

SÉCURITÉ

Izola Bank s'engage à préserver la sécurité et la confidentialité de vos informations personnelles. Izola Bank s'engage à maintenir un haut niveau de résilience opérationnelle numérique, garantissant que nos systèmes et services sont suffisamment robustes pour résister, réagir et se rétablir après des perturbations liées aux TIC, telles que des cyberattaques ou des défaillances systèmes. Notre cadre global de gestion des risques liés aux TIC est régulièrement évalué et testé pour protéger vos opérations bancaires. Nos efforts de résilience opérationnelle numérique, requis par le règlement DORA, renforcent en outre notre capacité à protéger vos données contre les violations et à garantir leur confidentialité et intégrité.

Chez Izola Bank, la sécurité et la vie privée de vos données personnelles sont essentielles. Nous respectons strictement les principes du Règlement général sur la protection des données (RGPD), veillant à ce que vos données personnelles soient traitées de manière licite, loyale et transparente, collectées uniquement à des fins spécifiques, explicites et légitimes, et conservées de façon sécurisée grâce à des mesures techniques et organisationnelles fiables.

Cela comprend la minimisation des données, le stockage sécurisé et des contrôles d'accès rigoureux. Vous disposez de droits fondamentaux sur vos données personnelles, notamment les droits d'accès, de rectification ou d'effacement, et nous nous engageons à faciliter l'exercice de ces droits. Pour plus d'informations, consultez notre [Politique de Confidentialité](#).

Dans le cadre de notre mission continue de garantir la meilleure sécurité possible contre les utilisateurs malveillants accédant ou manipulant vos données, nous avons mis en place plusieurs services et fonctionnalités pour sécuriser vos sessions de banque en ligne via ordinateurs et appareils mobiles.

Il est tout aussi important que vous jouiez un rôle actif pour protéger vos informations personnelles. Vous trouverez ci-après des conseils et lignes directrices pour gérer efficacement votre sécurité.

1. Accès à nos sites web

La seule manière de vous assurer que vous visitez le site légitime d'Izola Bank est de taper directement l'adresse web dans la barre d'adresse de votre navigateur Internet. Une fois l'adresse confirmée, ajoutez-la à vos favoris pour accéder systématiquement au bon site. Vérifiez également que l'adresse commence par **https://**. N'accédez jamais au site bancaire via un lien dans un e mail, même si celui-ci semble provenir d'Izola Bank.

Sites autorisés uniquement

Site principal :	https://www.izolabank.com
Site web Izola Online :	https://ebanking.izolabank.com
Site de factoring :	https://factor.izolabank.com
Transfert sécurisé de fichiers :	https://sft.izolabank.com
Site d'épargne :	https://www.izolabank.com/be-fr/epargne-personnelle/epargne

2. E-mails ou appels téléphoniques

Veillez noter qu'Izola Bank ne vous demandera jamais :

- votre mot de passe, code PIN ou mot de passe à usage unique (OTP) ;
- de communiquer ces informations à un employé, quelles que soient les circonstances ;
- d'accorder un accès à distance à votre appareil.

Si vous avez demandé une action spécifique, telle qu'une réinitialisation de mot de passe, vous recevrez un e-mail de notre part ; toutefois, restez toujours vigilant et ne cliquez sur aucun lien dans des e-mails non sollicités. Les criminels peuvent utiliser des techniques de plus en plus sophistiquées, y compris l'Intelligence Artificielle (IA), pour créer des e-mails, messages, sites web ou appels téléphoniques convaincants qui semblent authentiques. Vérifiez toujours les communications via les canaux officiels d'Izola Bank avant d'agir. Soyez attentif aux messages inattendus ou urgents indiquant que votre compte a été bloqué, suspendu ou nécessite une vérification immédiate. En cas de doute, accédez à notre site web en saisissant directement l'adresse dans votre navigateur ou contactez notre [Help Centre](#).

L'intégrité et l'authenticité des e-mails prétendument envoyés par Izola Bank ne peuvent être garanties, puisqu'ils peuvent être interceptés, modifiés ou falsifiés. Si vous recevez un e-mail qui semble frauduleux, demandez des informations relatives à votre compte, ou si vous avez des doutes quant à l'authenticité d'une communication prétendant provenir d'Izola Bank, n'y répondez pas, ne cliquez sur aucun lien et contactez-nous via notre [Help Centre](#).

Izola Bank attend de ses clients qu'ils protègent leurs appareils, identifiants et informations de sécurité. La Banque peut ne pas être responsable des pertes résultant de logiciels malveillants, d'un accès non autorisé par des tiers ou d'autres cyberattaques lorsque celles-ci résultent d'une fraude du client, d'une négligence grave, du non-respect des consignes de sécurité ou du défaut de notification rapide à la Banque d'une utilisation non autorisée, sous réserve de la législation applicable.

