

BEVEILIGING

Izola Bank zet zich in voor de veiligheid en vertrouwelijkheid van uw persoonlijke gegevens. Izola Bank streeft naar een hoog niveau van digitale operationele veerkracht, waarbij onze systemen en diensten voldoende robuust zijn om ICT-gerelateerde verstoringen, zoals cyberaanvallen of systeemstoringen, te weerstaan, erop te reageren en ervan te herstellen. Ons uitgebreid kader voor ICT-risicobeheer wordt regelmatig geëvalueerd en getest om uw bankverrichtingen te beschermen. Onze inspanningen op het vlak van digitale operationele veerkracht, zoals vereist door DORA, versterken onze capaciteit om uw gegevens te beschermen tegen inbreuken en zorgen voor hun vertrouwelijkheid en integriteit.

Bij Izola Bank staan de veiligheid en privacy van uw persoonlijke gegevens voorop. Wij houden ons strikt aan de beginselen van de Algemene Verordening Gegevensbescherming (AVG), waarbij uw persoonlijke gegevens rechtmatig, eerlijk en transparant worden verwerkt, uitsluitend verzameld worden voor specifieke, uitdrukkelijke en legitieme doeleinden, en veilig worden bewaard via sterke technische en organisatorische maatregelen.

Dit omvat gegevensminimalisatie, veilige opslag en strikte toegangscontroles. U beschikt over fundamentele rechten met betrekking tot uw persoonsgegevens, waaronder het recht op toegang, correctie of verwijdering van uw gegevens, en wij zetten ons in om deze rechten te faciliteren. Raadpleeg ons [Privacybeleid](#) voor meer informatie.

Als onderdeel van onze voortdurende inspanningen om de best mogelijke beveiliging te bieden tegen kwaadwillende gebruikers die toegang willen tot of misbruiken van uw gegevens, hebben we verschillende diensten en functies opgezet om uw online bankieren via desktop en mobiele apparaten te beveiligen.

Het is net zo belangrijk dat u ook zelf een actieve rol speelt in het beveiligen van uw persoonlijke gegevens. Hier vindt u extra informatie met tips en richtlijnen over hoe u uw veiligheid het best beheert.

1. Toegang tot onze websites

De enige manier om zeker te zijn dat u de officiële website van Izola Bank bezoekt, is door het webadres rechtstreeks in de adresbalk van uw internetbrowser te typen. Zodra u hebt bevestigd dat het adres correct is, raden wij u aan het in uw browser te bookmarken (toevoegen aan Favorieten), zodat u vanaf dat moment altijd de juiste link gebruikt. Zorg er ook voor dat de link begint met **https://**. Open de website van de Bank nooit via een URL-link in een e-mail, zelfs als de e-mail afkomstig lijkt van Izola Bank.

Geen andere websites dan de volgende mogen worden gebruikt

Hoofdwebsite:	https://www.izolabank.com
Izola Online-website:	https://ebanking.izolabank.com
Factoringwebsite:	https://factor.izolabank.com
Beveiligde bestandsoverdracht:	https://sft.izolabank.com
Spaarwebsite:	https://www.izolabank.com/be-nl/personal-banking/sparen

2. E-mails of telefoongesprekken

Let op: Izola Bank zal nooit:

- vragen naar uw wachtwoord, pincode of eenmalig wachtwoord (OTP);
- u vragen dergelijke informatie aan een medewerker bekend te maken, onder welke omstandigheden dan ook;
- u vragen externe toegang tot uw toestel te verlenen.

Als u een specifieke actie hebt aangevraagd, zoals het opnieuw instellen van uw wachtwoord, ontvangt u een e-mail van ons. Wees echter altijd voorzichtig en klik niet op links in ongevraagde e-mails. Criminelen kunnen steeds geavanceerdere technieken gebruiken, waaronder Kunstmatige Intelligentie (AI), om overtuigende e-mails, berichten, websites of telefoongesprekken te creëren die echt lijken. Controleer communicatie altijd via de officiële kanalen van Izola Bank voordat u actie onderneemt. Wees alert op onverwachte of dringende berichten waarin wordt beweerd dat uw rekening is geblokkeerd, opgeschort of onmiddellijk moet worden geverifieerd. Bij twijfel typt u het adres van onze website rechtstreeks in uw browser of neemt u contact op met ons [Helpcentrum](#).

De integriteit en authenticiteit van e-mails die van Izola Bank lijken te komen, kunnen niet worden gegarandeerd omdat informatie mogelijk wordt onderschept, verwijderd, verloren of gewijzigd. Als u een e-mail ontvangt die frauduleus lijkt, waarin accountinformatie wordt gevraagd, of als u twijfelt aan de authenticiteit van een communicatie die beweert van Izola Bank afkomstig te zijn, antwoord dan niet, klik niet op links en neem contact met ons op via ons [Helpcentrum](#).

Izola Bank verwacht dat klanten hun toestellen, inloggegevens en beveiligingsgegevens veilig bewaren. De Bank is mogelijk niet aansprakelijk voor verliezen die voortvloeien uit malware, ongeoorloofde toegang door derden of andere cyberaanvallen wanneer deze het gevolg zijn van fraude door de klant, grove nalatigheid, het niet naleven van veiligheidsinstructies of het niet tijdig melden van ongeoorloofd gebruik, met inachtneming van de toepasselijke wetgeving.

