Podstawowe zasady bezpiecznego korzystania z bankowości elektronicznej

Korzystamy z konta bankowego przez internet czy z kart płatniczych albo mobilnych rozwiązań płatniczych w różnych miejscach, nie zawsze bezpiecznych. Niekiedy robimy to szybko, nie zastanawiamy się, czy odpowiednio zadbaliśmy o bezpieczeństwo pieniędzy. Choć przez internet, dzięki karcie płatniczej czy płatności mobilnej, dokonujemy bezgotówkowych transakcji, to szkody – jeśli się na nie narazimy – będą realne i liczone w pieniądzu. Warto przypomnieć sobie o podstawowych zasadach bezpieczeństwa przy korzystaniu z bankowości internetowej.

W bankowości elektronicznej stosuje się wiele zabezpieczeń Banki wprowadziły: mechanizmy identyfikacji płatności, szyfrowanie transmisji, kody wysyłane w formie SMS, jednorazowe kody autoryzujące transakcje (tzw. „zdrapki"), limity transakcji czy automatyczne wygaszanie sesji po pewnym okresie nieaktywności. To nie oznacza jednak, że nie musimy być ostrożni. Bezpieczeństwo naszych oszczędności w wysokim stopniu zależy od nas samych.

Zabezpieczenie sieci bezprzewodowej w domu (biurze)

Korzystając z internetu, upewnijmy się, że sieć jest odpowiednio zabezpieczona. Dostęp powinien być chroniony hasłem, a szyfrowanie danych włączone (najlepiej za pomocą protokołu WPA2). To absolutne minimum, dobrze jest również, gdy sieć posiada filtrowanie adresów MAC (to znaczy, że mogą się do niej dołączyć jedynie komputery zapisane na liście użytkowników), a nazwa samej sieci jest niestandardowa albo ukryta.

Zabezpieczmy komputer, tablet lub telefon. Korzystajmy z legalnego oprogramowania, które jest na bieżąco aktualizowane. Pamiętajmy o zainstalowaniu programu antywirusowego i o tym, że również smartfon powinien go mieć. Postarajmy się o oprogramowanie *anty-malware*, które chroni nas m.in. przed programami *ransomware* (zaszyfrowującymi dane, za odblokowanie których hakerzy mogą zażądać zapłaty). Zwracajmy uwagę, aby aplikacje, które ściągamy na smartfon, tablet pochodziły ze sprawdzonego źródła.

Publiczne sieci i komputery

Unikajmy logowania się do konta z publicznej (otwartej) sieci internetowej, w kawiarni, na lotnisku czy w hotelu. Nie znamy zastosowanego tam poziomu zabezpieczeń sieci, nie wiemy, kto ma do niej dostęp. W miejscu, w którym korzysta z sieci wiele osób, istnieje ryzyko, że może być zainstalowane oprogramowanie rejestrujące loginy i hasła.

Wybór długiego i trudnego hasła

Gdy otwieramy konto internetowe, musimy ustalić hasło. Banki niekiedy mają automatyczną ocenę słabości lub siły naszej propozycji. Ważne, byśmy nie tworzyli prostych haseł, na przykład imienia czy daty urodzenia. Niekiedy proste słowa możemy zapisać od końca albo zamiast mianownika w rzeczownikach zastosować dopełniacz lub zapisać jako hasło czasownik.

Podpowiedzi na tworzenie silnych haseł jest tyle, ile wyobraźni ludzkiej. Jedna to wykorzystanie wierszyka, jaki znamy. Wybieramy pierwszą literę z każdego wyrazu i układamy ciąg znaków. Inna to zapisanie po każdej literze (raz małej, raz dużej) cyfry. Ważne, by nie pogubić się w kombinacjach i nie zapisać ich w miejscu łatwym do znalezienia. Jeśli korzystamy z tego samego hasła na komputerze stacjonarnym i smartfonie, sprawdźmy, czy znaki, które wprowadzamy z klawiatury komputera, potrafimy wprowadzić też z telefonu. Hasło powinno być odpowiednio długie, co oznacza, że powinno mieć zazwyczaj od 8 do 14 znaków. Każdy dodatkowy znak zwiększa siłę hasła. Ponadto, jeżeli system na to pozwala, stosujmy spacje. Tak powstają frazy złożone z kilku słów, które są trudniejsze do odgadnięcia przez niepowołane osoby, a łatwe dla nas do zapamiętania. Im bardziej różnorodne znaki, tym trudniejsze do odgadnięcia hasło (litery, cyfry i symbole). Przy tworzeniu należy korzystać z całej klawiatury, a nie tylko z liter.

Hasła nie wolno ujawniać innym osobom. Nie należy podawać go w wiadomościach e-mail bądź też w odpowiedzi na żądanie, które zostało przesłane pocztą e-mail. Co jakiś czas, pół roku – rok, należy je zmieniać.

Bezpieczeństwo logowania

Nie klikajmy w linki zawarte w listach e-mail, które wysłano rzekomo w imieniu banku. Banki nigdy nie proszą nas o dane. Nie wysyłają do klientów pytań dotyczących haseł lub innych poufnych danych ani próśb o ich aktualizację. Jeśli dostaniemy SMS lub e-mail w tej sprawie, nie odpowiadajmy na niego, bo jest to próba wyłudzenia danych przez oszustów.

