Terms and conditions for accessing and using the E-Banking (online banking) Services – Individuals

These Terms and Conditions should be read in conjunction with the General Terms and Conditions of Banque de Luxembourg (hereinafter the "Bank") which apply to the relationship between the Client and the Bank, particularly with regard to the governing law and jurisdiction.

1. Purpose

These terms and conditions govern the Client's access to and use of online banking services via the Bank's E-Banking website and/or BL-Mobile Banking app (hereinafter the "E-Banking Services"), as well as the procedure for providing proof of trading and transactions carried out through one or more accounts held with the Bank over which they have signature power either as account holder, representative or attorney (hereinafter the "Accounts Available Online").

These Terms and conditions for accessing and using the E-Banking Services shall not create any new information or advisory obligation, nor do they constitute a new mandate under the responsibility of the Bank.

The Bank's E-Banking Services offer the following features in particular:

- Presentation of the Bank, its products and services,
- Market information,
- Financial research and analysis,
- Consulting Accounts Available Online,
- Perform some banking transactions,
- Electronic communication,
- Viewing and generating documents,
- Electronic signature of documents and instructions,
- Entering/modifying some personal data,
- Aggregation of accounts held with other payment service providers.

By accessing the E-Banking Services, the Client acknowledges and accepts that the Attorney may view any credit cards linked to the Accounts Available Online, request to block these cards or change their usage limit, and activate the 3D Secure service in accordance with the General terms and conditions governing payment cards.

Some of the functionalities mentioned above may be exclusive or may appear different on the E-Banking space or in the BL-Mobile Banking app.

The Bank reserves the right to modify these services at any time.

2. Fees and charges

Access to the E-Banking Services is invoiced according to the Bank's applicable charges. The Client hereby confirms that they have been informed of and accept such charges. Other charges, such as internet subscription (via an internet service provider) and roaming and data charges, shall be borne by the Client.

The Bank's Fees and Charges relating to transfers, stock market orders, interest rates and exchange rates shall apply.

3. Security of the E-Banking Services

3.1. Access modes

In order to access the E-Banking Services, the Client shall ensure that they have internet access through the internet service provider of their choice. The Bank accepts no liability with regard to the Client's internet connection, which shall be exclusively at the Client's own risk.

The E-Banking Services shall be accessed via the BL-Mobile Banking app or the E-Banking website, the address of which shall be provided to the Client along with their identifiers, or via any other web address that the Bank provides to the Client by whatever means it deems appropriate, including electronically.

If the E-Banking Services access mode is a LuxTrust Signing Server (LuxTrust Scan or LuxTrust Mobile App), the Client shall receive a text message or letter from LuxTrust containing the identifiers that correspond to their choice in order to enable them to connect to the E-Banking Services, identify themselves and sign instructions. The Client should memorise their identifiers and then destroy the letter or delete the text message. If the E-Banking Services access mode is another authentication method recognised by LuxTrust, the Client shall receive the means as well as the terms and conditions of use from the provider of their authentication solution.

Where applicable, any device to be used for authentication purposes shall be provided or sent in a separate envelope.

The Client expressly authorises the Bank and LuxTrust to supply identifiers and means for access to the E-Banking Services to current or future attorneys who have signature power or right of inspection on the Accounts Available Online when such persons request access.

3.2. Client due diligence

To prevent fraudulent use of the E-Banking Services, the Client undertakes to protect all of their identifiers and to take security measures to maintain sole control over their access authentication modes (authentication device and identifier received by LuxTrust or another recognised provider of their authentication solution, password, one-time password), which they alone know and retain. The Client shall be solely responsible for ensuring that their personal codes are kept strictly confidential. They must not be written down, disclosed or shared with a third party or saved to the hard drive of one or more devices.

The Client is aware of the fact that the Bank will never contact them by telephone, email, text message or any other means of communication to obtain confidential information (identifier, password, one-time password) or to invite them to connect to the Bank's E-Banking Services via a link in an email or text message.

The Client should therefore consider as suspect any unsolicited email or text message that claims to come from the Bank asking them to communicate bank details and/or their password. In addition, the Bank recommends that the Client manually enter the address https://www.banquedeluxembourg.com and check that there are no spelling mistakes rather than clicking on a link in an email or text message.

The Client undertakes to familiarise themselves with the risks described in the appendix entitled "Notice concerning the risks inherent to credit transfers made via the E-Banking (online banking) Services" and to follow the recommendations and security provisions in the

"Security Information" on the E-Banking website and/or BL-Mobile Banking app as well as in the appendix entitled "What can you do to reduce risk? Review of best security practices on the internet".

Failure to comply with these security provisions shall be considered gross negligence and the Client shall be held liable for any losses that may result from fraudulent use of the E-Banking Services.