3. Cyberbeveiligingsproblemen

Als u op enig moment vermoedt dat de beveiliging van uw Izola Bank-rekeningen in gevaar is gebracht, bijvoorbeeld wanneer u onverwachte OTP-berichten ontvangt, inlogactiviteiten opmerkt die u niet herkent, ongeoorloofde wijzigingen aan uw contactgegevens ziet of onverwacht geen toegang meer hebt tot uw rekening, neem dan onmiddellijk [contact met ons op](#).

Izola Bank zal de nodige maatregelen treffen om uw rekening te beschermen.

In overeenstemming met de regelgeving heeft Izola Bank robuuste procedures voor incidentbeheer en bedrijfscontinuïteit ontwikkeld en geïmplementeerd. Hoewel wij streven naar een ononderbroken dienstverlening, verbinden wij ons ertoe u onmiddellijk te informeren bij een ernstige ICT-gerelateerde storing die onze diensten beïnvloedt, met de nodige maatregelen of alternatieve kanalen voor bankieren.

4. Inloggen op Online Bankieren

Onze website is beveiligd met de nieuwste SSL-technologieën, die certificeren dat de website daadwerkelijk toebehoort aan **Izola Bank p.l.c. [MT]**.

Wanneer u toegang krijgt tot uw Izola Online, controleer dan of het adres <https://ebanking.isolabank.com/> is. Verschillende webbrowsers tonen SSL-certificaatindicatoren (zoals hangslotsymbolen, groene balken of bedrijfsnamen) op verschillende manieren. Raadpleeg de instructies van uw browser voor het controleren van het SSL-certificaat en de geldigheid van de site voordat u inlogt. Als u twijfelt, log dan niet in en neem [contact met ons op](#).

5. Toegang tot Mobiel en Online Bankieren

De officiële Izola Bank-app is de enige veilige manier om toegang te krijgen tot uw Izola Bank-rekeningen via een mobiel apparaat. Download de Izola Bank-app uitsluitend via de officiële Apple App Store of Google Play Store. Controleer vóór het downloaden of de uitgever "Izola Bank plc" is. Gebruik nooit links uit e-mails, sms-berichten of sociale media om toegang te krijgen tot uw bankdiensten, zelfs als ze van Izola Bank lijken te komen. Raadpleeg ons [Helpcentrum](#) voor meer informatie over registratie, activatie en toegang tot onze diensten.

Altijd onthouden

- Gebruik Izola Online uitsluitend vanaf vertrouwde toestellen met een beveiligde internetverbinding en zorg ervoor dat u een bijgewerkte webbrowser gebruikt.*
- Zorg ervoor dat het besturingssysteem en de beveiligingssoftware op de toestellen (mobiel, laptop) waarmee u onze Izola Online-diensten gebruikt, up-to-date zijn, aangezien dit het risico op cyberdreigingen verder beperkt.
- Voer uw inloggegevens alleen in nadat u hebt gecontroleerd dat de site echt is, zoals hierboven beschreven.
- Geef uw wachtwoord, pincode of eenmalige wachtwoorden nooit aan iemand anders, zelfs niet als die zich voordoeft als een medewerker van de Bank.
- Log altijd uit na afloop van uw online bankiersessie.
- Vermijd toegang tot online bankieren via openbare of gedeelde toestellen, aangezien deze mogelijk niet veilig zijn.
- Vermijd het gebruik van openbare, onbeveiligde wifi-netwerken (zoals in luchthavens of cafés) terwijl u verbonden bent met uw Izola Bank app of Izola Online.
- Klik niet op links in ongewenste e-mails, sms-berichten of sociale mediaberichten die van Izola Bank afkomstig lijken.
- Vertrouw geen websites met vreemde of verkeerd gespelde domeinnamen (zoals izolabank.com of izolabank-secure.net).
- Negeer geen browserwaarschuwingen over onveilige of verdachte websites
- Sla uw onlinebankieringsgegevens niet op op openbare, gedeelde of onbeveiligde toestellen. Als u een wachtwoordmanager gebruikt, zorg er dan voor dat deze betrouwbaar is, beveiligd wordt met een sterk hoofdwachtwoord en waar mogelijk beschermd is met multifactorauthenticatie.
- Om veiligheidsredenen is het gebruik van geroote of jailbreakte toestellen voor toegang tot de diensten van Izola Bank verboden.

6. Geo-blokkering van jurisdicties

De websites maken gebruik van geo-blokkerende technologie en zijn niet beschikbaar in geselecteerde jurisdicties. De websites, mobiele en online bankieren zijn beschikbaar in de volgende landen:

Andorra, België, Bulgarije, Cyprus, Denemarken, Duitsland, Estland, Finland, Frankrijk, Gibraltar, Griekenland, Hongarije, Ierland, IJsland, Isle of Man, Italië, Kroatië, Letland, Liechtenstein, Litouwen, Luxemburg, Malta, Monaco, Nederland, Noorwegen, Oostenrijk, Polen, Portugal, Roemenië, San Marino, Slovenië, Slowakije, Spanje, Tsjechië, Verenigd Koninkrijk, Zweden en Zwitserland.

*Belangrijke informatie

Browsers: Hoewel verschillende browsers kunnen worden gebruikt, raden wij aan de nieuwste versie van Google Chrome, Microsoft Edge of Mozilla Firefox te gebruiken. Voor de beste prestaties en veiligheid moeten browsers gedownload worden van hun officiële websites of app stores en up-to-date gehouden worden.

Ondersteunde mobiele besturingssystemen: de vier meest recente versies van Android en de drie meest recente versies van iOS. Indien de app niet beschikbaar is voor uw toestel, kunt u Izola Online nog steeds gebruiken via een webbrowser op uw mobiele telefoon, tablet of computer.