Urząd Komunikacji Elektronicznej | UKE

Bezpieczna bankowość elektroniczna

Redakcja:

Departament Polityki Konsumenckiej, 2019

Urząd Komunikacji Elektronicznej (UKE)

Urząd Komunikacji Elektronicznej | UKE

Sesja bankowa

Bankowość elektroniczna jest dziś bardzo powszechna. Dostęp do rachunku, konta oszczędnościowego, produktów inwestycyjnych można uzyskać w każdym miejscu, o ile nawiązane jest połączenie internetowe. Za pomocą kilku kliknięć zrobimy przelew, czy zakupy. O bezpieczeństwo takich operacji musi zadbać również sam użytkownik. Nie jest to trudne i wystarczy zastosować się do kilku prostych zasad.

Aktualizacje

Każde oprogramowanie może zawierać wrażliwe obszary, które stanowią furtkę dla wszelkiego rodzaju ataków hakerskich i złośliwych aplikacji. Dlatego bardzo ważne jest, aby urządzenia, z których korzystamy z bankowości elektronicznej posiadały aktualne oprogramowanie.

Na komputerach trzeba sprawdzić wersję systemu operacyjnego i przeglądarki. Dodatkowo w przypadku urządzeń mobilnych bank dostarcza aplikację do bankowości elektronicznej. Ona również powinna mieć zainstalowane wszystkie aktualizacje.

Antywirus

Bezpieczeństwo w bankowości elektronicznej powinno być oparte także na programie antywirusowym (z najnowszymi aktualizacjami), jak również zaporach (firewall). Tego typu oprogramowanie może chronić nie tylko przed złośliwym oprogramowaniem, ale także przed przekierowywaniami na strony, które podszywają się pod witryny banków.

Urząd Komunikacji Elektronicznej | UKE

Weryfikacja autentyczności

Strony, które podszywają się pod oryginalne witryny nieznacznie różnią się w adresie. Należy zweryfikować, czy wpisany w pasku adres jest prawidłowy. Wchodząc na stronę banku powinniśmy samodzielnie wpisać adres, a nie klikać w linki prowadzące w mailach lub na stronach nie należących do banku. Banki nie wysyłają maili z linkami do swoich serwisów e-bankowości.

Każda strona bankowa musi mieć certyfikat SSL. Można go sprawdzić po prawej stronie paska adresowego (zielona lub czerwona kłódka). Fałszywe strony często wykorzystują spreparowane certyfikaty. Dlatego ważne jest, aby certyfikat miał jak najwięcej szczegółowych informacji (nazwa banku, wystawca certyfikatu, termin ważności).

Połączenie ze stroną banku musi być szyfrowane. Wskazuje na to prefiks https://

Oprócz szyfrowania https:// można zainstalować dedykowane bankowości elektronicznej aplikacje, które dodatkowo szyfrują połączenie.

Uwierzytelnienie użytkownika

Hasło do serwisu bankowości elektronicznej powinno być silne i unikalne. Najlepiej gdy składa się z małych i wielkich liter, cyfr oraz znaków specjalnych. Po zakończonej sesji zawsze należy się wylogować.

Dobrym zabezpieczeniem jest dwuetapowość uwierzytelnienia. Jeżeli bank oferuje takie rozwiązanie, warto z niego skorzystać. Po zalogowaniu przy wykonywaniu każdej operacji bank prosi o dodatkowe uwierzytelnienie kodem PIN otrzymanym na telefon.

Urząd Komunikacji Elektronicznej | UKE

Kontrola

Tuż przed ostateczną weryfikacją kodem PIN trzeba upewnić się, czy podany numer rachunku bankowego jest tym, na który chcemy wysłać przelew. Po zakończeniu operacji należy sprawdzić, czy właściwa kwota została pobrana z naszego konta.

Często banki udostępniają opcję powiadamiania SMS'em lub e-mailem o wszelkich aktywnościach na koncie. Gdy mamy taką możliwość zalecamy się jej włączenie.

Nieznane urządzenie lub sieć

Bezwzględnie należy unikać logowania i wykonywania operacji bankowych na urządzeniach, które nie są naszymi prywatnymi. Korzystając z bankowości elektronicznej powinniśmy mieć pełną kontrolę nad komputerem lub telefonem.

Niekiedy zachodzi konieczność zalogowania się do banku z prywatnego urządzenia, ale w publicznej sieci (np. w kawiarni, hotelu). Wówczas należy stworzyć połączenie VPN (Virtual Private Network). Instrukcja do każdego systemu operacyjnego wyjaśnia krok po kroku jak stworzyć takie połączenie.

Skimming

Czy wiesz czym jest skimming? Coraz więcej transakcji w sklepach realizowanych jest bezgotówkowo, z kolei oszczędności trzymane są na kontach bankowych i lokatach, a nie w domu. Te zmiany wpływają też na przestępczy półświatek. Powoli miejsce kieszonkowców zajmują „kieszonkowcy elektroniczni".

Urząd Komunikacji Elektronicznej | UKE

Co to jest skimming?

Przestępstwo skimmingu polega na kopiowaniu paska magnetycznego karty bankomatowej. Wyróżnić można trzy rodzaje skimmingu:

- kopiowanie karty przy okazji jej wykorzystania w bankomacie,
- kopiowanie karty w placówce handlowej,
- zdalne sczytywaniem karty gdy mamy ją przy sobie.

Ochrona przed skimmingiem?

Podczas operacji bankomatowych (wpłaty, wypłaty), przy wpisywaniu kodu PIN zawsze drugą ręką należy zasłaniać klawiaturę. Trzeba się także upewnić, czy osoby postronne nie znajdują się na tyle blisko, aby mogły podejrzeć PIN. Ważne jest także zwrócenie uwagi na wygląd bankomatu, czy nie są do niego doklejone lub przyczepione na magnes nietypowe elementy. Do skanowania kart wykorzystywane są nakładki, które przestępcy montują przy czytniku kart. Skanery takie z reguły wystają poza obudowę. Są najczęściej powiązane z nakładka na klawiaturę, której zadaniem jest sczytanie wpisywanego kodu PIN. Nakładka na klawiaturę, podobnie jak skaner, zazwyczaj wystaje poza obrys bankomatu. Niektóre bankomaty wyposażone są w antyskimmery. Są to wystające poza obudowę przezroczyste nakładki na czytnik kart, których zakończenie nie jest gładkie i ma uskok. Jeżeli cokolwiek podejrzanego znajduje się na bankomacie, najlepiej jest poinformować o tym bank lub policję. Odpowiednia informacja i dane kontaktowe są bankomacie.

Jeżeli w sklepie płacimy za zakupy kartą i wręczamy ją ekspedientowi, w żadnym momencie nie można jej tracić z oczu. W chwili nieuwagi możliwe jest szybkie zeskanowanie karty w przenośnym skanerze. Podobnie jak w bankomacie, wpisując kod PIN na terminalu, drugą ręką trzeba zasłonić

klawiaturę. Należy się także upewnić, że inne osoby w kolejce nie są zbyt blisko. Elektroniczni kieszonkowcy mogą być również wyposażeni w czytniki, które skanują karty na odległość. Aby zabezpieczyć się przed tym, dobrze jest nosić kartę w specjalnym etui, które uniemożliwia skanowanie. By kontrolować oszczędności warto zachowywać potwierdzenia operacji, które później można porównać z wyciągami generowanymi przez bank. Można również zastanowić się nad wyłączeniem możliwości płatności kartą bez potwierdzania kodem PIN.