Bank Millennium, z kolei Bank Zachodni BZ WBK w ramach swojej infolinii wykorzystuje system biometrii głosowej. Poza tym warto wspomnieć o projekcie badawczym banku PKO BP, Politechniki Gdańskiej oraz firmy Microsystems, polegającym na wprowadzeniu globalnego rozwiązania z zakresu biometrii. W wybranych placówkach PKO BP województwa kujawsko-pomorskiego i pomorskiego klienci mogą skorzystać z biostanowisk, które weryfikują tożsamość poprzez cechy szczególne, takie jak skan naczyń krwionośnych dłoni i twarzy, podpis czy głos [Boczoń 2017].

Klienci europejskich banków chcą, by ich pieniądze były bezpieczne, dlatego większość z nich (67%) rozumie znaczenie poufnych danych w procesie ochrony prywatności. Wśród klientów banków wzrasta również zainteresowanie i chęć uwierzytelniania płatności z wykorzystaniem biometrii. Dwuetapowe uwierzytelnianie jest uznawane przez trzy czwarte badanych jako bezpieczny sposób autoryzacji płatności. Największym zaufaniem klienci banków darzą weryfikację linii papilarnych (81%) i skanowanie tęczówki oka (76%) [Ziemkowska 2016, s. 35–39].

Polacy oczekują, że banki niezwłocznie będą ich informować o zaistnieniu i skutkach cyberataku oraz że od razu zostaną wprowadzone procedury eliminujące takie zagrożenie. Taką deklarację złożyło 83% badanych [Barbrich, Minkina, Polak 2018, s. 13], co pokazuje, jak wysokim zaufaniem klienci darzą banki i przerzucają na nie pełną odpowiedzialność za bezpieczeństwo. Jednak rola banków w zakresie ochrony danych osobowych i funduszy konsumentów nie kończy się tylko na trosce o systemy zabezpieczeń. Bankowcy twierdzą, iż przy korzystaniu z niektórych usług duża odpowiedzialność spoczywa również na klientach. Dlatego zadaniem banku jest także edukowanie konsumentów w zakresie potencjalnych zagrożeń oraz metod ich zwalczania. Przykładem takich działań jest uczestnictwo instytucji depozytowo-kredytowych w ogólnopolskim programie „Bezpieczeństwo w cyberprzestrzeni", w ramach którego w placówkach oświatowych przeprowadzane są zajęcia z zakresu cyberbezpieczeństwa [Barbrich, Minkina, Polak 2018, s. 16–17].

2.3. Bezpieczeństwo z perspektywy klientów banków

Wiedza Polaków z zakresu bezpieczeństwa usług bankowych jest tematem wielu badań. Z tych najnowszych wynika, że 37% obywateli Rzeczypospolitej nie ma pojęcia o bezpieczeństwie bankowości mobilnej, a 30% o bankowości internetowej. Z kolei Polacy wiedzą znacznie więcej o ochronie tak usług bankowych w placówce banku, jak i bankomatów. Brak wiedzy w tej sferze wykazało odpowiednio 16% i 17% badanych [Barbrich, Minkina, Polak 2018, s. 9–11].

Poziom wiedzy z zakresu bezpieczeństwa w sieci w Polsce jest na takim samym poziomie jak w całej Unii Europejskiej (46%). Najlepiej poinformowani w tej dziedzinie są mieszkańcy Danii (76%), a największe braki wiedzy występują wśród Bułgarów (27%). Co ciekawe, to właśnie w Bułgarii obywatele uważają, że rośnie ryzyko stania się ofiarą cyberataku (87%), w Polsce podobnie sądzi 82% badanych [Barbrich, Minkina, Polak 2018, s. 12].

Mimo iż banki starają się (skutecznie) zapobiegać atakom oszustów posługujących się metodą nazywaną phishing[6], to klient musi wykorzystywać wiedzę z zakresu cyberbezpieczeństwa i przestrzegać podstawowych zasad podczas korzystania z usług bankowości internetowej. Przede wszystkim nigdy nie należy podawać żadnych danych niezbędnych w procesie logowania do bankowości internetowej osobom trzecim, a wejście do serwisu bankowości internetowej powinno odbywać się wyłącznie poprzez wpisanie odpowiedniego adresu w pasku przeglądarki. Dodatkowo przed zalogowaniem należy sprawdzić, czy połączenie z bankiem jest szyfrowane, to znaczy, czy przed adresem znajduje się przedrostek „https://" (a nie „http://"), a obok niego umieszczony jest symbol kłódki. Należy również kliknąć ten symbol i sprawdzić poprawność certyfikatu klucza publicznego [Górnisiewicz, Obczyński, Pstruś 2014, s. 19]. Niestety, zaledwie co czwarty Polak podczas korzystania z bankowości internetowej zwraca uwagę na wymienione aspekty [Barbrich, Minkina, Polak 2018, s. 20].

