Bezpieczeństwo Twojego komputera a serwisy transakcyjne Banku BGŻ

Przypominamy, że bezpieczeństwo przeprowadzania własnych transakcji w serwisach bakowości internetowej w Banku BGŻ w dużej mierze zależy od Ciebie i zabezpieczeń urządzeń, przy pomocy których łączysz się z Bankiem.

Przed zalogowaniem i wykonaniem transakcji sprawdź czy:

- Jest wpisany prawidłowy adres strony https://makler.bmbgz.pl
- W pasku adresu strony widać zamkniętą kłódkę, oznaczająca szyfrowane połączenie z bankiem,
- Strona bmBGŻ.net jest zabezpieczona ważnym certyfikatem wystawionym dla witryny makler.bmbgz.pl, której właścicielem jest Bank Gospodarki Żywnościowej S.A., potwierdzonym przez VeriSign. Poprawność sprawdzisz klikając w zamkniętą kłódkę widoczną w oknie przeglądarki,
- Przed potwierdzeniem dowolnej operacji zawsze weryfikuj wyświetlane informacje – w szczególności numer konta i rodzaj operacji wyświetlany na stronie www oraz dane otrzymane w sms.

Zabezpiecz urządzenia, z których korzystasz

Aby zminimalizować ryzyko związane z korzystaniem ze internetowego dostępu do Banku, należy stosować szczególne środki ostrożności oraz zadbać aby urządzenie dostępowe (np. komputer, telefon, tablet oraz urządzenia sieciowe np. router Wi-Fi) nie były podatne na zagrożenia.

- Połączenie z Internetem musi być bezpieczne (unikaj łączenia się z publicznej sieci WiFi, ogólnodostępnych sieci i komputerów, do których inni mają swobodny dostęp)
- Zawsze korzystaj z aktualnych wersji systemu operacyjnego i przeglądarki internetowej,
- Korzystaj z aktualnego, prawidłowo skonfigurowanego oprogramowania zabezpieczającego przed szkodliwym oprogramowaniem (antywirusy, antymalware) oraz połączeniami sieciowymi (personal firewall – zapory sieciowe),
- Stosuj bezpieczne hasła, stosuj dodatkowe hasła do profilu na komputerze, ogranicz fizyczny dostęp dla osób niepowołanych,
- Nie instaluj oprogramowania z niesprawdzonych źródeł (np. pirackiego), oraz nie otwieraj załączników w poczcie email od nieznanych nadawców,
- Aby bezpiecznie wylogować się z systemu bmBGŻ.net korzystaj zawsze z przycisku „Wyloguj" lub „Wyjdź",
- W przypadku braku możliwości weryfikacji zabezpieczeń we własnym zakresie, zalecamy skorzystanie z profesjonalnych firm świadczących usługi informatyczne.

Pamiętaj, że bank nigdy nie prosi o:

- Instalację certyfikatów lub programów na komputerach i telefonach komórkowych,
- Podanie danych kart płatniczych i kredytowych (numer karty, kod PIN, CVV2) oraz danych dotyczących Twojego telefonu (numer i model),
- Udział w testowaniu nowych funkcjonalności serwisu transakcyjnego,

- Wykonanie przelewów testowych ani zwrotu środków na rachunki innych klientów.

Dlaczego zabezpieczenia są tak ważne?

Poziom bezpieczeństwa komunikacji pomiędzy każdą witryną internetową a jej klientem zależy w od poziomu bezpieczeństwa każdego z elementów uczestniczących w tej komunikacji. Bank utrzymuje w swoich systemach najwyższe standardy bezpieczeństwa. Ale jeśli komputer (tablet, telefon), przy pomocy którego się z nami łączysz, jest podatny na włamanie lub co gorsza już zainfekowany złośliwym oprogramowaniem, łatwo może dojść do sytuacji, w której cyberprzestępca, mając do dyspozycji wykradzione z tego urządzenia dane uwierzytelniające (login, hasło, SMS potwierdzający transakcję, kod z tokena…) będzie usiłował podszyć się pod Ciebie lub podsunąć Ci do zatwierdzenia przelew wg własnego wyboru.

Odpowiednie przygotowanie urządzeń do bezpiecznej pracy - i utrzymanie tego stanu – znacznie ułatwi śledzenie informacji branżowych związanych z bezpieczeństwem informatycznym oraz aktualizowanie wiedzy dotyczącej nowych zagrożeń. Szczególnie przydatne informacje z tego zakresu, przeznaczone do szerokiego grona użytkowników serwisów bankowych, można znaleźć między innymi na stronach internetowych takich instytucji jak:

- CERT - www.cert.pl, zwłaszcza cykl artykułów OUCH pod adresem: http://www.cert.pl/ouch
- ZBP - www.zbp.pl, zwłaszcza informacje dla konsumentów: zbp.pl/dla-konsumentow