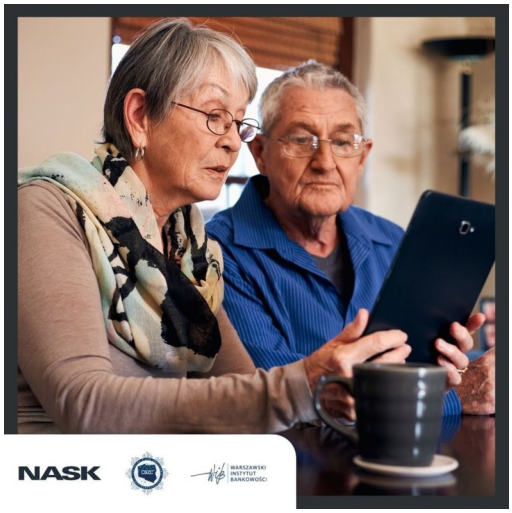
Bezpieczna bankowość elektroniczna

Bankowość elektroniczna, czyli możliwość wykonywania operacji bankowych za pomocą komputera lub smartfona to dziś podstawowa usługa i zaleta posiadania konta bankowego i karty płatniczej. Dzięki niej możemy realizować zakupy przez internet w dowolnym miejscu na świecie, opłacać rachunki a także kontrolować stan swojego budżetu bez wychodzenia z domu, przez całą dobę, 7 dni w tygodniu.



O ile same systemy bankowości elektronicznej posiadają wiele zaawansowanych rozwiązań technologicznych i są bezpiezpieczne, to jednak musimy zachować czujność i rozwagę by przypadkiem nie trafić na fałszywe bramki płatności lub fałszywe strony logowania podszywające się pod nasz bank.
Cyberprzestępcy tworzą łudząco podobne strony do tych oryginalnych a następnie próbują zmanipulować odbiorców, by dokonywali płatności za pośrednictwem spreparowanych stron. Wówczas nasze dane tj. login i hasło zamiast do banku, trafiają w ręce przestępców. Dzięki temu mają dostęp do naszego konta i będą próbować skraść wszystkie nasze oszczędności.

Poniżej kilka przykładowych sytuacji, w których możemy otrzymać link do fałszywych bramek płatności:

- Fałszywe sklepy internetowe, które kuszą bardzo atrakcyjnymi promocjami i cenami popularnych produktów a tak naprawdę działają w celu wyłudzenia od nas danych karty płatniczej lub danych do logowania, które podajemy by opłacić zamówienie.
- Fałszywe wiadomość SMS z wezwaniem do szybkiego uregulowania płatności. Taka wiadomość może dotyczyć m.in. nieopłaconej faktury, dopłaty do przesyłki kurierskiej, konieczności opłacenia zaległego podatku itp.)
- Fałszywe wiadomości rozsyłane m.in. za pośrednictwem mediów społecznościowych np. od naszego znajomego lub członka rodziny. W takiej wiadomości zazwyczaj znajduje się prośba o wsparcie finansowe z powodu nioczekiwanego wydarzenia (wypadek, awaria, brak portfela). Tutaj należy zachować szczególną czujność - konto znajomego mogło zostać przejęte przez przestępców a wiadomość została automatycznie rozesłana do wszystkich osób w bazie kontaktów, czego właściciel konta może nie być świadomy.
- Fałszywa wiadomość o konieczności aktualizacji danych do logowania np. z powodu ataku hakerskiego na bank i wycieku danych do logowania.
- Fałszywe reklamy w wyszukiwarkach, które prowadzą do nieprawdziwych stron internetowych, łudząco podobnych do tych oficjalnych. Oszuści najczęściej wykorzystują wizerunek instytucji finansowych (m.in. banków), i na pierwszy rzut oka, ich strony wyglądają jak te prawdziwe. Dlatego zawsze należy weryfikować adres domeny, na którą zostajemy przekierowani, zwłaszcza wtedy, gdy zostajemy proszeni o podanie swoich wrażliwych danych lub zalogowanie się do usług internetowych (np. bankowość elektroniczna)
- Cyberprzestępcy szukają swoich ofiar także w lokalnych serwisach sprzedażowych. Kontaktują się z osobą, która wystawiła ogłoszenie, nawiązują kontakt i informują, że są zainteresowani zakupem. Proszą abyśmy podali dane swojej karty płatniczej, tłumacząc, że jest to niezbędne w celu szybkiej „finalizacji transakcji”.

