Korzystając z internetowego systemu I-Bank należy się stosować

do podstawowych zasad bezpieczeństwa:

1. Należy korzystać z legalnego oprogramowania i regularnie je aktualizować. Na komputerze, na którym będzie uruchamiany system I-BANK musi być zainstalowane oprogramowanie JAVA w najnowszej wersji.

2. Należy okresowo zmieniać hasło logowania i kod PIN do systemu I-BANK.

3. Oprogramowanie JAVA wymaga zgody Klienta na uruchamianie zewnętrznych programów. Z tego względu przy próbie odwołania się systemu I-BANK do zasobów lokalnych komputera w celu obsługi kluczy cyfrowych, program JAVA wyświetla komunikat ostrzegawczy. Jeśli komunikat pojawił się podczas korzystania z programu bankowości internetowej, to należy zezwolić na jego pracę po uprzednim upewnieniu się, że odwołanie dotyczy systemu I-BANK. W przeciwnym razie należy zablokować program.

4. Program I-BANK należy uruchamiać za pośrednictwem strony www banku, na komputerze dobrze zabezpieczonym przed dostępem osób nieuprawnionych.

5. Przed uruchomieniem programu I-BANK należy zabezpieczyć swój komputer stosując program antywirusowy, który jest regularnie aktualizowany, stosując firewall (odpowiednio skonfigurowany) i programy antyspywerowe (zabezpieczyć komputer przed możliwością instalacji programów szpiegujących, np. Keyloggerów). Należy zabezpieczyć komputer przed możliwością instalacji programów umożliwiających przejęcie zdalnej kontroli nad komputerem.

6. Należy regularnie skanować komputer i urządzenia mobilne programami zabezpieczającymi.

7. Jeśli do autoryzacji przelewów jest używany klucz cyfrowy, to należy go wyciągnąć z portu USB po zakończeniu pracy z programem i chronić przed nieuprawnionym użyciem.

8. Jeśli autoryzacja przelewów jest wykonywana za pomocą kodów SMS, to należy sprawdzić, czy na telefonie jest zainstalowane aktualne oprogramowanie antywirusowe. Swojego numeru telefonu nigdy nie należy podawać w korespondencji elektronicznej, ankietach, formularzach itp. Bank wysyła kody SMS i informacje SMS z następujących numerów telefonów: +48 695 416 715, +48 798 741 663.

9. W przypadku utraty środków autoryzacji (hasła, klucza lub telefonu komórkowego) należy niezwłocznie powiadomić bank w celu zablokowania dostępu do programu.

10. Zaleca się korzystać z bankowości internetowej wyłącznie na komputerze, na którym zablokowany jest dostęp do internetu i poczty e-mail. Odblokowane jest wyłącznie połączenie ze stroną internetową banku. Można to uczynić poprzez instalację maszyn wirtualnych, z których jedna będzie przeznaczona wyłącznie do obsługi bankowości elektronicznej a druga do korzystania z internetu (maszyny są wzajemnie izolowane).

11. Korzystanie z bankowości elektronicznej powinno odbywać się na komputerze, który do połączenia z internetem wykorzystuje konta z ograniczonymi uprawnieniami.

12. Na komputerze przeznaczonym do obsługi systemu I-BANK nie należy używać oprogramowania pozyskanego za pośrednictwem programów typu peer 2 peer (wszystkie pliki ściągane tą metodą są szczególnie narażone na obecność wirusów komputerowych, ponieważ ich pobieranie odbywa się bezpośrednio z komputera innego użytkownika podłączonego do sieci).

13. Należy chronić swój program pocztowy przed spamem w celu uniknięcia wyłudzenia informacji. Nie należy otwierać podejrzanych maili oraz odnośników i załączników.