Celem ataków hakerskich są również komputery i inne urządzenia klientów banków służące do korzystania z bankowości internetowej. Przed takowymi atakami można się uchronić, należy jednak pamiętać o kilku podstawowych zasadach bezpieczeństwa. Zaleca się łączenie z bankowością internetową tylko poprzez zaufane urządzenia, nie należy natomiast korzystać w tym celu z kafejek internetowych bądź publicznie dostępnych hot-spotów[7], gdyż może być tam zainstalowane złośliwe oprogramowanie. Urządzenia, z których korzystają klienci banków do używania bankowości internetowej, powinny być zabezpieczone najnowszym oprogramowaniem antywirusowym oraz zaporą sieciową[8]. Zainstalowany i aktualizowany

[6] Phishing – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub organizację w celu wyłudzenia określonych informacji (np. danych niezbędnych do logowania się do bankowości internetowej) lub nakłonienia ofiary do realizacji określonych zadań [Górnisiewicz, Obczyński, Pstruś 2014, s. 7].

[7] Hot-spot – punkt dostępu do sieci bezprzewodowej, umożliwiający podłączonym do niego urządzeniom dostęp do internetu [Górnisiewicz, Obczyński, Pstruś 2014, s. 7].

[8] Zapora sieciowa (ang. *firewall*) – oprogramowanie lub urządzenie służące do kontrolowania przepływu danych do i z danego urządzenia (np. komputera) [Górnisiewicz, Obczyński, Pstruś 2014, s. 7].

program antywirusowy posiada zaledwie 21% Polaków [Barbrich, Minkina, Polak 2018, s. 19]. Użytkownicy muszą także pamiętać, aby nie instalować nielegalnego oprogramowania na swoich urządzeniach, gdyż może być to bardzo ryzykowne [Górnisiewicz, Obczyński, Pstruś 2014, s. 19–22].

Bankowość internetowa zabezpieczona jest odpowiednim loginem i hasłem. Hasło powinno być trudne, najlepiej winno zawierać znaki specjalne, dużą literę i liczby, oraz powinno być zmieniane z określoną częstotliwością. Obowiązek zmiany hasła spoczywa na użytkownikach, aczkolwiek banki starają się zmuszać co jakiś czas swoich klientów do utworzenia nowego hasła. Badania pokazują, że w Polsce zaledwie 30% osób zmieniło hasło w ciągu ostatnich 12 miesięcy – podobnie pod tym względem kształtuje się średnia w Unii Europejskiej. Najczęściej czynią to Łotysze (68%), najrzadziej zaś Rumuni (7%). Ponadto warto zwrócić uwagę, iż w Polsce aż 84% populacji używa takiego samego hasła do różnych stron internetowych, podczas gdy w krajach Unii Europejskiej przeciętnie jest to 72%. Najlepiej pod tym względem prezentują się Szwedzi (40%), a najgorzej Bułgarzy (87%) [ZBP 2018, s. 14].

Podczas korzystania z oferty sklepów internetowych płatności za zakupy da się zrealizować przy użyciu karty płatniczej. Można tego dokonać, podając dane z karty: jej numer, datę ważności, dane posiadacza oraz specjalny kod CVC2/CVV2 umieszczony na odwrocie karty. Ten trzycyfrowy kod jest jednym z systemów zabezpieczeń kart płatniczych stosowanym przez banki. Jednak w niektórych krajach na świecie kod ten nie jest wymagany podczas autoryzacji płatności. Potwierdza to historia pewnej kobiety, która po przejściu huraganu w USA otrzymała kartę płatniczą z Czerwonego Krzyża, następnie jej zdjęcie zamieściła na portalu społecznościowym. W ciągu kilku minut z jej konta zniknęły wszystkie środki pieniężne [Górnisiewicz, Obczyński, Pstruś 2014, s. 28–31]. Klienci banków muszą zatem zachować szczególną ostrożność i pamiętać, żeby nie umieszczać poufnych danych w internecie, gdyż opublikowane w tym miejscu informacje pozostają tam na zawsze.