Jak się chronić przed fałszywymi bramkami płatności?

- Zwracaj uwagę na adres witryny - czy nie zwiera błędów, literówek, znaków specjalnych. Jeśli cokolwiek budzi Twoją wątpliwości lepiej zrezygnuj z transakcji.
- Nigdy nie loguj się do konta bankowego za pośrednictwem linków otrzymanych w mailu, w wiadomości SMS lub za pośrednictwem komunikatora. Do bankowości elektronicznej loguj się bezpośrednio z oficjalnej strony banku. Najbezpieczniej wpisz ją ręcznie w pasu przeglądarki.
- Czytaj uważnie wszelkie powiadomienia z banku, zwłaszcza gdy dotyczą autoryzacji płatności. Jeśli cokolwiek budzi Twój niepokój - skontaktuj się z bankiem.
- Zawsze weryfikuj wiarygodność osoby, która się z Tobą kontaktuje i nakłania Cię do podjęcia działań związanych z płatnością. Nie udostępniaj swoich danych osobowych lub finansowych, osobom, których nie znasz. Jeśli masz jakiekolwiek wątpliwości, zadzwoń do banku lub zaufanej osoby i zapytaj o radę.

Na co jeszcze warto zwrócić uwagę by bezpiecznie korzystać z bankowości elektronicznej?

Bezpieczne hasła do logowania

Stosuj bezpieczne hasła czyli składające się z minimum 14 dużych i małych znaków. Zaleca się stosowanie kombinacji przypadkowych słów. W ten sposób Tobie będzie łatwiej zapamiętać hasło a oszustom trudniej je złamać. Dobry przykład to: NaKolacjeZjemZielonePomidory. Po więcej informacji nt. tworzenia bezpiecznych haseł odsyłamy do strony CERT Polska - link.

Różne usługi i różne hasła

W sytuacji gdy posługujesz się jednakowym hasłem do wszystkich usług i zostanie one złamane (np. wycieknie w wyniku cyberataku), przestępcy automatycznie będą próbować wykorzystać je także w innych miejscach i serwisach. Dlatego zadbaj o to, żeby stosować unikatowe hasła do każdej usługi, a w szczególności do najważniejszych kont takich jak: poczta, bank czy media społecznościowe.

Weryfikacja dwuetapowa

To dodatkowe zabezpieczenie używane w celu ochrony naszych kont internetowych przed nieautoryzowanym dostępem. Oprócz standardowego hasła, które zazwyczaj używamy do logowania, musimy wprowadzić dodatkowy kod np. wysyłany na telefon.Dzięki zastosowaniu weryfikacji dwuetapowej, nawet jeśli ktoś pozna Twoje hasło, nie będzie w stanie uzyskać dostępu do konta bez drugiego czynnika uwierzytelniającego. Takie rozwiązanie zwiększa poziom bezpieczeństwa Twoich transakcji finansowych.

Dodatkowe kody autoryzujące i limity transakcji

Zorientuj się w banku, w jaki sposób możesz zabezpieczyć finanse przed nieautoryzowanymi transakcjami. Zazwyczaj odbywa się to za pomocą kodów autoryzujących przesyłanych na telefon lub autoryzacji za przy pomocy aplikacji mobilnych. Wówczas przed każdą transakcją będziesz proszony o podanie jednorazowego kodu. Taki kod będzie ważny tylko przez kilka minut.

Ustal także dzienne limity transakcji oraz limity maksymalnych kwot na koncie bankowym. W sytuacji gdy dojdzie do nieautoryzowanej transakcji np. w wyniku kradzieży danych karty płatniczej, limity będą chronić Cię przed utratą wszystkich oszczędności.

Zdrowy rozsądek przede wszystkim

W każdej sytuacji dotyczącej płatności internetowych zachowaj szczególną uważność i zasadę ograniczonego zaufania.

Trudno przewidzieć wszystkie scenariusze działań i sposoby manipulacji stosowane przez cyberprzestępców, gdyż są one nieustannie modyfikowane i „udoskonalane". Jest jednak jedna uniwersalna i ponad czasowa zasada: zdrowy rozsądek przede wszystkim!

***

Materiał przygotowany w ramach kampanii pt. *#Halo! Tu cyberbezpieczny Senior*! przygotowanej przez NASK, Centralne Biuro Zwalczania Cyberprzestępczości w Policji oraz Warszawski Instytut Bankowości.

***