14. Nie należy otwierać podejrzanych SMS-ów oraz podawanych w nich odnośników.

15. Nie należy instalować na komputerze i w telefonie oprogramowania niewiadomego pochodzenia.

16. Nie należy podłączać telefonu do niezaufanych komputerów.

17. Nie należy zezwalać na niezaufane połączenia typu Bluetooth i WiFi z Twoim telefonem komórkowym. Należy wyłączyć Bluetooth i moduł WiFi jeśli nie są używane.

18. Należy unikać korzystania z bankowości elektronicznej na nieznanym komputerze.

19. Nie wolno udostępniać osobom trzecim haseł, kodów PIN i innych elementów służących logowaniu do internetowego systemu I-Bank.

20. Nie należy zapisywać haseł i kodów PIN uzyskanych na wydruku z Banku służących logowaniu do internetowego systemu I-Bank. Uzyskany wydruk należy zniszczyć a informacje na nim zawarte zapamiętać.

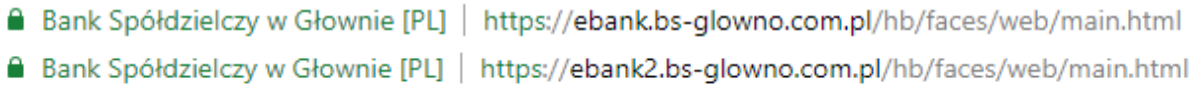
21. Wszystkie hasła i kody należy przechowywać w miejscach trudno dostępnych dla innych osób.

22. Nie należy stosować hasła do logowania się na stronie Banku na innych stronach internetowych.

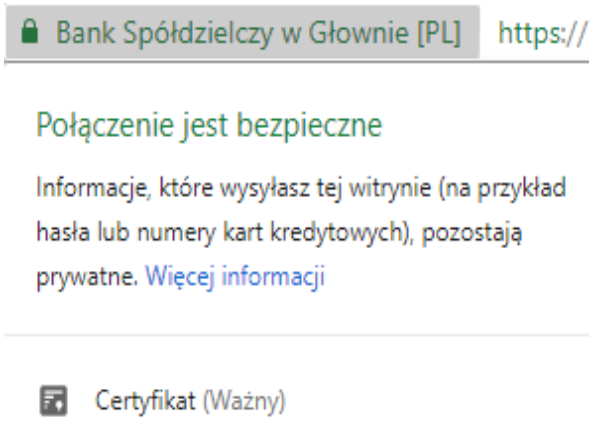
23. Nie wolno odpowiadać na e-maile, w których nadawca prosi o podanie numeru PIN, haseł i innych treści dostępowych do internetowego systemu I-Bank. Bank nigdy nie wysyła wiadomości z prośbą o podanie haseł dostępu, kodów PIN i innych treści służących logowaniu do internetowego systemu I-Bank.

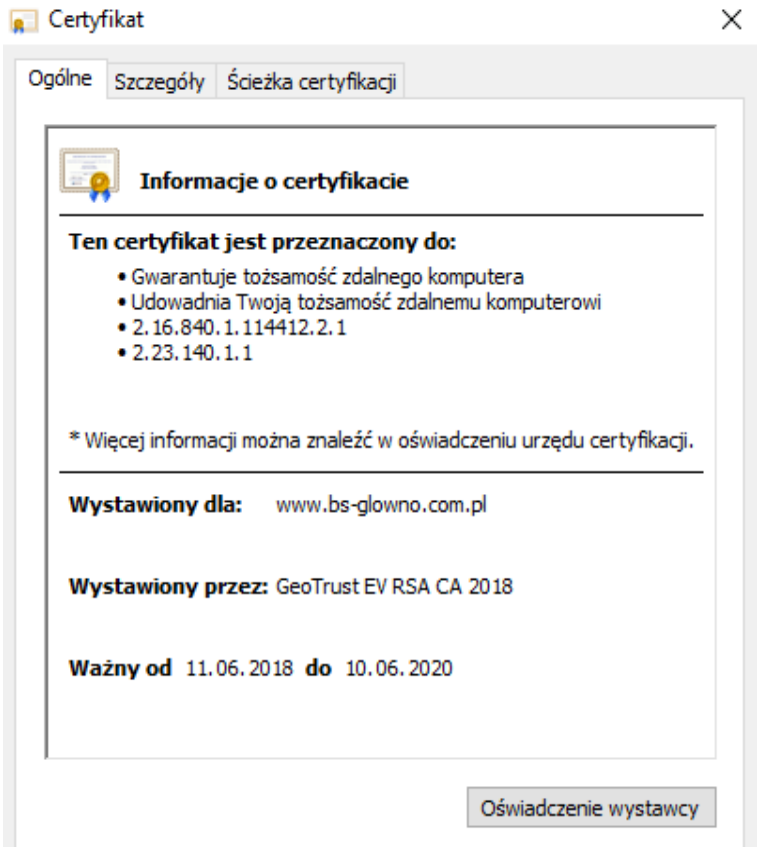
24. Podczas logowania należy zawsze upewnić się czy wprowadzony adres strony bankowej jest poprawny, tzn. żadna z wprowadzonych liter nie jest zamieniona innym znakiem lub jest wprowadzona podwójnie itp.

