



Mobilny Bank
Powered by Raiffeisen Bank Polska S.A.

Bezpieczeństwo bankowości mobilnej



**Raiffeisen
BANK**

Raiffeisen Bank Polska S.A.

ostatnia aktualizacja: 21.04.2010 r.

Autor: Janusz Nawrat

Czym jest bankowość mobilna?

Bankowość mobilna jest jednym z elektronicznych kanałów dostępu do banku, wykorzystującym w charakterze terminali dostępu telefony komórkowe, a jako medium dostępowe, sieci operatorów telefonii komórkowej. Bankowość mobilna cieszy się wciąż rosnącym zainteresowaniem klientów. Klientami bankowości mobilnej stają się przede wszystkim osoby otwarte na innowacje, ceniące swobodę zarządzania swoim kontem w banku z każdego miejsca na świecie i o każdej porze doby.

Wszystko, czego potrzeba do korzystania z bankowości mobilnej to odpowiedni telefon dostosowany technologicznie do wymagań aplikacji oferowanej przez bank. Większość tzw. inteligentnych telefonów (smartfonów), w tym urządzenia działające pod kontrolą systemów Symbian, Windows CE, Android i iPhone OS, dostępnych obecnie na rynku spełnia minimalne wymagania takich aplikacji.

Z jakimi zagrożeniami musi liczyć się użytkownik bankowości mobilnej?

Wraz z postępowaniem technologicznym, **telefon komórkowy w coraz większym stopniu upodabnia się do klasycznego urządzenia komputerowego**, co obok rozlicznych korzyści, takich chociażby, jak coraz większa funkcjonalność urządzenia, uniwersalność jego zastosowań i przyjazność interakcji z użytkownikiem, niestety, ma także pewne negatywne skutki. Rośnie bowiem poziom istotności i liczba zagrożeń, jakim użytkownik musi stawić czoło, chcąc, aby korzystanie z telefonu komórkowego jako uniwersalnego urządzenia komunikacji bezprzewodowej i dostępu do banku nadal pozostało czynnością bezpieczną. Charakter wspomnianych zagrożeń staje się coraz bliższy temu, czemu sprostać muszą stojące na biurku lub przenośne, klasyczne komputery podłączone do sieci.

Bezpieczne korzystanie z bankowości mobilnej jest z znacznym stopniem zależne od bezpieczeństwa telefonu komórkowego, pełniącego rolę terminala dla tego rodzaju elektronicznego kanału dostępu.

Tak, jak krytycznym czynnikiem decydującym o bezpieczeństwie korzystania z bankowości internetowej jest odpowiednie zabezpieczenie komputera użytkownika, analogicznie w bankowości mobilnej, równie ważne jest spełnienie minimalnych wymagań bezpieczeństwa w zakresie zabezpieczenia telefonu komórkowego oraz bezpiecznych praktyk jego stosowania.

Coraz większym zagrożeniem dla użytkowników tzw. inteligentnych telefonów komórkowych (smartfonów) staje się **oprogramowanie złośliwe** takie jak wirusy, robaki internetowe, oprogramowanie szpiegujące, wytrychy czy konie trojańskie. Już teraz, pod pojęciem bezpiecznego smartfona rozumie się takie urządzenie, które obowiązkowo posiada zainstalowane dobre oprogramowanie antymalware.

Skala zjawiska tworzenia i propagowania oprogramowania złośliwego przeznaczonego do infekowania telefonów komórkowych nie jest jeszcze co prawda tak duża jak w przypadku komputerów, ale wykazuje stałą tendencję wzrostową. Ze stałym wzrostem zagrożenia należy się więc liczyć. Zagrożenie, wynikające z infekcji telefonu oprogramowaniem złośliwym ma dokładnie taki sam charakter jak dobrze znane zagrożenia w świecie klasycznych komputerów. Zainfekowanie telefonu oznacza ryzyko kradzieży poświadczeń tożsamości (loginów i haseł do bankowości mobilnej, ujawnienia numerów kart kredytowych, PIN-ów i innych wrażliwych danych. Na tym jednak nie koniec. Infekcja telefonu w pewnych przypadkach wiąże się także z poważnym ryzykiem podmiiany danych transakcyjnych (na przykład kont beneficjentów zleczanych przelewów). Mowa tu oczywiście o klasycznych środkach z arsenału kategorii ataków man-in-the-browser. Na szczęście jednak to zagrożenie nie dotyczy klientów bankowości mobilnej Raiffeisen Bank Polska S.A., bowiem aplikacja udostępniana przez bank jest w pełni niezależna od przeglądarki.

