**Zasady ogólne**

**1. Pamiętaj, żaden bank nigdy nie wysyła do swoich klientów pytań dotyczących haseł lub innych poufnych danych ani próśb o ich aktualizację.**
Banki nigdy nie podają w przesyłanych wiadomościach linków do stron transakcyjnych. Listy, wiadomości e-mail lub telefony w takich sprawach należy traktować jako próbę wyłudzenia poufnych informacji. Nie odpowiadaj na nie przekazując swoje poufne dane. Bezzwłocznie skontaktuj się ze swoim Bankiem i poinformuj o zdarzeniu.

**2. Sprawdź na stronie Twojego Banku jakie zabezpieczenia stosowane są w serwisie internetowym.**Przy każdym logowaniu bezwzględnie stosuj się do zasad bezpieczeństwa tam opublikowanych. W przypadku pojawienia się jakichkolwiek nieprawidłowości natychmiast skontaktuj się z pracownikiem Banku.

**3. Komputer lub telefon komórkowy podłączony do Internetu musi mieć zainstalowany program antywirusowy i musi on być na bieżąco aktualizowany.**
Niezbędna jest również aktywacja istotnych modułów w pakiecie ochronnym takich jak monitor antywirusowy, skaner poczty czy firewall. Częstym błędem jest wyłączanie wspomnianych modułów w celu redukcji obciążenia systemu.

**4. Dokonuj płatności internetowych tylko z wykorzystaniem „pewnych komputerów”.**Nie dokonuj płatności internetowych z komputerów znajdujących się w miejscach publicznych np. w kawiarenkach internetowych lub na uczelni.

**5. Skontaktuj się ze swoim dostawcą Internetu w celu upewnienia się, że korzysta on bezpiecznych kanałów dystrybucji tej usługi.**Zwracaj szczególną uwagę na jakość i bezpieczeństwo usług internetowych dostarczanych przez Twojego dostawcę. Jeśli masz jakieś wątpliwości w tym zakresie zawsze masz prawo zapytać się dostawcy o jakość bezpieczeństwa oferowanego przez niego.

**6. Instaluj na swoim komputerze tylko legalne oprogramowanie.**Programy niewiadomego pochodzenia, w tym ściągane za pośrednictwem programów typu Peer-to-Peer (P2P) mogą być przygotowane przez hakerów i zawierać wirusy lub inne szkodliwe oprogramowanie.

**7. Zaleca się okresowe wykonanie skanowania komputera, w szczególności przed wejściem na stronę internetową banku i wykonaniem jakiejkolwiek transakcji.**Większość programów antywirusowych przy włączonym monitorze antywirusowym ma detekcję (wykrywalność) taką samą jak skaner antywirusowy i nie ma konieczności skanowania komputera. Jest jednak część programów, których detekcja monitora antywirusowego jest niższa aniżeli skanera, powoduje to jednak lukę w systemie bezpieczeństwa.

**8. Aktualizuj system operacyjny i istotne dla jego funkcjonowania aplikacje np. przeglądarki internetowe.**Hakerzy stale szukają luk w oprogramowaniu, które są następnie wykorzystywane do przestępstw internetowych. Producenci systemów operacyjnych i aplikacji publikują stosowne „łaty”, których celem jest usuwanie podatności ich produktów na ataki przeprowadzane za pośrednictwem znalezionych luk.

**9. Nie otwieraj wiadomości i dołączonych do nich załączników nieznanego pochodzenia.**
Często załączniki takie zawierają wirusy lub inne oprogramowanie, które pozwala na szpiegowanie Twoich działań.

**10. Unikaj stron zachęcających do obejrzenia bardzo atrakcyjnych treści lub zawierających atrakcyjne okazje.**Szczególnie niebezpieczne mogą być strony internetowe zawierające treści pornograficzne. Ponadto z pozoru niewinne strony zawierające programy typu „freeware” również mogą być bardzo niebezpieczne, ponieważ hakerzy bardzo często dekompilują je uzupełniając o złośliwy kod.

**11. Po zalogowaniu do systemu transakcyjnego nie odchodź od komputera, a po zakończeniu pracy wyloguj się i zamknij przeglądarkę.**

**12. Jeśli przy logowaniu pojawią się nietypowe komunikaty lub prośby o podanie danych osobowych lub dodatkowe pola z pytaniem o hasła do autoryzacji, natychmiast zgłoś problem do swojego Banku.**

**13. Nie wchodź na stronę internetową Twojego banku za pośrednictwem linków znajdujących się w przychodzących do Ciebie mailach (Phishing).**
Używaj do tego celu adresu podanego Ci przez Bank, z którym podpisał(aś/eś) umowę o otwarcie i prowadzenia rachunku bankowego. Nie jest również wskazane wykorzystywanie mechanizmu „Zakładek” (Firefox) lub „adresów Ulubionych” (Internet Explorer), gdyż istnieją szkodliwe obiekty, które potrafią modyfikować zachowane tam adresy.

**14. Nigdy nie używaj wyszukiwarek internetowych do znalezienia strony logowania Twojego Banku.**Wyszukane w nich linki mogą prowadzić do fałszywych stron lub stron zawierających wirusy.

**15. Przed zalogowaniem sprawdź, czy połączenie z bankiem jest bezpieczne.**Adres witryny internetowej Twojego Banku powinien rozpoczynać się od skrótu: "**https://**", a nie "http://". Brak litery "s" w skrócie "http" oznacza brak szyfrowania, czyli, że Twoje dane są transmitowane przez internet tekstem jawnym, co naraża Cię na ogromne niebezpieczeństwo.