25. Należy zawsze sprawdzać, czy połączenie z Bankiem jest szyfrowane, tzn. czy w pasku adresu przeglądarki internetowej, adres strony zaczyna się od **https://**



a także czy na pasku na dole lub u góry przeglądarki internetowej pojawił się symbol zamkniętej kłódki . Klikając na ten symbol można sprawdzić czy certyfikat Banku jest poprawny i aktualny.





26. Nie należy odchodzić od komputera w momencie kiedy jesteśmy zalogowani do internetowego systemu I-Bank.

27. Klucz cyfrowy otrzymany z Banku służy wyłącznie logowaniu do systemu I-Bank, nie można wykorzystywać go w innym celu.

28. Każdorazowo przed podpisaniem oraz wysłaniem przelewu sprawdzić poprawność numeru rachunku (tzw. NRB) odbiorcy.

29. Bank nie wysyła wiadomości e-mail, które zawierają prośby o podanie danych osobowych, numerów PIN, haseł czy telefonów. Wszelkie informacje dotyczące systemu I-Bank podawane są na tablicy informacyjnej po zalogowaniu się do panelu Klienta systemu I-Bank.

30. Należy zawsze zachować podstawowe zasady bezpieczeństwa. Traktować z dozą nieufności wszystkie wiadomości e-mail, SMS-y i telefony, w których zawierają się prośby o podanie danych osobowych, numerów PIN czy haseł. W razie wszelkich, budzących wątpliwość sytuacji związanych z autentycznością transakcji w systemie I-BANK należy niezwłocznie poinformować o tym bank.

31. System Windows XP nie jest już rozwijany przez producenta i wykryte luki w zabezpieczeniach nie są już naprawiane. Z tego względu nie zaleca się na systemie Windows XP uruchamiania połączenia z bankiem.

32. Kończąc pracę należy zawsze opuścić stronę Banku naciskając przycisk „KONIEC PRACY".

Stosowanie się do powyższych zasad znacznie zwiększa bezpieczeństwo transakcji dokonywanych elektronicznymi kanałami dostępu oraz ogranicza ryzyko podatności na działanie takich programów jak: Keyloggery, trojany (Carberp, Citadel, SpyEye, ZeuS) oraz coraz częściej występującym atakom typu Man In The Endpoint!

Opis zagrożeń

Keylogger (ang. "key" – klawisz, "log" – dziennik) – rodzaj oprogramowania lub urządzenia rejestrującego klawisze naciskane przez użytkownika komputera. Częściej spotykane są keyloggery programowe.