Chociaż bezpieczne korzystanie z mobilnych aplikacji bankowych jest możliwe dzięki dwustopniowemu poziomowi zabezpieczeń, cyberprzestępcy nadal znajdują sposoby na dokonywanie kradzieży, głównie dzięki smartfonom i tabletom końcowych użytkowników. Na ataki najbardziej narażone są osoby korzystające z systemu operacyjnego Android. Liczba „złośliwych plików" przygotowanych dla tego systemu stale rośnie. Pod koniec III kwartału 2015 r. odnotowano ich blisko 1,6 mln [Piesik 2016]. Niebezpieczne jest ponadto instalowanie aplikacji z nieznanych źródeł, może to doprowadzić do infekcji urządzenia. Jednym z przykładów jest trojan Zeus, który udaje certyfikat do wykonywania przelewów, w rzeczywistości jednak kradnie SMS-y zawierające jednorazowe kody wysyłane przez banki. Inny niebezpieczny trojan o nazwie Android.BankBot.65.origin został stworzony do wykradania pieniędzy z kont bankowych, a wbudowany był m.in. w aplikację rosyjskiego państwowego Sbierbanku [Piesik 2016, s. 100–103].

3. Metodyka badań własnych

Celem określenia poziomu wiedzy na temat bezpieczeństwa wybranych usług bankowych oraz stopnia przestrzegania przez studentów podstawowych zasad bezpiecznego korzystania z tych usług przeprowadzone zostało autorskie badanie ilościowe – metodą ankiety internetowej – wśród studentów publicznych szkół wyższych w Poznaniu korzystających z wybranych usług bankowych.

Sformułowano hipotezę główną, według której w przypadku studentów Uniwersytetu Ekonomicznego w Poznaniu występuje większa znajomość zasad bezpiecznego korzystania z bankowości oraz częstsze przestrzeganie tych zasad niż wśród studentów pozostałych publicznych uczelni wyższych w Poznaniu.

W badaniu wzięło udział 274 studentów. Połowa próby, czyli 137 osób, to studenci Uniwersytetu Ekonomicznego w Poznaniu. Pozostałe osoby studiują na innych publicznych uczelniach w Poznaniu (w tym 69 studentów Uniwersytetu im. Adama Mickiewicza, 32 studentów Politechniki Poznańskiej, 18 studentów Uniwersytetu Przyrodniczego, 11 studentów Uniwersytetu Medycznego i 7 studentów Akademii Wychowania Fizycznego). W większości na pytania odpowiadały kobiety (75%). W badaniu wzięli udział respondenci w różnym wieku, największą grupę stanowiły osoby z pierwszego roku studiów – 28%, potem z trzeciego – 26% i drugiego roku studiów licencjackich – 18%, pozostali to studenci studiów magisterskich.

Badanie zostało przeprowadzone w dniach 14 i 15 marca 2017 r. Respondenci odpowiedzieli na 38 pytań zamieszczonych w ankiecie udostępnionej na platformie internetowej Google. Do analizy danych wykorzystano głównie miary statystyki opisowej. Do przetworzenia danych wykorzystano program IBM SPSS Statistics oraz arkusz kalkulacyjny Microsoft Excel. Ankieta internetowa został zamieszczona na portalu społecznościowym w zamkniętych grupach studentów poszczególnych uczelni w Poznaniu.

Wśród respondentów nie znalazła się ani jedna osoba, która nie posiada konta w banku i nie korzysta z bankowości internetowej. Natomiast mobilnymi aplikacjami swoich banków nie posługuje się 34,3% badanych. Ankieta została skonstruowana w taki sposób, by osoby, które nie używają mobilnej bankowości, nie odpowiadały na pytania dotyczące bezpieczeństwa oraz wygody tej usługi. Dlatego w zagadnieniach związanych z mobilną bankowością próba wyniosła 217 respondentów. Poza tym warto podkreślić, iż studenci częściej i bardziej świadomie korzystają z internetu niż przedstawiciele innych grup społecznych, co może mieć swoje odzwierciedlenie w wynikach badania. Ponadto rezultatów niniejszego badania nie należy uogólniać na populację, gdyż próba nie była dobrana w sposób losowy. Niniejsza analiza stanowi raczej wstęp do poznania omawianego zjawiska.

4. Postrzeganie aspektu bezpieczeństwa podczas korzystania z bankowości

4.1. Znajomość i przestrzeganie zasad bezpiecznego korzystania z wybranych usług bankowych

Jako jeden z głównych powodów, dla których wciąż duża liczba studentów nie decyduje się na korzystanie z nowoczesnych usług bankowych (bankowości mobilnej nie używa nieco ponad 34% badanych), zostało wymienione ograniczone bezpieczeństwo. Powszechne jest bowiem twierdzenie, iż usługi tego typu nie są odpowiednio zabezpieczone przed oszustami. Warto podkreślić, że studenci przywiązują dużą wagę do tego, by ich fundusze były bezpieczne – zdecydowana większość potrafi wymienić podstawowe zasady bezpiecznego korzystania z bankomatu, bankowości mobilnej i internetowej.

