Zasady bezpiecznego korzystania z bankowości elektronicznej

1. **Nigdy nie podajemy danych do logowania do bankowości elektronicznej-** poprzez mail, telefon, list. **Pamiętaj !!! – bank nigdy nie prosi klienta o takie dane**. Jeśli ktoś żąda od nas takich informacji, to powinien to być dla nas sygnał ostrzegawczy, nie powinniśmy ich ujawniać, lecz niezwłocznie o zaistniałej sytuacji powiadomić bank.
2. **Zabezpieczamy telefon, komputer, tablet-** wszystkie media z których korzystamy z bankowości elektronicznej, powinny być odpowiednio zabezpieczone. Korzystamy z legalnego oprogramowania, które jest na bieżąco aktualizowane. Wykorzystujemy programy antywirusowe. Pamiętamy, że również smartfon powinien mieć zainstalowany program antywirusowy. Postarajmy się o oprogramowanie antymalware, które chroni nas też przed programami typu ransomware, czyli takimi, które zaszyfrują nasze dane i zażądają okupu za ich odblokowanie.
3. **Nie otwieramy podejrzanych maili i załączników-** nie otwieramy załączników nawet od znanych nam osób, jeśli się ich nie spodziewaliśmy.
4. **Staramy się bacznie przyglądać stronie banku-** warto się jej dobrze przyjrzeć i zapamiętać jej cechy szczególne, aby ustrzec się sytuacji, że zostaniemy przekierowani na łudząco podobną stronę, ale będącą pod kontrolą przestępcy, a nie banku. Taka fałszywa strona może zawierać np. linki bezpośrednio odsyłające do zarażonych plików, które infekują system.
5. **Czego musimy przestrzegać przy logowaniu do bankowości elektroniczne-** na stronę bankowości nigdy nie wchodzimy korzystając z przesłanych pocztą elektroniczną linków. Zawsze używamy adresu bezpośredniego. Przy logowaniu zwracamy uwagę na dwa elementy: szyfrowanie połączenia i certyfikat bezpieczeństwa. Symbol kłódki w pasku adresu przeglądarki oraz „https" na początku adresu strony, na której się logujemy to elementy, które muszą być na stronie. Klikając na kłódkę możemy sprawdzić certyfikat i jego ważność. Musi być ważny i wydany dla Państwa banku. Brak litery „s", czyli „http://" a nie „https://" świadczy o braku szyfrowania, czyli o tym, że dane są transmitowane przez sieć tekstem jawnym, co naraża nas na ogromne niebezpieczeństwo.
6. **Po zakończeniu czynności bankowych wylogowujemy się z aplikacji bankowej.**
7. **Sprawdzamy datę ostatniego logowania do bankowości elektronicznej-** sprawdźmy, czy rzeczywiście w tym terminie korzystaliśmy z bankowości elektronicznej. Jeśli nie- powinniśmy zgłosić taki fakt do banku.

8. **Tworzymy silne hasło do konta-** musi być ono unikalne, możliwie skomplikowane, ale dające się zapamiętać. Pamiętajmy, aby go nikomu nie udostępniać. Zmieniamy je natychmiast, jeśli tylko uważamy, że ktoś mógł je podejrzeć. Aby ułatwić sobie zapamiętanie długich, skomplikowanych haseł można stosować różne sztuczki. Np. bierzemy jakiś tekst, wierszyk, który znamy na pamięć. Wybieramy sobie pierwszą literę z każdego wyrazu i układamy ciąg znaków. Możemy dołożyć cyfry, zmieniać litery na duże i małe, wykorzystywać znaki alfanumeryczne.
9. **Weryfikujemy kody wysyłane przez SMS-** cyberprzestępcy do potwierdzenia operacji potrzebują kodu wysyłanego przez SMS. Należy pamiętać, aby dokładnie czytać takie SMS, zawsze sprawdzać, czy zgadza się numer rachunku odbiorcy oraz kwota operacji.
10. **Zrezygnujmy z listy kodów jednorazowych-** jeśli korzystamy z autoryzacji przelewów za pomocą listy kodów jednorazowych poprośmy w banku o zmianę na autoryzację SMS.
11. **Nie korzystamy z otwartych sieci WIFI-** dostęp do sieci WIFI w galeriach handlowych, dworcach, lotniskach jest przeważnie darmowy, ale korzystanie z tego typu sieci do prowadzenia operacji bankowych jest raczej nieodpowiedzialne. Tego rodzaju sieci są stosowane przez cyberprzestępców jako idealne miejsce do roznoszenia różnego rodzaju oprogramowania, które trudno nazwać przyjaznym. Korzystajmy z sieci WIFI, tylko wtedy, gdy gwarantują one odpowiedni poziom bezpieczeństwa.
12. **Rozważnie korzystamy z sieci Internet-** korzystając ze sklepów internetowych, serwisów aukcyjnych, wybierajmy te, które mają dobre opinie, wysokie oceny w rankingach. Strony zawierające treści pornograficzne, pirackie oprogramowanie są bardzo niebezpieczne. Często korzystanie z dziwnych, podejrzanych (np. sugerujących jakieś wyjątkowe okazje) linków na stronie może doprowadzić do infekcji malwarem, czy ransomware. Linki są tak skonstruowane, że bezpośrednio odsyłają do zarażonych plików, które infekują system.
13. **Uważnie korzystajmy z przeglądarek-** zwracajmy uwagę na popularne wtyczki do przeglądarki. Wystarczy zadbać, żeby były one aktualne, bo cyberprzestępcy przeważnie wykorzystują podatności, dla których producenci wydali już poprawione wersje oprogramowania.
14. **Pilnujemy kart-** nie zostawiamy kart bankomatowych, kart kredytowych, bez kontroli, zwłaszcza w obecności osób trzecich. Nie robimy kartom zdjęć i nie umieszczamy w Sieci, zwłaszcza numerów CVV2 lub CVC2 (ostatnich 3 cyfr numeru umieszczonego na pasku do podpisu na odwrocie karty).

