izola Bank

SECURITY

Izola Bank is committed to maintaining a high level of digital operational resilience, ensuring our systems and services are robust enough to withstand, respond to, and recover from ICT-related disruptions, such as cyberattacks or system failures. Our comprehensive ICT risk management framework is regularly reviewed and tested to protect your banking operations. Our digital operational resilience efforts, mandated by DORA, further strengthen our capacity to protect your data from breaches and ensure its confidentiality and integrity.

At Izola Bank, the security and privacy of your personal data are paramount. We adhere strictly to the principles of the General Data Protection Regulation (GDPR), ensuring that your personal information is processed lawfully, fairly, and transparently, collected only for specified, explicit, and legitimate purposes, and kept secure through robust technical and organisational measures. This includes data minimisation, secure storage, and strict access controls. You have fundamental rights regarding your personal data, including the right to access, rectify, or erase your information, and we are committed to facilitating these rights. For more details, refer to our Privacy Policy.

As part of our ongoing efforts to provide the best security possible against malicious users accessing or tampering with your data, we have set up several services and features to help secure your online banking sessions with us via desktop and mobile devices.

It is equally important that you also take an active role to keep your personal information secure. To help guide you here is some additional information with tips and guidelines on how best to manage your security.

1. Accessing our websites

The only way to ensure that you are visiting the legitimate Izola Bank website is by typing the web address directly in your Internet browser's address bar. Once you confirm that the website address is correct, we recommend that you bookmark it in your browser (add it to Favourites), as to ensure that you access the correct link from that point onwards. Please also ensure that the link starts with **https://**. Never access the Bank's website through a URL link in an email, even if the email appears to have come from Izola Bank.

No websites other than the following should be used

Main Website:	https://www.izolabank.com
Internet Banking Website:	https://ebanking.izolabank.com
Factoring Website:	https://factor.izolabank.com
Secure File Transfer Website:	https://sft.izolabank.com
Savings Website:	https://savings.izolabank.com

2. Emails or Phone Calls

Please be aware that Izola Bank will never request your password or PIN code via email or phone. We will also never ask you to disclose such information to any employee under any circumstance.

If you have requested a specific action, such as a password reset, you will receive an email from us, however always remain cautious, and do not click on any link in unsolicited emails. When in doubt, access our website by typing the address directly in your browser.

The integrity and authenticity of emails seen as originating from Izola Bank cannot be guaranteed due to information possibly being intercepted, deleted, lost, or modified. Should you receive any email that appears to be fraudulent, or an email that requests you to send account information , do not reply to it, and please contact us via our Help centre.

Izola Bank is not responsible for any loss due to issues arising from malware, unauthorised third-party access or any other cybersecurity attacks.

3. Cybersecurity Concerns

If at any point you have reason to suspect that the security surrounding your Izola Bank accounts may have been compromised, please contact us immediately.

Izola Bank will take the necessary action to safeguard your account.

In line with regulatory requirements, Izola Bank has also developed robust incident management and business continuity plans and has put these in place. While we strive for uninterrupted service, in the event of a significant ICT-related incident impacting our services, we are committed to informing you promptly about the incident and any necessary mitigation measures or alternative channels for banking.

4. Logging in to Online Banking

Our website is protected using the latest SSL technologies, which provide a way of certifying that the website genuinely belongs to **Izola Bank p.l.c. [MT]**.

When accessing your Online Banking, please ensure that the website address is https://ebanking.izolabank.com/. Different web browsers may display SSL certificate indicators (such as padlock icons, green bars, or company names) in varied ways. We recommend that you refer to your browser's specific instructions for confirming the validity of the SSL certificate and verifying the legitimacy of the site before logging in. If you have any doubts, please do not log in and contact us.

5. Accessing Mobile Banking

Using the official Izola Bank app is the sole secure method for accessing your Izola Bank accounts on a mobile device. Always download the Izola Bank app exclusively from the official Apple App Store or Google Play Store. Verify that the publisher is "Izola Bank plc" before downloading. Never access your banking services through links found in emails, SMS messages, or social media, even if they appear to originate from Izola Bank. For more information on how to register, activate and access our services, please refer to our Help centre.

Always remember

- You should only access Online Banking from trusted computers where Internet access is secured, and ensure you are using an updated web browser.*
- We recommend that the operating system and antivirus installed on the personal device (Mobile, Laptop) you use to access the Online Banking services are kept updated, as this will further minimise the risk of threats.
- You should only enter your credentials after you have verified that the site is genuine, as explained further above on this page.
- Do not disclose your password, PIN, or one-time passwords to anyone, even if they claim to represent the Bank.
- Log out of your online banking session after use, especially on shared or public devices.
- You should avoid accessing your Izola Bank Mobile App and Internet Banking using open unsecured public Wi-Fi networks like those typically found at airports and coffee shops.
- Do not click on links in unsolicited emails, SMS messages, or social media posts claiming to be from Izola Bank.
- Do not trust websites with unusual or misspelt domains (e.g., izolabarnk.com and izolabank-secure.net).
- Do not ignore browser warnings about insecure or suspicious websites.
- Do not save your credentials on shared or public computers.

6. Geo-Blocking Jurisdictions

The websites use geo-blocking technology which renders them unavailable in selected jurisdictions. The websites, mobile banking and Internet banking are available in the jurisdictions listed below:

Andorra, Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Gibraltar, Greece, Hungary, Iceland, Ireland, Isle of Man, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Slovenia, Spain, Sweden, Switzerland, United Kingdom, Slovakia and the United States of America.

*Important Information

Web Browsers: While a wide range of browsers can be used , we recommend using the latest version of Google Chrome, Microsoft Edge or Mozilla Firefox. To ensure the best performance and security, web browsers should be downloaded from their official websites or from official stores and should be kept up to date.

Supported Mobile Operating Systems: The two most recent major versions of Android and iOS.

izola Bank

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

SEEN0725