Podczas wpłacania i wypłacania pieniędzy z bankomatu najczęściej uwagę studentów przykuwa wygląd bankomatu, czyli to, czy nie ma na nim zainstalowanych nakładek na klawiaturę, czytnika kart lub dodatkowych kamer zamontowanych przez oszustów (co trzecie wskazanie). Równie istotną zasadą bezpieczeństwa, jaką kierują się młodzi ludzie, jest zwracanie uwagi na inne osoby w pobliżu bankomatu (33%). Kolejny istotny czynnik to lokalizacja bankomatu. Badani przyznają, że najczęściej korzystają z bankomatów umieszczonych przy oddziałach banku, natomiast obawiają się używania tych znajdujących się w miejscach nietypowych. Co ciekawe, jedynie 17% młodych ludzi podczas wpisywania kodu PIN zasłania klawiaturę ręką. Warto zwrócić uwagę, że studenci wszystkich uczelni porównywalnie dobrze poradzili sobie z wymienieniem podstawowych zasad bezpiecznego korzystania z bankomatu. Wiedzę w tym zakresie posiadało 96% studentów UEP i 92% studentów pozostałych uczelni.

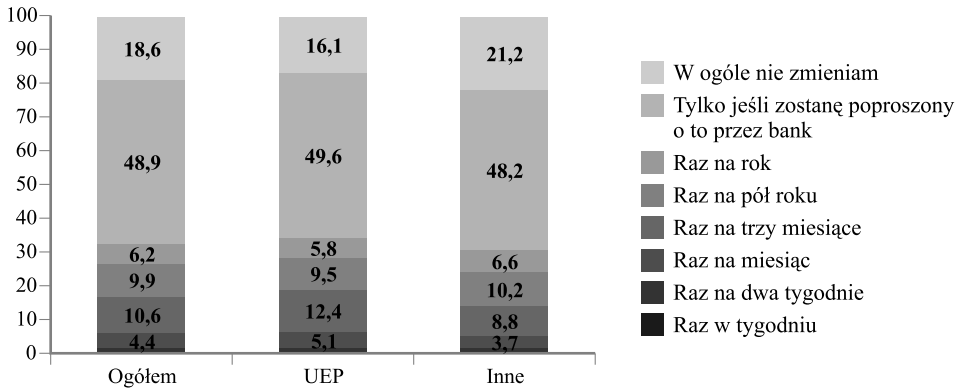
Podobne wyniki otrzymano także w zakresie zasad bezpiecznego korzystania z bankowości internetowej. Zdecydowana większość studentów w obydwu analizowanych grupach (UEP – 93%, pozostali – 81%) posiada wiedzę co do zasad bezpieczeństwa i nie występują w tym zakresie znaczące różnice pomiędzy grupami badanych. Poza tym tylko niespełna 5% osób nie wie, na co zwracać uwagę podczas korzystania z tej usługi, a zaledwie 8% nie koncentruje się na niczym, gdyż uważa bankowość internetową za całkowicie bezpieczną. Co trzeci student deklaruje, że sprawdza, czy strona internetowa posiada odpowiedni certyfikat, czy przed adresem witryny znajduje się „https" oraz widnieje ikona kłódki. Oprócz tego podczas korzystania z tej usługi bankowej 16% zwraca szczególną uwagę na odpowiednie zalogowanie oraz wylogowanie, natomiast 13% korzysta tylko z zaufanych sieci internetowych. Niestety, jedynie 5% młodych ludzi dba o to, by posiadać najnowszą wersję programu antywirusowego.

Z bankowości mobilnej korzysta dwie trzecie ankietowanych. Niestety, wśród nich aż 14% używa aplikacji bankowej bez podstawowej wiedzy na temat bezpieczeństwa tej usługi. Natomiast dla co trzeciego studenta ważne jest, z jakiej sieci internetowej korzysta (czy jest to sieć publicznie dostępna, czy domowa) oraz z jakim urządze-

niem się posługuje (czy jest to urządzenie z systemem Android, czy iOS). Bardzo wiele osób (58%) przyznaje, że gdy są połączeni z internetem dostępnym publicznie, to unikają posługiwania się bankową aplikacją mobilną. Oprócz tego co czwarty student zwraca uwagę na otoczenie, czyli czy ktoś za nim nie stoi, czy ludzie wokół nie wzbudzają podejrzeń. Stosunkowo często młodzi ludzie twierdzą, że aplikacja powinna być zabezpieczona trudnym hasłem, a podczas jego wpisywania nikt nie powinien zaglądać przez ramię. Natomiast 7% studentów zwraca uwagę także na to, by zawsze po skorzystaniu z bankowej aplikacji mobilnej odpowiednio się wylogować. W przypadku wiedzy dotyczącej zasad bezpiecznego korzystania z tej usługi ponownie studenci nie różnią się między sobą (82% UEP *vs.* 78% inne uczelnie).