**16. Sprawdzaj prawidłowość certyfikatu.**Zanim wpiszesz identyfikator bądź login i hasło sprawdź, czy  połączenie z bankiem odbywa się z wykorzystaniem szyfrowania. Jeżeli znajdziesz symbol kłódki, kliknij na niego dwa razy, aby sprawdzić, czy wyświetlony certyfikat jest ważny i czy został wydany dla Twojego Banku. Jeśli certyfikat utracił ważność lub nie został wystawiony dla Twojego Banku albo nie można go zweryfikować zrezygnuj z połączenia.

**17. Nigdy nie udostępniaj osobom trzecim identyfikatora ani hasła dostępu.**
Identyfikator jest poufnym numerem nadawanym przez Bank, nie możesz go zmienić.

**18. Nie zapisuj nigdzie haseł służących do logowania i pamiętaj o ich regularnej zmianie.**
Idealnym rozwiązaniem jest zmienianie haseł raz w miesiącu, ale o ile system tego na Tobie nie wymusi zmieniaj je przynajmniej raz na dwa miesiące używając kombinacji dużych i małych liter oraz cyfr.

**19. Sprawdzaj datę ostatniego poprawnego oraz niepoprawnego logowania do systemu.**

**20. Korzystaj z infolinii udostępnionej przez Twój bank.**Zawsze masz prawo skorzystać z infolinii swojego banku jeśli masz wątpliwości w zakresie bezpiecznych transakcji bankowych wykonywanych za pośrednictwem internetu.

**21. Odwiedzaj regularnie Portal „Bezpieczny Bank” na stronie internetowej ZBP – www.zbp.pl**
Jeśli chcesz wiedzieć więcej na temat bezpiecznego posługiwania się bankowością elektroniczną, w tym internetową regularnie odwiedzaj ten Portal. Tam fachowcy z zakresu bezpieczeństwa banku wyjaśniają jak uniknąć czyhających w sieci niebezpieczeństw.

**Zasady dotyczące płatności kartami płatniczymi przez Internet**

**22. Zachowaj rozwagę przy przekazywaniu numeru karty.**
Nie należy udostępniać numeru karty nikomu, kto do nas dzwoni, również w sytuacji, gdy osoba dzwoniąca informuje, że są problemy z komputerem i proszą o weryfikację informacji. Nie ma zwyczaju by firmy dzwoniły prosząc przez telefon o numer karty płatniczej. Jeżeli to my inicjujemy połączenie, również nie należy udostępniać numeru karty przez telefon, gdy nie mamy pewności, że rozmówca zasługuje na zaufanie.

**23. Nigdy nie odpowiadaj na pocztę elektroniczną, z której wynika konieczność podania informacji o karcie – zgłoś taką sytuację w swoim banku.**
Nigdy też nie odpowiadaj na maile, które zapraszają do odwiedzenia strony internetowej w celu weryfikacji danych, w tym o kartach. Ten rodzaj oszustwa jest nazywany „phishingiem”.

**24. Nigdy nie podawaj informacji o karcie na stronach, które nie są bezpieczne.**
Przykładowo strony z treściami pornograficznymi lub strony nieznanych szerzej firm oferujące markowy towar po rewelacyjnych cenach. Przed wprowadzeniu numeru karty w formularzu na stronie należy upewnić się, czy dane przesyłane z formularza są odpowiednio chronione (czyli – upraszczając – czy adres strony z formularzem rozpoczyna się od https i czy strona posiada odpowiednie certyfikaty – te informacje podaje przeglądarka, zazwyczaj w pasku statusu na dole okna).

**25. Nie zapisuj kodu PIN na karcie, ani nie przechowuj go razem z kartą.**
W takich okolicznościach nie tylko działasz niezgodnie z przepisami prawa, ale także w przypadku kradzieży portfela czy portmonetki i posłużenia się Twoją kartą płatniczą bank będzie zwolniony z obowiązku pokrycia powstałej szkody

**26. Chroń swój numer karty i inne poufne kody umożliwiające dokonane transakcji np. numer PIN, numer CVV2 lub CVC2 – ostatnie trzy cyfry numeru umieszczonego na pasku do podpisu na odwrocie karty.**
Przestępcy mogą wchodzić w ich posiadanie, rejestrując obraz karty np. przy użyciu telefonu komórkowego z aparatem fotograficznych, kamerą video lub w inny sposób.

**27. Dokonuj transakcji w znanych i zweryfikowanych przez siebie sklepach internetowych. W przypadku mniejszych serwisów zbadaj ich wiarygodność, na przykład dzwoniąc do takiego serwisu i weryfikując jego ofertę, warunki dokonania transakcji oraz reklamacji.**Upewnij się, czy nie jesteś na stronie internetowej podszywającej się pod stronę Twojego banku/sklepu (podobna nazwa i wygląd strony, którą posługują się nieuczciwi naśladowcy w celu zmylenia i wyłudzenia pieniędzy). Zapoznaj się z regulaminem sklepu internetowego, a szczególnie z informacjami dotyczącymi bezpieczeństwa transakcji. Przed dokonaniem transakcji upewnij się, że transmisja odbywa się w bezpiecznym połączeniu za pomocą protokołu SSL/TLS.