Hasło może być wprowadzane za pomocą klawiatury standardowej lub klawiatury ekranowej co zabezpiecza przed jego podsłuchaniem przez programy tzw. *Keyloggery.* Dla klientów, którzy otrzymali klucz cyfrowy, system I-Bank wymusza stosowanie silnego uwierzytelnianie podczas logowania. W takim przypadku po podaniu identyfikatora i hasła klient musi dodatkowo podłączyć do portu USB swój klucz cyfrowy i podpisać znacznik sesji wygenerowany przez serwer. Dla klientów, którzy nie mają klucza, cyfrowego, podczas logowania jest stosowane uwierzytelnienie na podstawie tylko identyfikatora i hasła. W takim przypadku komputer klienta musi być zabezpieczony przed możliwością instalacji złośliwego oprogramowania potrafiącego podsłuchać hasło klienta (*keyloggery*). Zalecane jest, aby w takim przypadku Klient podczas wpisywania hasła **posługiwał się klawiaturą ekranową.**

Koń trojański, trojan – określenie oprogramowania, które podszywając się pod przydatne lub ciekawe dla użytkownika aplikacje dodatkowo implementuje niepożądane, ukryte przed użytkownikiem różne funkcje (programy szpiegujące, bomby logiczne, furtki umożliwiające przejęcie kontroli nad systemem przez nieuprawnione osoby itp.).

Najpopularniejszymi szkodliwymi działaniami są:

- instalowanie w systemie backdoora i udostępnianie kontroli nad systemem nieuprawnionym osobom w celu rozsyłania spamu, dokonywania ataków DDoS itp.,
- szpiegowanie i wykradanie poufnych danych użytkownika (spyware),
- utrudnianie pracy programom antywirusowym,

- zmienianie strony startowej przeglądarki WWW i prezentowanie reklam,
- działania destruktywne (kasowanie plików, uniemożliwianie korzystania z komputera.

Niektóre trojany mają kilka dodatkowych funkcji, takich jak wyłączenie monitora, wysunięcie klapki nagrywarki CD/DVD, otworzenie strony internetowej.

Trojan przechwytuje loginy i hasła do bankowości internetowej wykorzystując m.in. phishing. Klient nieświadomy, że zamiast na stronę swojego banku trafił na stronę stworzoną przez przestępców (strona ta może być łudząco podobna do strony banku), podaje swój login oraz hasło. Dodatkowo, co charakterystyczne dla tego typu ataku, Klient jest proszony o podanie modelu telefonu komórkowego i numeru telefonu np. w celu przesłania "certyfikatu bezpieczeństwa" lub oprogramowania zabezpieczającego. Następnie na wskazany telefon komórkowy, przestępcy przesyłają SMS z odnośnikiem do złośliwej aplikacji dostosowanej do modelu telefonu.

Aplikacja ta po zainstalowaniu monitoruje przychodzące SMS-y i uruchamia funkcję pozwalającą na zarządzanie telefonem Klienta. Głównym zadaniem tej aplikacji jest przesyłanie SMS-ów autoryzacyjnych przychodzących z banku na numer telefonu cyberprzestępcy i ukrywanie tych działań.

Trzeba podkreślić, że opisany sposób ataku jest możliwy wyłącznie przy aktywnym udziale klienta banku. Klient – nieświadomy zagrożenia – potwierdza komunikaty wyświetlane na jego komputerze lub na telefonie komórkowym przez złośliwe oprogramowanie i jednocześnie zezwala na ich zainstalowanie. Z tego względu w programie JAVA pojawiły się komunikaty ostrzegawcze. Mają one za zadanie zwrócić uwagę Klienta na problem zabezpieczenia jego komputera.

Autoryzacja przelewów kluczem cyfrowym skutecznie chroni treść przelewu przed atakami typu: phishing, trojany keyloggery.

Man In The Endpoint – przejęcie przez hakera kontroli nad komputerem.

