10 przykazań bezpiecznego korzystania z bankowości internetowej

Polskie banki i SKOK-i mają jedne z najbezpieczniejszych systemów bankowości internetowych na świecie. Słabym ogniwem w procesie zabezpieczeń niestety najczęściej okazujemy się my sami. Przez nieuwagę lub brak odpowiedniej wiedzy narażamy się na ryzyko utraty środków z rachunku.

Wystarczy jednak trzymać się kilku żelaznych reguł, by uchronić swoje oszczędności przed oszustami.

Oto 10 przykazań bezpiecznego korzystania z bankowości internetowej:

1. Zawsze sprawdzaj adres strony logowania

Do logowania się na konto w E-SKOK zawsze używajmy strony podanej przez SKOK. Jeśli zapomnimy adresu, nie powinniśmy korzystać z wyszukiwarek internetowych.
Do strony logowania dostaniemy się bezpośrednio ze strony głównej naszego SKOKU **www.kasyblachnickiego.pl** Przed zalogowaniem się należy sprawdzić, czy adres strony połączenia zaczyna się od protokołu **https://** i czy w adresie znajduje się **symbol zamkniętej kłódki**, który oznacza, że cały proces będzie przebiegać bezpiecznie. Specjaliści zalecają, by nie przechowywać adresu strony do logowania w ulubionych zakładkach przeglądarki. Oszuści znają bowiem sposoby, jak podmienić taką zakładkę na fałszywą.

2. Uważaj na fałszywe maile i załączniki

Pamiętaj, że SKOK **nigdy nie przesyła mailem linków kierujących do systemu transakcyjnego**. Jeśli dostaniesz taką wiadomość, należy przesłać ją do SKOK-u, w którym mamy rachunek. Na tym polega **phishing** - popularna wśród złodziei metoda oszukiwania klientów banków. Tworzą fałszywą stronę logowania do złudzenia przypominającą oryginał, a następnie wysyłają do losowo wybranych osób maile rzekomo w imieniu SKOK-u z prośbą o pilne zalogowanie się do bankowości internetowej. Klient, który zaloguje się na takiej fałszywej stronie, udostępnia złodziejom dane do logowania na konto. Inną, stosowaną przez cyberprzestępców metodą wyłudzania danych, jest przesyłanie klientom fałszywych maili z załącznikami zawierającymi wirusy.

3. Zmieniaj hasła

Hasło do systemu bankowości internetowej lub bankowości mobilnej **powinniśmy regularnie zmieniać**. W ten sposób zminimalizujemy ryzyko włamania na nasze konto. Warto też zadbać o to, by nie było zbyt proste. Najlepiej skonstruować hasło zawierające minimum 8 znaków a w nim znaki specjalne np.: !@#$%, duże litery i cyfry.

Ustaw indywidualny obrazek bezpieczeństwa (anty-phishingowy), który będzie wyświetlany w drugim kroku logowania do Serwisu internetowego Usługi eSKOK.

4. Chroń dane do logowania

Dane do logowania do systemu E-SKOK można porównać do kombinacji szyfru w tradycyjnym sejfie. Jeśli ujawnimy je komuś, to tak jakbyśmy dali dostęp do sejfu, w którym trzymamy kosztowności. Dlatego **powinien znać je tylko klient**. Nie należy ich ujawniać osobom trzecim, nawet bliskim. Także dlatego, że SKOK ma prawo odmówić uznania reklamacji, jeśli ustali, że ktoś inny posługiwał się danymi dostępowymi. **Dotyczy to również współmałżonka**, nawet jeśli konto jest wspólne.

Podczas logowanie się do bankowości elektronicznej E-SKOK po wpisaniu swojego loginu i hasła otrzymasz na wskazany w placówce SKOK nr telefonu jednorazowy kod weryfikacyjny który po wpisaniu na stronę logowania pozwoli na korzystanie z usługi E-SKOK.

5. Korzystaj z własnego komputera

Bankowość internetowa umożliwia korzystanie z e-banku z dowolnego miejsca na ziemi i dowolnego komputera. W praktyce jednak **należy zachować szczególną ostrożność jeśli korzystamy z obcego urządzenia** i pamiętać o tym, by się wylogować po sesji. Pod żadnym pozorem nie powinniśmy korzystać z bankowości internetowej w kafejkach internetowych. Nie mamy bowiem żadnej gwarancji, że na takim komputerze nie zainstalowano oprogramowania wirusowego, które "podsłucha" znaki wpisywane przez nas podczas logowania do systemu.

6. Aktualizuj system i przeglądarki

Należy dbać o bezpieczeństwo swojego komputera. Firmy dostarczające systemy operacyjne co pewien czas publikują aktualizacje, które uszczelniają system przed potencjalnymi atakami hakerów. Jeśli korzystamy z bankowości internetowej, **powinniśmy też zadbać o bezpieczną przeglądarkę internetową**. Dostawcy oprogramowania dbają o to, by regularnie łatać ewentualne dziury w swoim oprogramowaniu.

7. Korzystaj z antywirusa

Pozycją obowiązkową w komputerze, z którego korzystamy, powinien być program antywirusowy. W internecie dostępne są bezpłatne programy antywirusowe. Zanim jednak skorzystamy z takiego oprogramowania, **należy zapoznać się z opiniami innych użytkowników**. Odnotowano przypadki pojawiania się fałszywych programów antywirusowych, które w rzeczywistości infekowały komputery złośliwym oprogramowaniem.