Celem badania było także określenie postrzegania bezpieczeństwa bankowości mobilnej. Sprawdzono, z którego systemu operacyjnego najczęściej korzystają studenci oraz który system operacyjny ich zdaniem najlepiej chroni przed atakami hakerów. Zgodnie z przewidywaniami najliczniejsi są użytkownicy Androida (78%), następnie iOS (15%), natomiast najmniej osób posiada system Windows Phone (3%). Niestety, jeśli chodzi o wiedzę na temat bezpiecznego oprogramowania na smartfony, to jej poziom nie jest zadowalający. Wyniki badania wskazują, że aż 62% osób nie wie, który system zapewnia największe bezpieczeństwo. Natomiast 22% poprawnie wskazuje na iOS, a co dziesiąty student twierdzi, że jest nim Android (oprogramowanie, w przypadku którego hakerzy mają najwięcej możliwości). Co ciekawe, najbardziej pewni swojej wiedzy na temat bezpiecznych systemów operacyjnych są posiadacze iOS, gdyż aż w 56% wskazali oni, że ich system najlepiej chroni przed złośliwym oprogramowaniem.

Wykres 1. Częstość zmieniania hasła używanego w bankowości mobilnej i internetowej wśród studentów według uczelni



Źródło: Opracowanie własne na podstawie przeprowadzonych badań.

Częstotliwość zmieniania haseł używanych w bankowości internetowej i mobilnej przez studentów wydaje się niepokojąca (wykres 1). Niemal połowa zabezpiecza swoje konto nowym hasłem tylko wówczas, gdy zostanie o to poproszona przez

bank, z usług którego korzysta. Natomiast prawie co piąty student nie zmienia hasła w ogóle, a co dziesiąty czyni to raz na trzy miesiące. Przyczyn tak rzadkiej zmiany zabezpieczeń można doszukiwać się w fakcie, iż wielu studentów w obecnych czasach staje przed koniecznością zapamiętywania wielu haseł do różnych kont, na przykład wirtualnego dziekanatu, poczty elektronicznej czy też serwisu filmów wideo. Co ciekawe, co piąty studiujący na pozostałych uczelniach nie zmienia zabezpieczeń swojego konta w ogóle.

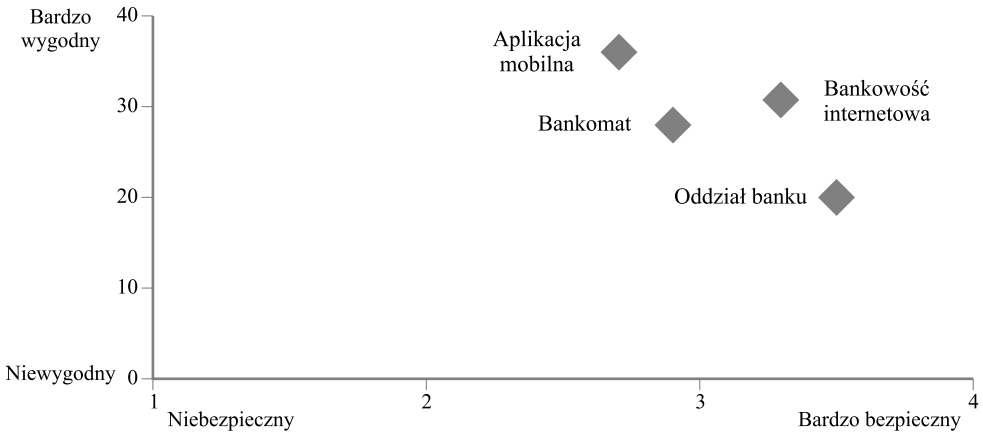
Zapamiętanie kodu PIN karty płatniczej nie sprawia trudności 96% ankietowanych. Interesujące jest, że częściej problem z tym mają kobiety oraz osoby studiujące na pozostałych uczelniach (UEP – 1%, inne – 6%). Natomiast co dziesiąty badany stosuje taki sam kod PIN także do odblokowywania innych kont bądź aplikacji.

Weryfikacji poddano również lęk przed utratą karty bankomatowej i dowodu osobistego. Wydawać by się mogło, iż większy niepokój winno budzić widmo kradzieży dowodu osobistego, gdyż dokument ten uprawnia do wzięcia choćby pożyczki gotówkowej o dużo wyższej wartości niż kwota płatności zbliżeniowych realizowanych kartą płatniczą (50 zł). Okazuje się, iż studenci UEP oraz innych uczelni publicznych w Poznaniu w zbliżonym stopniu obawiają się utraty tak dowodu osobistego (69%), jak i karty płatniczej (62%).