3. Problèmes de cybersécurité

Si vous suspectez à tout moment que la sécurité de vos comptes Izola Bank est compromise, notamment si vous recevez des messages OTP inattendus, constatez une activité de connexion que vous ne reconnaissez pas, observez des modifications non autorisées de vos coordonnées ou êtes soudainement incapable d'accéder à votre compte, [contactez-nous](#) immédiatement. Izola Bank prendra les mesures nécessaires pour protéger votre compte.

Conformément aux exigences réglementaires, Izola Bank a développé et mis en œuvre des plans robustes de gestion des incidents et de continuité des activités. Bien que nous visons une disponibilité sans interruption, en cas d'incident majeur lié aux TIC affectant nos services, nous nous engageons à vous informer rapidement de l'incident ainsi que des mesures de remédiation ou canaux alternatifs disponibles.

4. Connexion à l'Online Banking

Notre site est protégé par les technologies SSL les plus récentes, certifiant qu'il appartient bien à **Izola Bank p.l.c. [MT]**.

Pour accéder à vos services bancaires, assurez-vous que l'adresse est <https://ebanking.izolabank.com/>. Les navigateurs peuvent afficher des indicateurs SSL (icônes de cadenas, barre verte, nom de société) de manière différente. Consultez les instructions de votre navigateur pour vérifier la validité du certificat SSL et l'authenticité du site avant de vous connecter. En cas de doute, ne vous connectez pas et [contactez-nous](#).

5. Accès au Mobile et Online Banking

L'app officielle Izola Bank est le seul moyen sécurisé d'accéder à vos comptes depuis un appareil mobile. Téléchargez l'application Izola Bank exclusivement depuis l'Apple App Store ou le Google Play Store, et vérifiez que l'éditeur est "Izola Bank plc". N'accédez jamais à vos services bancaires via des liens dans des e mails, SMS ou réseaux sociaux, même s'ils semblent provenir d'Izola Bank. Consultez notre [Help_Centre](#) pour obtenir des informations sur l'enregistrement, l'activation et l'accès à nos services.

À retenir

- N'accédez à Izola Online qu'à partir d'appareils de confiance disposant d'une connexion sécurisée et d'un navigateur à jour.*
- Maintenez à jour le système d'exploitation et le logiciel de sécurité de vos appareils (mobile, ordinateur), pour réduire le risque de menaces.
- Ne saisissez vos identifiants qu'après avoir confirmé l'authenticité du site tel qu'indiqué précédemment.
- Ne communiquez jamais votre mot de passe, code PIN ou mot de passe à usage unique, même si l'on prétend représenter la Banque.
- Déconnectez-vous après chaque session.
- Évitez d'accéder aux services bancaires en ligne depuis des appareils publics ou partagés, car ils peuvent ne pas être sécurisés.
- Évitez les connexions lorsque vous êtes connecté à des réseaux Wi-Fi publics non sécurisés (aéroports, cafés...).
- N'ouvrez pas les liens reçus dans des e mails, SMS ou contenus sur les réseaux sociaux prétendument envoyés par Izola Bank.
- Méfiez-vous des sites web aux noms de domaine inhabituels ou mal orthographiés (ex. : izolabank.com, izolabank-secure.net).
- Ne négligez pas les alertes de votre navigateur concernant des sites suspectés non sécurisés.
- N'enregistrez pas vos identifiants de banque en ligne sur des appareils publics, partagés ou non sécurisés. Si vous utilisez un gestionnaire de mots de passe, assurez-vous qu'il est fiable, protégé par un mot de passe maître robuste et sécurisé par une authentification multifacteur lorsque celle-ci est disponible.
- Pour des raisons de sécurité, l'utilisation d'appareils rootés ou jailbreakés pour accéder aux services d'Izola Bank est interdite.

6. Géoblocage des juridictions

Nos sites web sont soumis à une géo restriction pour certaines régions. Les services online et mobile banking sont disponibles dans les pays suivants:

Andorre, Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Gibraltar, Grèce, Hongrie, Île de Man, Irlande, Islande, Italie, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Monaco, Norvège, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni, Saint-Marin, Slovaquie, Slovénie, Suède et Suisse.

*Informations importantes

Navigateurs Web : Bien qu'un grand nombre de navigateurs soit compatible, nous recommandons les dernières versions de Google Chrome, Microsoft Edge ou Mozilla Firefox. Pour une performance et sécurité optimales, téléchargez-les uniquement depuis leurs sites officiels ou app stores, et gardez-les à jour.

Systèmes d'exploitation mobiles pris en charge : les quatre versions les plus récentes d'Android et les trois versions les plus récentes d'iOS. Si l'application n'est pas disponible au téléchargement sur votre appareil, vous pouvez toujours utiliser Izola Online via un navigateur web sur votre téléphone mobile, votre tablette ou votre ordinateur.