8. Sprawdzaj SMS-y autoryzacyjne

Jednym z najpopularniejszych narzędzi autoryzujących transakcje internetowe są SMS-y. Generowane w czasie rzeczywistym, unikalne dla każdej transakcji, zapewniają bezpieczeństwo realizowanej operacji. **Warto jednak dokładnie przeczytać SMS, który otrzymamy do potwierdzenia przelewu** i sprawdzić, czy rzeczywiście autoryzujemy tę operację, którą chcieliśmy. Jeśli mamy zainfekowany telefon, może się okazać, że złodzieje zdążyli dokonać podmiany.
Nie odpowiadaj na maile dotyczące prośby o weryfikację danych, a w szczególności nie przesyłaj pocztą elektroniczną swojego loginu i hasła dostępu.

Nie uruchamiaj Usługi eSKOK przy użyciu załączników lub odnośników otrzymanych pocztą e-mail lub w wiadomości SMS.

9. Sprawdzaj dane przed wysłaniem przelewu

Zanim wyślemy przelew, **powinniśmy dokładnie sprawdzić numer rachunku odbiorcy**. Specjaliści zajmujący się bezpieczeństwem wykryli wirusy, które podmieniają numery rachunków kopiowanych ze schowka. **Ostatnio pojawiła się też nowa odmiana szkodnika.** Podmienia numer rachunku już w trakcie ręcznego wpisywania znaków na klawiaturze. Przed wysłaniem przelewu, warto więc sprawdzić, czy numer, który przed chwilą wpisywaliśmy jest prawidłowy.

Nie kopiuj numerów rachunków bankowych do przelewów (metodą: „kopiuj-wklej”), ale wpisuj je samodzielnie i przed akceptacją dokładnie weryfikuj.

10. Kupuj w bezpiecznych sklepach

Jeśli płacimy za zakupy internetowe kartą płatniczą, należy zachować ostrożność. Nie powinno się korzystać z nieznanych, podejrzanych sklepów internetowych. Podobnie jak system bankowości internetowej, **także sklep powinien udostępniać bezpieczną stronę do wykonywania płatności** (obowiązkowe https:// w adresie). W przypadku kart płatniczych wrażliwe dane to numer, data ważności, oraz kody CVV i CVV2.

Bezpieczeństwo karty płatniczej

Karta płatnicza Visa SKOK jest wyposażona w mikroprocesor, który zapewnia najwyższe standardy bezpieczeństwa Twojej karty.

Zasady bezpieczeństwa

Bezpieczeństwo Twojej karty płatniczej zależy również od Ciebie!
Przedstawiamy zasady bezpieczeństwa, które powinny być przestrzegane przez użytkownika:

- podpisz kartę zaraz po jej otrzymaniu;
- nie udostępniaj karty i kodu PIN innym osobom!
- nie przechowuj karty razem z kodem PIN! Najlepiej, jeśli zapamiętasz kod PIN;
- przy zmianie kodu PIN należy pamiętać, by był on trudny do odgadnięcia dla innych, nie był prostą kombinacją cyfr, datą urodzenia itp.;
- przechowuj kartę z zachowaniem należytej staranności, karta to dostęp do Twoich pieniędzy na rachunku!
- przed potwierdzeniem transakcji zawsze sprawdź kwotę transakcji;
- przysłaniaj ręką klawiaturę bankomatu lub terminala podczas wprowadzania numeru PIN;
- kontroluj stan rachunku karty na bieżąco. Jeśli pojawią się podejrzane transakcje, należy niezwłocznie skontaktować się z Centrum Kart SKOK i zastrzec kartę;
- nie trać karty z zasięgu wzroku podczas dokonywania płatności;
- nie przechowuj karty w pobliżu urządzeń elektronicznych – może to spowodować jej uszkodzenie.

Odpowiedzialność za nieuprawnione transakcje

Posiadacz rachunku odpowiada za nieautoryzowane transakcje do wysokości równowartości w walucie polskiej 50 euro ustalonej przy zastosowaniu kursu średniego ogłaszanego przez NBP obowiązującego w dniu wykonania transakcji.
Powyżej tej kwoty odpowiedzialność przejmuje Wydawca.

Bezpieczne transakcje

Transakcje wykonywane kartą Visa SKOK, także zbliżeniowe, są autoryzowane (oznacza to, że sprawdzane są m.in.: status karty, dostępne środki oraz limity). Zapewnia to bezpieczeństwo środków zgromadzonych na rachunku i kontrolę wydatków.

Wszystkie transakcje wykonywane kartą wymagają Twojego potwierdzenia:

- jeśli wypłacasz gotówkę z bankomatu – podaj kod PIN;
- jeśli płacisz zbliżeniowo za drobne zakupy do 100 zł – zbliż kartę do czytnika po pojawieniu się kwoty transakcji na terminalu;
- jeśli płacisz zbliżeniowo i kwota transakcji jest równa lub wyższa niż 100 zł lub płacisz kartą w sposób tradycyjny – podaj kod PIN;
- jeśli robisz zakupy w internecie – podaj dane karty oraz trzycyfrowy kod CVV2.