Co można zrobić, aby unikać zagrożeń:

1. Do logowania się do bankowości używaj wyłącznie zaufanego sprzętu. Nie loguj się z niezaufanych komputerów oraz z publicznych sieci WiFi.
2. Loguj się wyłącznie na stronie [www.velobank.pl](http://www.velobank.pl) klikając klawisz „Zaloguj się”. Adres strony wpisuj ręcznie – nie korzystaj z żadnych linków, które kierują Cię do strony logowania.
3. Po kliknięciu w klawisz „Zaloguj się” znajdziesz się na stronie logowania <https://secure.velobank.pl/>. Sprawdź czy w pasku znajduje się ikona kłódki oraz czy adres rozpoczyna się od https://. Oznacza to, że połączenie jest szyfrowane.
4. Kliknij w kłódkę i sprawdź czy certyfikat bezpieczeństwa został wystawiony na secure.velobank.pl
5. Do bankowości internetowej ustaw hasło, którego nie używasz w żadnym innym miejscu. Jeśli podejrzewasz, że ktoś mógł je poznać, zmień je. Możesz to zrobić po zalogowaniu do bankowości internetowej w zakładce Ustawienia, Zmiana hasła.
6. Dodatkowym zabezpieczeniem podczas logowania jest włączenie maskowania hasła do bankowości internetowej. Polega ono na tym, że zamiast pełnego hasła poprosimy Cię o wprowadzenie tylko kilku wybranych znaków, np. trzeci, piąty i dziewiąty znak hasła. System przy każdym logowaniu losuje inne znaki do wypełnienia.
7. Nie zapisuj na swoim komputerze i telefonie loginu oraz hasła do bankowości internetowej i mobilnej.
8. Nie udostępniaj nikomu danych logowania do Twojej bankowości ani kodów autoryzacyjnych.
9. Czytaj uważnie treści SMS-ów, które od nas otrzymujesz. Zanim wpiszesz kod SMS, sprawdź czy zgadza się rodzaj dyspozycji, którą chcesz zlecić, kwota transakcji, konto odbiorcy.
10. Kiedy kończysz korzystać z bankowości internetowej użyj przycisku „Wyloguj” w prawym górnym rogu ekranu.
11. Korzystaj z systemu operacyjnego, przeglądarek internetowych i programów antywirusowych wspieranych przez producentów. Regularnie je aktualizuj.
12. Nie instaluj oprogramowania z niezaufanych źródeł. Aplikacje na telefon pobieraj i instaluj wyłącznie z oficjalnych sklepów Google Play, Apple App Store lub HUWAWEI AppGallery.
13. Na bieżąco aktualizuj aplikację bankowości mobilnej VeloBank i ValoBank Private do najnowszych dostępnych wersji.
14. Nie odpowiadaj na wiadomości od podejrzanych nadawców. Nie otwieraj załączników w tych wiadomościach i nie korzystaj z zawartych w nich linków.
15. Nie instaluj aplikacji do udostępniania zdalnego pulpitu.
16. Regularnie sprawdzaj historię operacji na Twoich rachunkach.
17. Dopasuj limity transakcji dla bankowości internetowej i mobilnej tak, aby odpowiadały indywidualnym potrzebom.
18. Sprawdzaj historię logowania do bankowości internetowej. Znajdziesz ją w sekcji Ustawienia, Hasła i bezpieczeństwo, Bankowość internetowa – Próby logowania.
19. Czytaj aktualności dostępne na naszej stronie internetowej oraz na stronie logowania do bankowości internetowej. Zamieszczamy tam m.in. ostrzeżenia przed aktualnymi metodami oszustw.
20. W razie wątpliwości i podejrzeń dotyczących bezpieczeństwa poinformuj nas o tym. Zadzwoń do Centrum Obsługi Klienta Private Banking (pod numerem +48 22 203 03 01) lub udaj się do dowolnego oddziału.