izola Bank

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
Internet Banking :	https://ebanking.izolabank.com
Site de factoring :	https://factor.izolabank.com
Transfert sécurisé de fichiers :	https://sft.izolabank.com
Site d'épargne :	https://savings.izolabank.com

2. E-mails ou appels téléphoniques

Notez qu'Izola Bank ne vous demandera jamais votre mot de passe ou code PIN par e mail ou téléphone. Nous ne vous demanderons jamais de fournir ces informations à un employé.

Si vous avez demandé une action spécifique, telle qu'une réinitialisation de mot de passe, vous recevrez un e mail de notre part, mais restez toujours vigilant et n'ouvrez pas les liens dans les e mails non sollicités. En cas de doute, accédez directement à notre site via votre navigateur.

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 suspect demandant des informations de compte, ne répondez pas et contactez-nous via notre Help Centre.

Izola Bank décline toute responsabilité pour les pertes résultant de logiciels malveillants, d'accès non autorisés par des tiers ou d'autres types de cyberattaques.

3. Problèmes de cybersécurité

Si vous suspectez à tout moment que la sécurité de vos comptes Izola Bank est compromise, contactez-nous immédiatement.

Izola Bank prendra les mesures nécessaires pour protéger votre compte.

Conformément aux exigences réglementaires, Izola Bank a mis en place 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'Internet Banking

Notre site est protégé par les technologies SSL les plus récentes, garantissant 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 Banking

L'app officielle Izola Bank est le seul moyen sécurisé d'accéder à vos comptes depuis un appareil mobile. Téléchargez-la uniquement 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'utilisez l'Internet Banking que depuis des ordinateurs de confiance avec une connexion sécurisée et un navigateur à jour.*
- Maintenez à jour le système d'exploitation et l'antivirus 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, surtout sur des appareils publics ou partagés.
- Évitez les connexions via 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. : izolabarnk.com, izolabank-secure.net).
- Ne négligez pas les alertes de votre navigateur concernant des sites suspectés non sécurisés.
- N'enregistrez pas vos identifiants sur des appareils publics ou partagés.

6. Géoblocage des juridictions

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

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

*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 deux versions majeures les plus récentes d'Android et d'iOS.

izola Bank

Head Office
Izola Bank p.l.c., 4, Castille Place, Valletta VLT1062 – Malta