Chociaż koncepcja ataków MitE jest znana od wielu lat, dopiero niedawno zaczęto aktywnie wykorzystywać ją w rzeczywistym świecie. Atak MitE nie wymaga dodatkowego serwera do przechwytywania ruchu pomiędzy Klientem a bankiem. Zamiast tego wszystkie zmiany są dokonywane w systemie lokalnym, czyli u ofiary. Z punktu widzenia hakera podejście to posiada wiele istotnych zalet. Po pierwsze, istnieje bezpośrednie połączenie z bankiem, dlatego taka transakcja nie zostanie oznakowana jako podejrzana tylko dlatego, że użytkownik zalogował się z nieznanego adresu IP. Po drugie, ataki MitE mogą by skuteczne, jeżeli ich celem będzie system posiadający złożone mechanizmy ochrony.
Jeden ze scenariuszy ataków zakłada zainfekowanie systemu za pomocą trojana, którego celem jest przechwycenie całego ruchu HTTPS. Przechwycony ruch jest następnie wysyłany do hakera, dostarczając im schemat strony internetowej. Schemat ten jest następnie wykorzystywany do stworzenia kolejnego trojana. Wykorzystywane w takich atakach trojany często będą mogły otrzymywać dane z serwera, na którym przestępcy przechowują informacje dotyczące numeru konta i kwoty, która ma zostać przelana. Ponieważ działanie to można wykonać dynamicznie, dane mogą zostać wysłane na każdą zainfekowaną maszynę, przy czym każda maszyna będzie przelewała środki do odpowiednich *mułów pieniężnych* (są to podstawione rachunki fikcyjnych osób, na które są przekazywane pieniądze ofiary).
Cyberprzestępcy modyfikują warianty szkodliwego oprogramowania należące do tej samej rodziny w zależności od stosowanych przez bank mechanizmów bezpieczeństwa, aby zapewnić jak największą skuteczność ataku. Na przykład, w przypadku jednego banku trojan potajemnie doda dodatkowe

informacje, w przypadku innego, potajemnie zastąpi transakcję użytkownika, aby nie wzbudzać podejrzeń.

Trzeba jednak zaznaczyć, że system I-Bank z włączoną autoryzacją za pomocą kluczy cyfrowych jest odporny na ataki przy pomocy znanych już trojanów np.: Carberp, Citadel, SpyEye czy najbardziej znany ZeuS. Jednak gdy Klient banku pozwoli hakerowi przejąć zdalną kontrolę nad własnym komputerem (atak Man-in-the-Endpoint), wówczas żadne zabezpieczenia nie są skuteczne.

Ataki socjotechniczne **-** w bezpieczeństwie teleinformatycznym zestaw metod mających na celu uzyskanie niejawnych informacji przez cyberprzestępcę. Ataki socjotechniczne opierają się na największej słabości każdego systemu informatycznego a mianowicie na czynniku ludzkim. Posługując się zdobytymi informacjami i dobrą znajomością ludzkiej psychiki, socjotechnicy mogą dokonywać kradzieży danych, o których ofiary najczęściej nigdy się nie dowiedzą. W kontekście bezpieczeństwa IT pod tym pojęciem rozumie się próby dotarcia do poufnych informacji za pomocą manipulacji.

Do tego celu przestępcy często wykorzystują różne środki komunikacji np. telefon czy pocztę elektroniczną. Podstawą większości ataków socjotechnicznych jest wykorzystanie pozornie nieistotnych informacji.

Dlatego tak ważne jest zachowanie czujności w kontaktach telefonicznych, mailowych czy bezpośrednich w kontekście wymienionych tu zagadnień.

UWAGA!

Rozwiązanie i proces bezpieczeństwa są tak "silne" jak jego najsłabsze ogniwo. Dlatego niniejsze zasady przypominają o rozważnym i świadomym korzystaniu z medium jakim jest Internet i zabezpieczaniu urządzeń końcowych. To od Użytkownika zależy czy kliknie w odsyłacz lub załącznik, czy posiada uaktualniony system operacyjny wraz z wszystkimi poprawkami oprogramowania. Należy mieć świadomość, że bezpieczeństwo pieniędzy zależy w dużej mierze, od tego czy sam Użytkownik będzie się stosował do zasad bezpiecznego korzystania z bankowości internetowej, o których przypomina mu niniejszy opis.