

Ostrzeżenie przed dopuszczaniem pośredników do rachunku bankowego w płatnościach internetowych

Urząd Komisji Nadzoru Finansowego (UKNF) zwraca uwagę na ryzyko związane z podawaniem danych umożliwiających logowanie do rachunku bankowego, zlecenie przelewów oraz pobieranie historii rachunku podmiotom innym niż bank, w którym prowadzony jest dany rachunek.

UKNF przypomina, że podstawową zasadą bezpieczeństwa w bankowości internetowej jest niepodawanie w żadnym wypadku komukolwiek danych pozwalających na dostęp do rachunku bankowego, gdyż grozi to utratą środków.

Niektóre sklepy internetowe umożliwiają nabywcom płatność zgodnie z następującym schematem: po dokonaniu zakupu towaru lub usługi na platformie internetowej i przejściu do etapu płatności, klient jest przekierowywany na stronę pośrednika, gdzie podaje dane do logowania do własnego rachunku bankowego (login/identyfikator oraz hasło). Jako że w zdecydowanej większości banków warunkiem realizacji zleconej płatności online jest podanie dodatkowego hasła jednorazowego (otrzymywanego w postaci generowanego automatycznie i przesyłanego sms-em w czasie rzeczywistym lub w postaci karty haseł jednorazowych), kolejnym krokiem jest podanie przez klienta tego hasła jednorazowego. Po otrzymaniu danych, pośrednik – zalogowany za pośrednictwem klienta na jego rachunek bankowy – inicjuje realizację płatności z rachunku klienta na rachunek dostawcy towaru lub usługi.

Oznacza to, że jeśli nabywca towaru lub usługi wybierze tę metodę płatności, zobowiązany jest:

- wskazać bank, w którym posiada rachunek i z którego zamierza wysłać płatność za towar lub usługę,
- podać pośrednikowi login i hasło do swojego konta bankowego; dodatkowo, gdy transakcja wymaga podania hasła jednorazowego (a co do zasady – wymaga), należy podać pośrednikowi również to hasło.

Ponadto, pośrednik często zastrzega sobie prawo do odczytania salda konta posiadacza rachunku oraz sprawdzenia historii transakcji na rachunku, w celu kontroli, czy na rachunku przeprowadzane były uprzednio transakcje za jego pośrednictwem.

Po stronie klienta skorzystanie z tej formy płatności wiąże się z następującymi czynnikami ryzyka:

- 1. Ryzykiem naruszenia umowy o prowadzenie rachunku bankowego oraz regulaminu,** który stanowi integralną część umowy o rachunek. Zgodnie z postanowieniami umów i regulaminów obowiązujących w bankach działających w Polsce, klient jest co do zasady zobowiązany do zachowania poufności i ochrony przed dostępem osób trzecich indywidualnych danych identyfikacyjnych, czyli loginu i hasła do strony transakcyjnej banku, z którego usług korzysta. Ten sam zakaz obejmuje też hasła jednorazowe. Tymczasem, w powyższym schemacie pośrednik w realizacji e-płatności uzyskuje dostęp do tych danych, a tym samym dostęp do rachunku i wszelkich informacji, do jakich normalnie dostęp ma wyłącznie jego właściciel.
- 2. Ryzykiem utraty prawa do reklamacji nieautoryzowanych transakcji.** Ujawnienie danych logowania może stanowić naruszenie umowy o prowadzenie rachunku i regulaminu, które mogą skutkować zwolnieniem banku z odpowiedzialności za ochronę środków zgromadzonych na rachunku. W rezultacie, w razie wystąpienia na rachunku nieautoryzowanych transakcji, klient może bezpowrotnie utracić szansę na uzyskanie odszkodowania.
- 3. Ryzykiem nieautoryzowanego przechwycenia danych logowania,** a w konsekwencji ryzykiem utraty kontroli nad środkami przechowywanymi na rachunku oraz nad danymi osobowymi i zakresem ich wykorzystania, w szczególności w zakresie danych o dokonywanych na rachunku operacjach i realizowanych transakcjach, które potencjalnie mogą zostać pozyskane i wykorzystane przez osoby trzecie.