SPARKASSE
Bank Malta plc

Security Notices

Sparkasse Bank Malta plc

Contents

SPARKASSE
Bank Malta plc

Spar Key

To maintain a high level of security around the Spar Key application, it is important to avoid using it on jailbroken or rooted devices, and to keep anti-virus software up to date to avoid instances of malware infections affecting app performance and security.

The PIN code used to open the app and receive confirmations is to be stored securely and not shared with other individuals who may have access to the device hosting the Spar Key application. Similarly the PIN should not be written down on desks or left in easy-to-find places. The Bank also advises against the use of PINs like “12345678”. Responsibility for device security rests with the customer not with the Bank.

Spar Key should only be downloaded from official channels, i.e. Google Play store for Android devices, the Apple App Store for Apple devices and by visiting the ‘’Apps’’ section on the Online Banking Service for the Windows Desktop version. Any Application which is not downloaded from any of these channels is not the Bank’s Application. If a customer receives an invitation to download the Application not as listed above, kindly contact the bank immediately and do not action the invitation.

The Bank also recommends that clients should not use Spar Key over unsecured public Wi-Fi connections. 3G or 4G connections are deemed safer. The same applies to downloading and installing Spar Key; unsecured public Wi-Fi connections are not recommended. Customers are advised to read through the User Manual, available on the Bank’s online banking system for additional security considerations concerning Spar Key.

The Bank recommends the use of Spar Key on multiple devices (you may have up to three), for service continuity purposes. In the event that a device is lost/stolen or otherwise compromised, customers are advised to immediately log into the Online Services (via one of the backup devices) and removing the lost/stolen/compromised device from their profile. This safety feature is important to bear in mind as the Bank provides online support only during office hours. Any lost/stolen/compromised devices are to be notified to the Bank as quickly as possible; to prevent such devices being used in a fraudulent manner.

SPARKASSE
Bank Malta plc

Spar Konnekt, PSD2 API

The Bank will only share its customers' information with a Third Party Provider ('TPP') with valid eIDAS certificates and subject to the appropriate consent being granted by customers. Similarly, payment transactions coming through a TPP will be only accepted subject to the TPP's eIDAS certificate being valid and successful application of Secure Customer Authentication ('SCA') by the customer where prompted throughout the payment journey.

The Bank recommends that its customers use only reputable TPPs, with proven track records and on whom there is sufficient publicly available information. Customers are advised to check that their chosen TPP websites are protected by secured encryption processes and are authentic. Customers should look out for the https:// text in the address bar and the padlock sign. This is especially true for API pages where it is required to enter credential information.

Furthermore the Bank advises against installing numerous financial apps on devices or entering credentials into numerous APIs, especially from publishers/companies that are not well known in the market. Doing so increases the chance that one of the apps installed or APIs used compromises online security.

SPARKASSE
Bank Malta plc

Protecting computers and other devices

The Bank recommends that its customers take the following measures among other possible security precautions:

- Anti-virus, anti-spyware and firewall protection - such software is to be regularly updated and computers should be scanned often against various threats;
- Downloads - Do not install files from unknown or untrusted websites;
- Emails and URL links - Do not open attachments from unknown senders and never access the Bank's website through a URL link received by email. Always type in the address yourself;
- Updates - Computer operating systems and web browsers are to be updated to the latest available versions; Google Chrome and Mozilla Firefox provide a better user experience when using the Bank's online services;
- Secure padlock - Our website is secured with an encryption process, unbroken key symbol or a locked padlock will appear in your web browser. Check for similar security details in other websites that request any credentials from you;
- Cache clearing - Browsing history and cache are to be deleted regularly; and
- Logging out - Always log out of the Bank's Online Banking service before closing browser or going to next website.

SPARKASSE
Bank Malta plc

Online Banking System considerations

- Log in - Never log in from public computers or internet cafes, spyware could be active which may track all your log in data;
- Do not open any other Internet websites or e-mails while a connection to our Online Banking Service is running.
- Be careful if you experience system interruptions or unusual error messages, (e.g. suddenly a white screen appears) or unusual error messages (e.g. “the system is currently busy). In this case, immediately cancel your connection and contact us;
- User name and password security and complexity - include nothing which may be connected to your personal life and ensure that the password is at least eight characters in length and at least include one of each of the following -> lower case letter, upper case letter, number, special character;
- Use of different log in details – ensure that you have distinct log in details across all your banking arrangements to avoid that someone could get access to all your bank accounts by obtaining a single password;
- Periodic change of your log in details – The Bank recommends that you change your passwords regularly and corporate customers are advised to implement a password management policy;
- Do not write down your log in details. - However if you must write them, make sure that it is in a secure place. When accessing online banking, pay attention to privacy;
- Do NOT share your login details – This also includes family and friends;
- Logout - always log out properly before you close the web browser and empty the browser cache regularly (recommended);
- Delivery of credentials – the Bank will request proof of identity of the persons collecting credentials in person from the Bank. This also applies to company drivers/couriers.
- Notify the Bank when problems are encountered – for example: lost/forgotten passwords, lost/stolen/compromised devices/ or other issues observed like suspected identity theft, security breaches, etc. The Bank should be notified so your profile/devices can be blocked pending the remediation of these issues.