Trzeba ponadto nieustająco pamiętać, iż **telefon komórkowy wyposażony w interfejsy sieciowe w postaci wbudowanego modemu GSM lub bezprzewodowej karty sieciowej (WiFi), od chwili nawiązania połączenia z siecią Internet, staje się takim samym, wyeksponowanym na ataki, elementem sieci jak klasyczny komputer.** Jest zatem potencjalnym celem ataków ze strony hackerów, botnetów czy oprogramowania złośliwego. Nie powinna więc podlegać dyskusji potrzeba wyposażenia go w skuteczną osobistą zaporę sieciową. Brak ochrony przed atakami z sieci Internet może skutkować na przykład infekcją telefonu oprogramowaniem złośliwym ze wszystkimi tego szkodliwymi skutkami (także dla bankowości mobilnej), opisanymi wcześniej lub wyprowadzeniem poufnych danych. Środkiem zaradczym jest instalacja na smartfonie zintegrowanego pakietu zabezpieczeń, obejmującego jako minimum skaner antywirusowy i osobistą zaporę sieciową. Dostępne na rynku produkty tego rodzaju na ogół oferują dodatkowo ochronę na poziomie kontroli procesów, przeciwdziałania atakom z sieci Internet i czasem także szyfrowania plików.

Przyjmując słuszne założenie, iż telefon komórkowy jest wymagającym ochrony urządzeniem komputerowym, nie należy instalować na nim **oprogramowania z niezaufanych źródeł** (na przykład nielegalnego oprogramowania poddanego przeróbkom w celu złamania zabezpieczeń praw autorskich i licencyjnych). Pamiętajmy, że takie oprogramowanie nierzadko posiada wbudowane w kod funkcje tylnych wejść (ang: *backdoors*), które mogą być wykorzystane przez agresorów do złamania zabezpieczeń telefonu, wygenerowania wysokich rachunków za transfer danych, zainstalowania oprogramowania złośliwego albo - najwyczejniej - wyprowadzenia wrażliwych danych z pamięci telefonu.

Nie należy zapominać także o tym, że źle napisana aplikacja często przyczynia się do osłabienia mechanizmów bezpieczeństwa telefonu, ponieważ jej podatności eksponują dodatkowo także system operacyjny i inne oprogramowanie zainstalowane na telefonie na atak agresorów, a wszak nie od dziś wiadomo, iż o bezpieczeństwie całości dowolnego rozwiązania zawsze decyduje najszabsze ogniwo w łańcuchu zabezpieczeń. Aplikacje instalowane na telefonie powinny być podpisane cyfrowo przez dostawcę. Podpis cyfrowy pozwala na zweryfikowanie pochodzenia aplikacji (od zaufanego dostawcy) i jej integralności (nikt nie ingerował w jej kod od momentu jej skompilowania przez zaufanego dostawcę).

Konsekwencją instalacji aplikacji z niezaufanych źródeł może być osłabienie mechanizmów zabezpieczeń telefonu (w postaci na przykład aktywacji tylnego wejścia, umożliwiającego przejęcie zdalnej kontroli nad urządzeniem, czy wyłączenie mechanizmów zabezpieczeń takich jak osobista zaporę sieciową czy skaner antywirusowy), wprowadzenie nowych podatności, z których każda jest potencjalnym celem ataku możliwego do przeprowadzenia z sieci Internet. Wobec tego, co zostało napisane zbędnym wydaje się dalsze opisywanie szkodliwych konsekwencji dla bezpieczeństwa korzystania z bankowości mobilnej.

Jednym z najpoważniejszych źródeł podatności i luk w bezpieczeństwie każdego rodzaju oprogramowania są jego, różnego rodzaju, usterki i wady. Przeważnie są to wady istniejące na poziomie kodu aplikacji, które mają istotne znaczenie dla bezpieczeństwa. Producenci oprogramowania usuwają ujawnione w nim błędy i usterki poprzez opracowywanie oraz dystrybucję do użytkowników odpowiednich poprawek i aktualizacji czyli „łatek” (ang: *patches*).

