Bezpieczeństwo w internecie

Poznaj najważniejsze zasady bezpieczeństwa w internecie.

Pamiętaj! Jeśli coś budzi Twoją wątpliwość lub nie działa tak jak powinno, jak najszybciej skontaktuj się z infolinią banku.

Bankowość internetowa

- Nigdy nie loguj się do bankowości internetowej z linku, który przyszedł do Ciebie mailem lub SMS-em, ani poprzez link z wyszukiwarki. Wpisuj adres strony logowania ręcznie lub korzystaj z przycisku logowania na oficjalnej stronie banku.
- Sprawdzaj adresy stron www, na których się logujesz, oraz ważność ich certyfikatów. Adres strony logowania powinien zaczynać się od ***https*** (oznacza to bezpieczne połączenie internetowe).
- Zadbaj o skomplikowane hasła, unikatowe i trudne do odgadnięcia przez postronne osoby.
- Nie używaj tego samego hasła do różnych kont.
- Nie zapisuj haseł na kartkach ani w plikach na komputerze.
- Login i hasło do bankowości oraz numery kart to dane, które powinny być znane tylko Tobie. Nigdy nie podawaj ich innym.
- Nie loguj się przez publiczną, niezabezpieczoną sieć wi-fi lub hotspot do bankowości internetowej czy aplikacji mobilnej.
- Nie loguj się do bankowości na urządzeniach publicznie dostępnych, np. w kafejkach czy w hotelach.
- Pamiętaj aby po każdej sesji wylogować się z bankowości internetowej.
- Ustaw bezpieczne limity operacji dla przelewów, płatności kartami i wypłat gotówki.

Komputer i telefon

- Regularnie aktualizuj oprogramowanie na komputerze i telefonie (system, aplikacje, przeglądarkę, antywirusy).
- Używaj zapory sieciowej (firewall) i systematycznie skanuj komputer programem antywirusowym.
- Nie instaluj na komputerze i smartfonie oprogramowania z nieznanych źródeł.
- Nie podłączaj zewnętrznych nośników danych (np. pendrive) do swojego komputera, jeśli nie masz pewności co do ich bezpieczeństwa. Podobnie z podłączaniem telefonu do komputera.
- Pobieraj aplikację mobilną banku i jej aktualizacje wyłącznie z autoryzowanych sklepów: Google Play i App Store.
- Zawsze blokuj dostęp do telefonu i komputera. Zabezpiecz telefon hasłem, wzorem, odciskiem palca lub Face ID.
- W razie utraty karty lub telefonu z aktywną aplikacją – od razu je zablokuj. Kartę możesz zablokować przez bankowość internetową lub mobilną, a aplikację przez infolinię banku.

Podejrzany kontakt

- Zastanawia Cię wiadomość o dziwnym zamówieniu lub zaległej płatności? Przed podjęciem czynności w niej wskazanej skontaktuj się z biurem obsługi klienta firmy, która wysłała tę wiadomość.
- Nie otwieraj załączników w niespodziewanych mailach, jeśli nie wiesz co może w nich być.
- Nie klikaj w linki i nie pobieraj żadnych aplikacji, jeśli nie znasz nadawcy wiadomości.
- Dokładnie czytaj powiadomienia o transakcjach, w tym SMS-y – jeśli coś się nie zgadza, nie zatwierdzaj operacji.
- Jeżeli dzwoni do Ciebie przedstawiciel banku, ale nie masz pewności, że nim jest – zerwij połączenie. Potem samodzielnie zadzwoń na naszą infolinię.
- Nie przekazuj kodu BLIK nikomu, nawet znajomemu.
- Kupujesz w nowym sklepie? Poszukaj opinii na jego temat (z różnych źródeł) i sprawdź czy adres sklepu na pasku przeglądarki jest zgodny z nazwą sklepu.
- Nie podawaj PIN-u do karty podczas zakupów w internecie. Do potwierdzenia transakcji kartą w internecie nigdy nie jest wymagane podanie PIN.
- Jeśli płacisz kartą płatniczą w sklepie internetowym, który obsługuje 3D Secure, wymagane może być dodatkowe potwierdzenie transakcji. Takie zakupy potwierdzisz na dwa sposoby: w aplikacji mobilnej SGB Mobile lub przez udzielenie odpowiedzi na pytanie weryfikacyjne oraz podanie hasła 3D Secure (jednorazowego kodu SMS), które otrzymasz na numer telefonu komórkowego podany przez Ciebie do kontaktu w Twoim Banku. Dowiedz się więcej o 3D Secure >>