4.2. Ocena rodzajów zabezpieczeń stosowanych przez banki

Podczas badania studenci ocenili również bezpieczeństwo korzystania z bankomatów, aplikacji mobilnych, bankowości internetowej oraz usług stacjonarnego oddziału banku. Ponadto wartościowali także wygodę korzystania z tych usług (w skali od 1 do 4, gdzie 1 – niebezpieczny / niewygodny, a 4 – bardzo bezpieczny / bardzo wygodny). Ich opinie przedstawiono na wykresie 2.

Wykres 2. Wygoda a bezpieczeństwo systemów autoryzacji usług bankowych



Źródło: Opracowanie własne na podstawie przeprowadzonych badań.

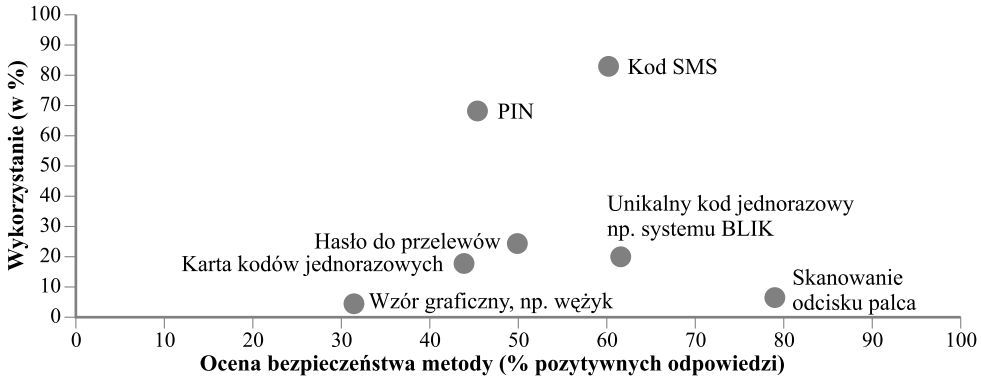
Za najbezpieczniejszy uważany jest oddział banku, zarazem jednak postrzegany jest jako najmniej wygodny. Bankowość internetowa oceniana jest jako stosunkowo bezpieczna i zarazem dość wygodna. Poziom ochrony zastosowany w bankowości mobilnej został oceniony najgorzej.

Otrzymane wyniki badań w dużej mierze pokrywają się z prezentowanymi w poprzedniej części artykułu. Warto przypomnieć, że również bankowcy, oceniając bezpieczeństwo świadczonych usług, najwyżej ocenili usługi świadczone w stacjonarnej placówce banku, podczas gdy za największe zagrożenie uznali czasowe awarie bankowości mobilnej.

Respondenci ocenili poziom bezpieczeństwa poszczególnych sposobów autoryzacji transakcji. Otrzymane wyniki – w kontekście korzystania z poszczególnych sposobów – przedstawiono na wykresie 3. Najczęściej wykorzystywanym sposobem autoryzacji transakcji wśród studentów jest kod SMS, ale to nie ta metoda uważana jest za najbezpieczniejszą. W opinii młodych ludzi za taką należy uważać technologię skanowania odcisku palca. Warto zwrócić uwagę, że kolejna nowość na rynku usług bankowych, czyli autoryzacja za pomocą systemu BLIK, również uważana jest za stosunkowo bezpieczną, mimo to nadal mało osób z niej korzysta. Bardzo częstą metodą wykorzystywaną podczas płatności jest kod PIN, choć w opinii studentów sposób ten znalazł się na trzecim miejscu od końca pod względem bezpieczeństwa.

Uznanie danej metody autoryzacji transakcji za najbezpieczniejszą uzależnione jest od kierunku studiów. Skanowanie odcisku palca jest najbardziej bezpieczne zdaniem osób uczęszczających na Uniwersytet Ekonomiczny, natomiast studenci pozostałych uczelni wskazali na pierwszym miejscu kod SMS (UEP 91% – inne 74%).

Wykres 3. Korzystanie z poszczególnych sposobów autoryzacji transakcji a postrzeganie ich poziomu bezpieczeństwa wśród studentów



Źródło: Opracowanie własne na podstawie przeprowadzonych badań.