System operacyjny telefonu wraz z oprogramowaniem standardowym także może wymagać okresowych aktualizacji, korygujących błędy oraz usuwający podatności i luki w bezpieczeństwie. Dotyczy to zwłaszcza otwartych platform takich jak Windows Mobile, Symbian itp. Sposób przeprowadzenia aktualizacji nie jest jednak zawsze czynnością łatwą do wykonania. Bywa tak, że w modelach telefonów niektórych dostawców taką operację można bezpiecznie wykonać jedynie w odpowiednich, specjalistycznych punktach usługowych, nierzadko z autoryzacją

producenta. Niewłaściwie przeprowadzona aktualizacja systemowego oprogramowania telefonu może doprowadzić do nieodwracalnej utraty cennych danych, a nawet awarii telefonu.

Obowiązkiem użytkownika, przed podjęciem ewentualnej decyzji o aktualizacji oprogramowania systemowego jest przygotowanie kopii zapasowej danych telefonu.

Aktualizację można przeprowadzić we własnym zakresie jedynie wówczas, jeśli jest to operacja bezpieczna, użytkownik wie jak ją przeprowadzić, ma do dyspozycji odpowiednie narzędzia w postaci przeznaczonego do tego celu oprogramowania narzędziowego od producenta telefonu, właściwe akcesoria (jak choćby kable do podłączenia telefonu do komputera), aktualizacja oprogramowania pochodzi z wiarygodnego źródła (od producenta telefonu), operacja aktualizacji nie narusza warunków gwarancji czy jakichkolwiek warunków ewentualnych umów licencyjnych, zostały przygotowane wcześniej (i przetestowane) kopie zapasowe danych z telefonu.

W przypadku, kiedy użytkownik nie jest w stanie z powodzeniem przeprowadzić wszystkich czynności aktualizacji, powinien rozważyć możliwość zlecenia tego specjalistycznej firmie usługowej.

Czy i ewentualnie jak często należy takie aktualizacje przeprowadzać, to oczywiście zależy od konkretnej platformy programowej smartfona. Prawidłowością jest, że otwarte platformy, nie związane z jednym konkretnym producentem skupiają na sobie większe zainteresowanie nie tylko legalnie działających specjalistów od wykrywania podatności, ale także świata hackerskiego.

Zalecane jest śledzenie doniesień o bezpieczeństwie wykorzystywanego przez siebie rodzaju smartfona oraz instalowanie aktualizacji i łatek zalecanych przez producentów.

Kolejnym ważnym czynnikiem decydującym o bezpieczeństwie telefonu i zapisanych w jego pamięci danych jest jego **ochrona przed zagubieniem** czy **kradzieżą**.

Wrażliwe dane (na przykład hasła, numery kart kredytowych, numery PIN itp.) zapisane w pamięci telefonu lub na karcie pamięci muszą być zabezpieczone przed ujawnieniem i wykorzystaniem przez przestępców. W praktyce zabezpieczenia takie sprowadzają się do ich zaszyfrowania. Na rynku dostępnych jest wiele komercyjnych produktów oferujących szyfrowanie wrażliwych danych w telefonie. Są też dostępne, nie mniej skuteczne, rozwiązania darmowe.

Nie tracą na aktualności także takie podstawowe zasady, jak niepozostawianie telefonu bez nadzoru (na przykład w samochodzie albo w kieszeni płaszcza w publicznej szatni, w środkach komunikacji, w pokojach hotelowych itp.) oraz bezpieczne przenoszenie telefonu (w taki sposób, aby nie wypadł lub nie został wyciągnięty z kieszeni przez złodzieja).

Zagubienie lub kradzież telefonu z niezabezpieczonymi danymi w postaci na przykład poświadczeń tożsamości do logowania się do bankowości mobilnej może mieć dla pierwotnego właściciela smartfona fatalne skutki.

Bezpieczne praktyki korzystania z bankowości mobilnej

Dokonany wcześniej krótki przegląd zagrożeń powinien doprowadzić nas do wniosku, że techniczne zabezpieczenia telefonu stanowią tylko jeden z aspektów bezpiecznego korzystania z bankowości mobilnej. Drugi, niemniej ważny, to sposób posługiwania się telefonem, czyli bezpieczne praktyki korzystania z bankowości mobilnej. O tym właśnie traktuje niniejszy rozdział.