15. **Na bieżąco przeglądamy historię rachunku i operacji na każdej karcie płatniczej pod kątem podejrzanych transakcji-** zapiszmy sobie numer centrum obsługi klienta Naszego Banku, gdzie można zastrzec kartę, zgłosić kradzież, zgubienie.
16. **Sprawdzamy bankomaty-** sprawdzamy bankomat, czy czytnik kart nie wygląda podejrzanie (najczęściej w oryginalnych bankomatach wlot na karty płatnicze jest wklęsły), czy klawiatura bankomatu jest równa lub lekko obniżona w stosunku do poziomu obudowy, czy do bankomatu nie są doklejone jakieś podejrzane urządzenia. Wprowadzając PIN, należy zawsze zasłaniać klawiaturę ręką, portfelem i to tak, aby nie można było PIN-u podejrzeć z żadnej strony. W miarę możliwości korzystamy z bankomatów zlokalizowanych wewnątrz obiektów usługowo-handlowych, które są obciążone mniejszym ryzykiem modyfikacji do celów przestępczych. Często i systematycznie kontrolujemy stan salda rachunku oraz historię transakcji. PIN do bankomatu nie powinien składać się z cyfr odpowiadających dacie urodzenia, czy też innym datom łatwym do odgadnięcia.
17. **Włączamy powiadomienia SMS-** warte rozważenia jest włączenie usługi dodatkowych wiadomości od banku, które informują o zmianach na rachunku, wypłatach, wpłatach. W przypadku niepokojących zdarzeń możemy szybko zareagować.
18. **Bezpiecznie dokonujemy przelewów internetowych-** co jakiś czas sprawdzamy, czy numery rachunków w przelewach zdefiniowanych wcześniej nie zostały zmienione, podmienione; nie kopiujemy numerów rachunków bankowych do przelewów (kopiuj-wklej), ale wpisujemy je samodzielnie i dokładnie weryfikujemy; przed potwierdzeniem transakcji przelewu weryfikujemy zgodność numeru konta odbiorcy oraz numeru, który jest w kodzie potwierdzającym transakcję. Przelewów dokonujemy tylko z „pewnych komputerów", czyli nie robimy ich z kawiarenek internetowych, czy innych przygodnych miejsc.
19. **Ustawiamy limity dla transakcji kartami płatniczymi-** ustawiając zbyt wysokie limity dla kart debetowych i kredytowych, szczególnie z funkcją zbliżeniową, ułatwiamy złodziejom kradzież środków. Może warto przemyśleć obniżenie tych limitów, aby ograniczyć straty przed zastrzeżeniem karty. Z uwagi na to, że kwestia bezpieczeństwa płatności zbliżeniowych jest w dalszym ciągu kontrowersyjna, każdy powinien rozważyć, czy chce korzystać z tego rozwiązania technicznego. Istnieją prawne możliwości rezygnacji z tego typu kart, lub wymiany karty na kartę z PIN kodem.
20. **Dbamy o swój telefon, smartfon-** logujemy się do mobilnych aplikacji bankowych tylko wtedy, gdy z nich korzystamy. Po skorzystaniu, wylogowujemy się.
21. **W miarę potrzeby kontaktujemy się z bankiem-** często zdarza się, że w trakcie korzystania z Internetu i konta bankowego, coś nas zaniepokoi: dziwne wiadomości

SMS, email, czy komunikat w systemie bankowym. W takiej sytuacji należy bez wahania skontaktować się z bankiem, bo być może ktoś usiłuje dostać się do naszego rachunku. Takich sytuacji nie wolno bagatelizować.

22. **Dbamy o dokumenty z naszymi danymi osobowym-** zwracajmy uwagę, komu powierzamy swoje dane: adres, telefon, czy numer i serię dowodu osobistego. Takie informacje są bardzo cenne dla przestępców, bo dzięki nim mogą założyć konto czy uzyskać kredyt. Każde dane można wykorzystać, dlatego wyróbmy sobie nawyk niszczenia tego typu informacji. Nie wyrzucajmy do śmietnika niepotrzebnych faktur, rachunków, pism z banków. Najlepiej je spalić, wrzucić do niszczarki. Podobnie, korzystając z bankomatu, nie wyrzucajmy papierowego potwierdzenia. Albo go nie drukujmy, albo zniszczmy lub weźmy do domu. Pilnujmy naszego dowodu osobistego, paszportu, prawa jazdy. Ich kradzież, zagubienie należy niezwłocznie zgłosić do najbliższego banku. Informacje o utracie powyższych dokumentów trafiają do wspólnej bazy danych „Dokumenty zastrzeżone”, która jest dystrybuowana do wszystkich placówek bankowych.