

De maatregelen die OBK neemt ter beveiliging van de webbanking

Veilige verbinding

OBK waarborgt een veilige verbinding die in- en uitgaande informatiestromen codeert. WEBBANKING wordt opgestart via de website www.obk.be. De veilige verbinding herkent u aan de 'https' aan het begin van de url, voor OBK is dit <https://webbanking.obk.be>. De verbinding wordt automatisch verbroken bij een periode van non-activiteit van 5 minuten.

De elektronische handtekening

OBK webbanking gebruikt 2 types van elektronische handtekening:

Om in te loggen (applicatie 1) gelden de combinatie van de gebruikersnaam, het wachtwoord en de veiligheidscode bestaande uit 6 cijfers, gegenereerd door de digipass met de bijhorende pincode, als elektronische handtekening.

Om binnen de geopende webbankingsessie financiële transacties goed te keuren (applicatie 2) geldt de veiligheidscode bestaande uit 8 cijfers, gegenereerd door de digipass met de bijhorende pincode, als elektronische handtekening.

Een periodiek overzicht van de transacties

OBK licht de cliënt in over de transacties die verricht werden en worden, via het rekeningoverzicht, de rekeninguittreksels alsmede de betaalagenda.

Nieuwe evoluties en aandachtspunten inzake het veilig gebruik - OBK informeert u

OBK informeert u tijdig over en/of sensibiliseert u voor nieuwe evoluties en aandachtspunten inzake het veilig gebruik door de cliënt van de webbanking. Dit onder andere via het berichtensysteem van webbanking.

Verplichtingen van de cliënt

Beveilig uw computer

Installeer een firewall

Bescherm uw computer tegen indringers van buitenaf door een firewall te installeren. Zo verkleint u de kans dat hackers toegang weten te krijgen tot uw financiële gegevens.

Installeer een degelijk en geactualiseerd antivirusprogramma en antispysware

Een antivirusprogramma spoort schadelijke software op die schade kan aanrichten in uw computer. Spysware is de naam voor software die informatie vergaart over computergebruikers.

Gebruik nooit publiek computers om uw bankverrichtingen uit te voeren

U weet niet of die computers zijn besmet met virussen of andere programma's die de veiligheid van uw transacties in gevaar kunnen brengen.

Beveilig uw draadloze internetverbinding

Verander de wachtwoorden die met uw apparatuur worden meegeleverd en verander ook de naam van uw netwerk om te voorkomen dat de burens of mensen die zich in uw buurt bevinden uw internetverbinding zouden gebruiken zonder dat u dat weet.

Meldt u beveiligd aan op uw eigen computer

Stel een wachtwoord in op uw computer per gebruiker.

Surf als een goede huisvader

Controleer steeds het adres van onze website

WEBBANKING wordt opgestart via de website www.obk.be. Een beveiligde verbinding herkent u aan 'https' aan het begin van de url, voor OBK is dit <https://webbanking.obk.be>.

Controleer of de WEBBANKING site in de beveiligde modus staat

Als u webbanking normaal opent, dan bevindt de site zich in de beveiligde modus. Deze modus kan u herkennen aan het gele veiligheidsslot rechts onderaan de webpagina. U kan ook het certificaat zelf verifiëren door te dubbelklikken op het gele veiligheidsslot of door de keuze 'eigenschappen/properties' (in het schermmenu op te roepen met de rechtermuisknop) aan te klikken. Onder 'certificaten' moet u kunnen vaststellen dat het certificaat werd verstrekt aan "webbanking.obk.be" door GlobalSign ServerSign CA, een instantie die certificaten aflevert. Enkel deze gegevens garanderen dat u in verbinding bent met webbanking van OBK.

Let op voor binnenkomende e-mails

OBK zal u nooit vertrouwelijke informatie vragen via e-mail. Geef nooit uw persoonlijke gegevens door via e-mail, een website of sms.

Wantrouw bijlagen bij uw e-mails. Als u niet zeker bent waar ze vandaan komen, maakt u ze best niet open.

Gebruik van uw elektronische handtekening

De webbankingtoepassingen, waarbij er gevraagd wordt naar uw elektronische handtekening, zijn beperkt:

applicatie 1: enkel aanloggen

applicatie 2: financiële transacties

De respectievelijke applicaties zullen nooit voor een andere toepassing gebruikt worden.

Het gebruiksrecht van webbanking is strikt persoonlijk

Laat uw wachtwoord en pincode nooit zomaar ergens rondslingeren. Bewaar ze zorgvuldig zonder ze te noteren in een gemakkelijk herkenbare vorm.

Laat u nooit bijstaan tijdens het gebruik van webbanking door familieleden of derden en deel uw wachtwoord en pincode nooit mee aan familieleden of derden.

Log steeds uit en laat uw computer nooit onbeheerd achter wanneer u OBK WEBBANKING hebt gebruikt

Sluit webbanking altijd correct af na het voltooien van een financiële transactie via de knop 'webbanking afsluiten'. Laat uw PC nooit onbeheerd achter na login op het OBK webbanking systeem.

Controleer steeds uw transacties aan de hand van uw betalingsagenda en rekeninguittreksels
Overloop regelmatig uw rekeningoverzicht, uw rekeninguittreksels alsmede uw betaalagenda.

Stel OBK onmiddellijk in kennis van:

- 1/ het verlies of de diefstal van uw geheime codes, digipass of het wachtwoord;
- 2/ ieder risico van misbruik van uw toegangsmiddelen of de schending van het geheim karakter van de codes of het wachtwoord;
- 3/ de boeking van transacties waarvoor uw geen opdracht heeft gegeven;
- 4/ iedere onregelmatigheid of fout op uw betaalagenda, rekeningoverzichten of rekeninguittreksels.

U kan OBK van deze feiten inlichten, ofwel op elk ogenblik via e-mail op helpdesk@obk.be, ofwel telefonisch op het nummer 09 269 39 10 bij de dienst Informatica op iedere bankwerkdag van 8u30 tot 12u30 en van 13u30 tot 17u00.

Binnen de 3 dagen dient de telefonische melding of de e-mail te worden bevestigd per aangetekende brief samen met een gedetailleerde beschrijving van de feiten. In geval van diefstal of verlies of in geval van misbruik dient de aangetekende brief vergezeld te zijn van een kopie van het proces-verbaal van aangifte of diefstal dat werd opgemaakt door de Federale Politie.