SPARKASSE
Bank Malta plc

Phishing Emails (a common scam used to obtain personal information including login credentials on fraudulent websites)

- Always exercise caution when receiving unexpected emails;
- Double check the sender's email address and look out for spelling errors or unfamiliar domain names;
- At times, phishing emails are not personalised. They might be addressed in a very generic format, for example ''Dear Reader'' or ''Dear valued customer'';
- Wrong spelling and/or grammar in a phishing email may be a tell-tale sign; if the email contains links or attachments, proceed with caution when opening or downloading. Place your cursor over the link and ensure that the website is a trusted one. Only open attachments from trusted senders. The Bank also recommends confirming authenticity of the email by phone. Avoid dialling telephone numbers listed on the email itself. Only use telephone or fax numbers which are listed on our website (https://www.sparkasse-bank-malta.com/en/contact);
- If you are suspicious of or uncomfortable with an email supposedly sent by the Bank, kindly contact your Relationship Officer without hesitation. Do not open any links or attachments if the email is suspicious or unusual.

SPARKASSE
Bank Malta plc

Identity Theft

Fraudsters may attempt to steal your personal information and use it to impersonate you. They may try to access your bank account, make payments on your behalf or simply request information from the Bank. To avoid this from happening, the Bank recommends the following:

- Do not post excessive personal information on your Social Media Accounts. The more information you make available online, the easier it would be for a fraudster to steal your identity;
- Avoid giving ID card details, email address and mobile number details in social media chats, as these are not private and massive data leaks often occur;
- Never divulge your banking credentials to anyone;
- Report lost or stolen devices to the Bank immediately; and
- If you plan on disposing of, selling or giving away your device, ensure that all data is deleted first, including (and especially) any kind of banking/authentication application including Spar Key.

Smishing (Suspicious Texts)

Sparkasse Bank Malta plc does not currently send alerts or notices via text messages. If you receive a text message claiming to be from Sparkasse Bank Malta plc, kindly contact the Bank without hesitation and do not perform any action requested within the text message.

Vishing (Suspicious Calls)

- Please proceed with caution if you receive an unexpected or unscheduled call claiming to be from Sparkasse Bank Malta plc. Always ask for the details of the caller especially if it is an unfamiliar voice. Most of the time, you will be always contacted by your Relationship Officer.
- Take extra care if the call involves urgent requests, last minute deadlines or (veiled) threats. A potential fraudster may attempt to alarm you with announcements that your account has been compromised or that there is something wrong with a payment or that your account will be closed if you do not immediately comply with some request, in order to trick you in handing over sensitive information or scanned copies of documents.
- Sparkasse Bank Malta plc does not ask for credentials (Login/Passwords/PIN codes). If a caller specifically requests these details, terminate the call and contact the Bank immediately. Take note of the number used to make this suspicious call, where possible, and notify it to the Bank.
- The Bank will never request remote access to your computer or other devices. If such requests are made by anyone, you may safely assume that it is not a Sparkasse Bank Malta plc employee.

SPARKASSE
Bank Malta plc

Fraud

The Bank takes the detection and prevention of fraud seriously.

The Bank urges its customers to pay close attention to which invoices they accept to pay, to avoid instances of fraudulent invoices being correctly settled via Spar Key. In these cases it would not always be possible to recover the amounts involved.

Protect your personal and business information by removing unnecessary information from your website, social media and other public available materials. Invoices, account information and client data (as applicable) should never be left unattended. Having proper controls can help discourage, prevent and detect and prevent internal fraud.

Customers are advised to routinely review account statements and perform reconciliations using different members of staff from those tasked with uploading payments; implementing proper segregation of duties to counter the risk of internal fraud (as applicable).

Due care should be taken when calls requesting urgent payments are received. Such calls may be fraudsters seeking to pressure you into acting without thinking or getting clearance from your superiors (as applicable). The same is true of emails seeking to impersonate high ranking officers of your organisation (as applicable), and instructing unexpected money transfers.
Ideally, accounts are set up with multiple signatories and a process whereby more than one signatory needs to approve each payment, to ensure that payments are not misappropriated to a fraudulent or incorrect account. The Bank caters for this operational setup, when requested.

Customers are advised to avoid giving anyone remote access to their devices or computers.