Jak wcześniej wspomniano, identyfikacja biometryczna polega na wykorzystaniu informacji biologicznej w celu weryfikacji tożsamości. U podstaw biometrii leży fakt, że ciało każdego człowieka posiada pewne niezmienne oraz niepowtarzalne

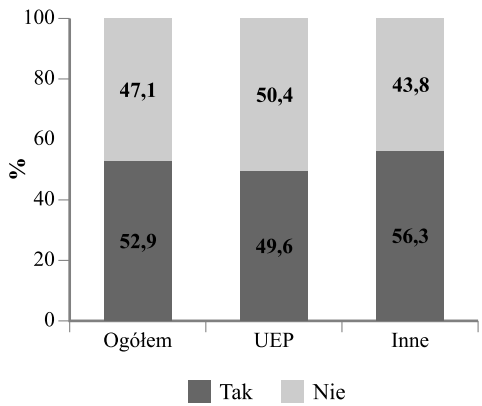
właściwości, które można wykorzystać do odróżnienia jednych osób od drugich, są to przykładowo linie papilarne, układ żył, głos [Kaszubski 2011, s. 5]. Z taką definicją zostali zapoznani respondenci, którzy następnie odpowiedzieli na kilka pytań dotyczących wykorzystania biometrii w usługach bankowych.

Warto przypomnieć, iż metoda autoryzacji płatności z użyciem identyfikacji biometrycznej została uznana przez studentów za najbardziej bezpieczną. Zatem można było spodziewać się, że prawie 87% uważa, iż zastosowanie informacji biologicznej zwiększa bezpieczeństwo systemu bankowego. W tym przypadku studenci wszystkich uczelni byli zgodni: UEP 89% – inne 86%. Należy dodać, iż metodę skanowania odcisku palca w swoim życiu zastosowało do tej pory zaledwie 41% młodych ludzi.

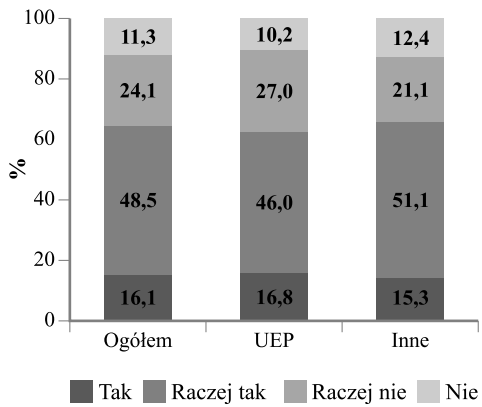
Bardzo interesująco prezentują się także wyniki badań dotyczących chęci skorzystania w przyszłości z autoryzacji płatności wykorzystujących biometrię oraz gotowości powierzenia swoich danych biometrycznych instytucjom bankowym.

Aż 65% studentów zgadza się, by ich odcisk palca znajdował się w bazie klientów banku, jednak zaledwie połowa wyraża chęć skorzystania z biometrii w usługach bankowych. Może to wydawać się trochę sprzeczne, że tak wiele osób jest gotowych do powierzenia swoich danych instytucji depozytowo-kredytowej, choć nie wyrażają oni chęci skorzystania z takiego innowacyjnego systemu płatności. Wykresy 4 i 5 przedstawiają opinie studentów dotyczące tego zagadnienia.

Wykres 4. Chęć skorzystania z systemu płatności opartego na identyfikacji biometrycznej wśród studentów według uczelni



Wykres 5. Gotowość powierzenia swoich danych biometrycznych instytucji bankowej



Źródło: Opracowanie własne na podstawie przeprowadzonych badań.

Analizując wyniki badania, należy stwierdzić, iż do powierzenia swoich danych biometrycznych instytucjom bankowym w jednakowym stopniu skłonne są osoby uczące się na wszystkich uczelniach w Poznaniu (UEP – 63%, inne – 66%).

Zaprezentowane wyniki dają podstawę do twierdzenia, iż identyfikacja biometryczna to dobry i dysponujący potencjałem kierunek rozwoju innowacyjnych i bezpiecznych usług bankowych. Należy jednak pamiętać, że wyrażenie chęci skorzystania z takiego sposobu płatności nie jest równoznaczne z używaniem tej nowości, gdy pojawi się na rynku.

5. Podsumowanie

Z przeprowadzonych analiz wynika, że studenci posiadają stosunkowo dobrą znajomość podstawowych zasad bezpiecznego korzystania z usług bankowych. Warto podkreślić, iż jest to wiedza na poziomie o wiele wyższym od przeciętnego tak w Polsce, jak i w całej Unii Europejskiej.

Znajomość przepisów prawa nie zawsze przekłada się na ich przestrzeganie. Zdecydowana większość osób wie, że nie wolno przechodzić na czerwonym świetle, ale i tak czasem im się to zdarza. Podobnie jest ze znajomością zasad bezpiecznego korzystania z usług bankowych wśród studentów. Bardzo wielu ankietowanych wskazywało, że podstawą zabezpieczenia się przed hakerami jest silne i zmieniane co jakiś czas hasło do konta. Natomiast aż połowa studentów zmienia to hasło tylko wówczas, gdy zostanie o to poproszona przez bank, z usług którego korzystają, a co dziesiąty badany stosuje taki sam kod PIN w zabezpieczeniach do kilku kont. Należy jednak podkreślić, że studenci w tym zakresie ponownie prezentują się znacznie lepiej niż ogół społeczeństwa w Polsce oraz w krajach Unii Europejskiej.