Nie sposób przecenić znaczenia właściwego zabezpieczenia telefonu, czyli blokady telefonu indywidualnie ustalonym kodem, nie zapisywania haseł logowania do jakichkolwiek systemów otwartym tekstem w pamięci telefonu, nie wysyłania haseł otwartym tekstem w komunikatach SMS, czy wreszcie fizycznego zabezpieczenia telefonu przed zagubieniem i kradzieżą.

W razie potrzeby do przechowywania w pamięci telefonu danych do logowania do bankowości mobilnej i innych wrażliwych danych (na przykład haseł czy poufnych notatek) zalecane jest zastosowanie oprogramowania szyfrującego, bądź to specjalistycznego do szyfrowania baz haseł,

bądź też oprogramowania do szyfrowania plików lub pamięci telefonu. Oferta tego typu oprogramowania jest dość bogata dla wszystkich popularnych platform smartfonów. Obejmuje ona również oprogramowanie dostępne bezpłatnie.

Użytkownika bankowości mobilnej obowiązują zawsze, w jego dobrze pojętym interesie, ogólne zasady bezpieczeństwa, takie jak nieujawnianie w jakikolwiek sposób haseł dostępu do bankowości mobilnej niepowołanym osobom i niepozostawianie telefonu bez nadzoru, zwłaszcza z otwartą sesją do bankowości mobilnej.

Czułości ze strony użytkownika, nie mniejszej niż w przypadku korzystania z klasycznego komputera, wymaga otwieranie załączników do wiadomości poczty odbieranej przez smartfon czy podążanie śladami zamieszczonych w tych wiadomościach odnośników (hiperlinków). Prawdopodobieństwo otrzymania scamu phishingowego jest identyczne w obu przypadkach. Statystyki ataków, choć mniejsze, ze względu na liczbę wirusów na platformy mobilne i dotąd wciąż niższy poziom zainteresowania przestępców tworzeniem oprogramowania złośliwego, dowodzą jednak, że nie należy usypiać czujności czy lekceważyć problemu.

Podsumowując, podajemy proste do zastosowania, złote zasady bezpiecznego korzystania z bankowości mobilnej:

- Traktuj swój telefon komórkowy, którego używasz do korzystania z bankowości mobilnej analogicznie jak traktujesz komputer, służący Ci do nawiązywania połączeń do bankowości internetowej. Zabezpiecz go, jeśli to możliwe, instalując na nim pakiet oprogramowania zabezpieczającego (składającego się głównie ze skanera antywirusowego i osobistej zapory sieciowej).
- Rozważ możliwość aktualizacji oprogramowania systemowego telefonu, zwłaszcza w takiej sytuacji, kiedy producent telefonu udostępnia poprawki bezpieczeństwa i zaleca ich zainstalowanie.
- Nie instaluj na swoim telefonie oprogramowania z niezauważanych źródeł.
- Nie zapisuj w pamięci telefonu wrażliwych danych (haseł, numerów kart kredytowych PIN-ów itp.) jawnym tekstem. Jeśli musisz zapisać tego typu informacje w pamięci telefonu, użyj oprogramowania szyfrującego. W tym przypadku pamiętaj jednak, aby główne hasło do bazy oprogramowania szyfrującego było odpowiednio silne i bezpiecznie przechowywane.
- Nie ujawniaj nikomu swoich poświadczeń tożsamości (loginów i haseł) w systemie bankowości mobilnej. Nie podawaj ich nigdy na żadnych stronach czy w odpowiedzi na żądania otrzymane e-mailem. Pamiętaj, że te informacje są Twoją tajemnicą i bank nigdy nie żąda ich podania za wyjątkiem logowania do aplikacji. Nie wysyłaj swoich poświadczeń tożsamości jawnym tekstem w komunikatach SMS i w wiadomościach poczty elektronicznej.
- Zabezpiecz telefon kodem zabezpieczającym.
- Nie pozostawiaj swojego telefonu komórkowego bez nadzoru zwłaszcza w samochodzie, w miejscach publicznych, w szatniach, w pokojach hotelowych. Nie narażaj swojego smartfona na zagubienie i kradzież.