Zawsze używajmy bezpośredniego adresu strony internetowej banku. W celu zapewnienia bezpiecznego dostępu do konta, należy wejść na stronę banku (samodzielnie wprowadzić adres), kliknąć odnośnik 'logowanie', a w pasku adresu u góry przeglądarki sprawdzić, czy widnieje tam faktyczny adres banku, zaczynający się od 'https' – to oznacza, że połączenie jest szyfrowane. Często w pasku adresu przeglądarki widnieje także ikona kłódki. Po skończonym korzystaniu z bankowości trzeba pamiętać o wylogowaniu się. Jeśli mamy możliwość ustawienia w swojej bankowości internetowej tak zwanego obrazka bezpieczeństwa, zróbmy to. Jest to małe, charakterystyczne zdjęcie (np. krajobrazu, figura geometryczna, znak graficzny), które wyświetla się podczas logowania, już po podaniu numeru klienta, a przed podaniem hasła. Obrazek bezpieczeństwa pozwala rozpoznać, czy strona jest autentyczna, czy fałszywa – służąca do tzw. *phishingu*, czyli próby przechwycenia danych.

Potwierdzenia kodem SMS

Większość banków wymaga od nas podania jednorazowego kodu potwierdzającego wykonanie operacji. Jednym z najpopularniejszych sposobów na zwiększenie bezpieczeństwa transakcji są jednorazowe kody potwierdzenia w formie SMSów. W celu potwierdzenia np. przelewu, tuż przed jego wysłaniem otrzymujemy od banku SMS zawierający kod do wpisania. Należy sprawdzić, czy wszystkie dane w SMSie i na ekranie komputera (dla naszej transakcji) są identyczne. Jeżeli dane nie zgadzają się, należy przerwać wykonywanie operacji i jak najszybciej przeskanować swój komputer pod kątem wirusów oraz zawiadomić o takiej sytuacji bank.

Inne zabezpieczenia

Sprawdzajmy datę ostatniego logowania do bankowości internetowej – zweryfikujmy, czy rzeczywiście w tym terminie korzystaliśmy z bankowości internetowej. Jeśli nie – powinniśmy zgłosić taki fakt do banku.

Robiąc przelewy internetowe, co jakiś czas sprawdzajmy, czy numery rachunków w przelewach zdefiniowanych wcześniej nie zostały zmienione, podmienione; nie kopiujmy numerów rachunków bankowych do przelewów (kopiuj – wklej), ale wpisujmy je samodzielnie i dokładnie weryfikujmy.

Ustawmy limity dla transakcji kartami płatniczymi i dla dziennych oraz miesięcznych limitów wypłat z konta. Jeśli zostawimy zbyt wysokie, a ktoś ukradnie nasze dane, łatwiej będzie mu nas okraść.

Karty płatnicze

Do karty płatniczej (debetowej lub kredytowej) dodawany jest czterocyfrowy kod PIN służący do potwierdzania transakcji gotówkowych (wypłat gotówki w bankomacie) i bezgotówkowych (w sklepach stacjonarnych). Należy go zapamiętać i pod żadnym pozorem nie zapisywać na karcie ani nie udostępniać innym osobom. Trzeba także uważać przy płaceniu lub wypłacaniu gotówki z bankomatu. Przed skorzystaniem z bankomatu upewnijmy się, że nie ma na jego obudowie żadnych podejrzanych elementów, które są wykorzystywane przez oszustów do dokonania przestępstwa zwanego *skimmingiem*. Polega ono na nielegalnym kopiowaniu zawartości pasków magnetycznych kart płatniczych (numer karty i jej data ważności) i przechwytywaniu numerów PIN. Szczególną uwagę powinniśmy zwrócić na następujące elementy:

- skimmer – urządzenie będące nakładką montowaną na czytniku kart w bankomacie, przy użyciu którego kopiowane są dane z paska magnetycznego karty
- nakładka na klawiaturę – pogrubiona i wystająca ponad powierzchnię blatu bankomatu klawiatura może świadczyć o zainstalowaniu specjalnej nakładki umożliwiającej przechwycenie i zarejestrowanie wprowadzanych przez klientów numerów PIN,
- ścianka bankomatu – może być w niej zainstalowana przez oszustów kamera rejestrująca wprowadzane przez klientów numery PIN.

Pilnujmy kart płatniczych – nie zostawiajmy ich bez kontroli, zwłaszcza w obecności osób trzecich. Nie róbmy

kartom zdjęć i nie umieszczajmy ich w sieci, zwłaszcza numerów CVV2 lub CVC2 (ostatnich 3 cyfr numeru umieszczonego na pasku do podpisu na odwrocie karty), które służą do potwierdzania płatności kartą w internecie.

Włączmy usługę 3D-Secure podnoszącą bezpieczeństwo transakcji kartami w internecie, jeśli bank to umożliwia. Usługa ta polega na tym, że płatność trzeba potwierdzić dodatkowym jednorazowym kodem 3D-Secure. Taki kod klienci otrzymują SMS-em wysłanym na numer telefonu komórkowego. Tylko potwierdzenie transakcji otrzymanym kodem umożliwia sfinalizowanie transakcji. Warto dodać, że usługa zadziała tylko wtedy, gdy jest wdrożona zarówno przez bank, jak i przez agenta rozliczeniowego, który uczestniczy w transakcji.

Na bieżąco przeglądajmy historię rachunku i operacji na każdej karcie płatniczej pod kątem podejrzanych transakcji. Zapiszmy sobie numer centrum obsługi klienta banku, gdzie można zastrzec kartę, zgłosić jej kradzież lub zgubienie.

Źródło artykułu oraz ikografiki: www.bankier.pl

Artykuł opublikowany na portalu bankier.pl dnia 2017-05-08