Nie sprawdziła się jednak postawiona w artykule hipoteza główna. Studenci Uniwersytetu Ekonomicznego nie odróżniają się znacząco od studiujących na pozostałych uczelniach publicznych w Poznaniu pod względem posiadanej wiedzy dotyczącej zasad bezpiecznego korzystania z wybranych usług bankowych. Pomimo iż nieco więcej studentów UEP potrafiło wymienić zasady ochrony klienta używającego bankomatu, korzystającego z oferty bankowości mobilnej i internetowej, to jednak różnice w posiadanej wiedzy między studentami z pozostałych uczelni publicznych w Poznaniu nie były tak istotne, by uznać hipotezę główną za prawdziwą.

Należy jednak zwrócić uwagę na ograniczony zakres przeprowadzonych badań (ankieta internetowa została przeprowadzona jedynie wśród studentów uczelni publicznych w Poznaniu). Warto byłoby przebadać populację wszystkich studentów w Polsce – zarówno tych uczących się na uczelniach publicznych, jak i tych korzystających z usług prywatnych szkół wyższych. Ponadto pod uwagę należałoby wziąć osoby młode, które nie studiują, ale korzystają z wybranych usług bankowych. Wówczas takie badania byłyby pełniejsze, a otrzymane wyniki mogłyby stanowić wartościowy przyczynek do dalszych analiz bądź też cenne potwierdzenie poglądów prezentowanych w niniejszym artykule.

Bibliografia

Barbrich P., Minkina P., Polak M., 2018, *Raport ZBP. Cyberbezpieczny portfel*, Związek Banków Polskich, Warszawa.

Boczoń W., 2017, *Biometria w bankowości. Co za jej pomocą załatwimy dziś w banku?,* https://www.bankier.pl/wiadomosc/Biometria-w-bankowosci-Co-za-jej-pomoca-zalatwimy-dzis-w-banku-7542743.html (dostęp: 16.06.2018).

Dunaj B. *et al.*, 1999, *Słownik współczesnego języka polskiego*, t. I, Wilga, Warszawa.

Fundacja Kronenberga, 2015, *Postawy Polaków wobec finansów*, Warszawa.

Górnisiewicz M., Obczyński R., Pstruś M., 2014, *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną*, KNF, Warszawa.

Jasiński A., 2007, *Bank jako ośrodek nowoczesnych technologii. Ewolucja bankowych technik zabezpieczeniowych i ich wpływ na architekturę współczesnych banków,* „Czasopismo Techniczne. Architektura" r. 104, z. 4-A.

Kaszubski R. (red.), 2011, *Prawne aspekty biometrii*, ZBP, Warszawa.

Mikowska M., 2016, *BANK.JEST.MOBI 2016*, TNS Polska, Warszawa.

Minkina P., 2016, *Raport #cyberbezpieczny portfel – zasady bezpieczeństwa*, ZBP, Warszawa.

Piesik L., 2016, *Zmasowany atak na Androida*, „Gazeta Bankowa" nr 2.

Raczkowski K. (red.), 2012, *Bezpieczeństwo ekonomiczne. Wyzwania dla zarządzania państwem*, Wolters Kluwers, Warszawa.

Schwab K., 2011, *The Global Competitiveness Report*, World Economic Forum, http://www3.weforum.org/docs/WEF_GCR_Report_2011-12.pdf (dostęp: 08.05.2017).

Ziemkowska D., 2016, *Skanowanie tęczówki, odcisków palców albo... selfie? Taki będzie kontakt z bankiem*, http://interaktywnie.com/biznes/artykuly/biznes/skanowanie-teczowki-odciskow-palcow-albo-selfie-taki-bedzie-kontakt-z-bankiem-253872 (dostęp: 08.05.2017).

Zięba R., 1999, *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje – struktury – funkcjonowanie*, Scholar, Warszawa.

Perception of safety of banking services use among the youth

Abstract. Technological environment of financial institutions is changing very rapidly. It contributes to a lot of new threats such as terrorism, cybercrime or viruses. Bank customers expect not only privacy and comfort but most of all they want to be sure that banks protect their money with the highest security standards. The purpose of the article is the evaluation of understanding and complying with security principles with respect to the use of the chosen banking services by students. The article contains the results of the author's own research which was carried out among 274 students of the public universities in Poznan in 2017. The anaysis characterises factors which bank customers take into account while using banking services so that their funds should be safe as well as the attitude towards biometrics and other security measures.

Keywords: mobile banking, online banking, consumer protection.
JEL Codes: G210, D18.