3.3. Blocking access to the E-Banking Services

3.3.1. At the request of the Client

Should the Client become aware or suspect that a third party has gained access to the E-Banking Services following the loss, theft, fraudulent use or unauthorised use of one of their means of identification, they shall immediately inform the Bank and LuxTrust or any other provider of their authentication solution of so that the access can be blocked, from 8am to 6pm Monday to Friday:

LuxTrust assistance: (+352) 24 550 550

BL-Support assistance: (+352) 26 20 26 30

If the Client accesses the E-Banking Services using another authentication method, they will contact the provider of this alternative authentication solution for assistance.

If it is not a business day, the Client will block their own LuxTrust tool, which they can do 24/7 on the LuxTrust website (https://www.luxtrust.lu/en/management).

If the Client accesses the E-Banking Services using another authentication method, they will visit the website of the provider of this alternative authentication solution.

3.3.2. On the initiative of the Bank

When the Bank's detection rules flag suspected fraud, established fraud or threats to the security of the Client's access to the E-Banking Services, in particular as regards suspected fraud involving transfers, the Bank will contact the Client by any means it deems appropriate and, where applicable, will inform them that their access to the E-Banking Services has been limited or blocked in order to minimise the risk of unauthorised or fraudulent activity; the Bank has no obligation or liability in relation to this security procedure.

The Bank reserves the right to limit, block or permanently withdraw the Client's access rights to the E-Banking Services should the Client fail to comply with their obligations or the Bank's recommendations, or in the event that the Bank considers it prudent to prevent the Client from gaining access for any other objectively justified reason linked to factors including, but not limited to:

- **the security of access to the E-Banking Services;**
- **the observation, presumption or risk of unlawful, unauthorised, abusive or fraudulent access;**
- **protecting the interests of the Client or of the Bank;**
- **accounts being liquidated or blocked, or if it transpires that the Client does not comply with their legal, regulatory or contractual obligations with regard to the services offered;**
- **a request from a legal authority;**
- **the death of one of the account holders;**
- **a significantly increased risk that the Client may not be able to honour their payment obligations with respect to a credit line (where the Bank has granted an overdraft to the Client accessing the E-Banking Services).**

In such cases, the Bank will inform the Client of the block and the reasons for it immediately after it is imposed, except where providing this information would be unacceptable for security reasons or prohibited under applicable legislation. The Bank will lift the block or arrange a new form of access when the reasons justifying the block cease to exist.

3.4. Access and security

Access to the E-Banking Services is protected by an encryption and identification solution.

The Client acknowledges that the Bank has provided all the necessary information concerning the security, efficiency and restrictions of this process. They accept as satisfying and formally discharges the Bank from any liability concerning the consequences of any breach of the security system by an unauthorised third party. They also authorise the Bank to modify the practical and technical workings of the E-Banking Services, and, in particular, the security system that offers access to the E-Banking Services, particularly in the event of any upgrades or technological improvements. The Client shall be informed of such improvements by any means deemed appropriate by the Bank.

The Client undertakes to strictly comply with the procedures for connecting to the E-Banking Services, as explained by the Bank, as well as any instructions for use displayed via the E-Banking Services or communicated to the Client by any other means. They undertake to check the secure character of the communication at each connection. In the event of this procedure not being observed and/or of any other instruction for use being ignored, e.g. attempts to connect to the E-Banking Services using an incorrect identifier, the Bank reserves the right to prevent the Client from further attempts to access the E-Banking Services.

The parties mutually agree that access to the E-Banking Services using one of the Client's identifiers shall be deemed to be made by the Client, with the Bank's connection log serving as proof thereof.

In addition, each connection to the E-Banking Services by an attorney or a representative of the Client using their identifier shall be deemed to have been made by that attorney or representative in the name of and on behalf of the Client. The Client remains entirely responsible for voluntary and involuntary actions and omissions on the part of their attorneys or representatives in the context of their use of the E-Banking Services until such time as their access is revoked on the initiative of the Client, their attorneys or representatives, or the Bank.

Excluding instances of gross misconduct or negligence on its part, the Bank accepts no liability and will not be blamed for any breach of secrecy should a third party access the Client's Accounts Available Online or gain any other kind of information as to their relationship with the Bank via the E-Banking Services and/or the BL Mobile Banking application or the internet.

4. Information accessible via the E-Banking Services

The Client may use the E-Banking Services to consult financial and economic information offered by the Bank as well as other parties, notably about the financial markets and investment funds.

In so far as possible the Bank shall display the date of publication or creation of the information on the E-Banking

Services and undertakes to keep this information as up-to-date as its paper-based information.

All information published via the E-Banking Services is provided for information purposes only and should not be interpreted as advice or guidance from the Bank. The Client undertakes to use the information with proper judgement and a critical eye.

The Client expressly releases the Bank from any liability relating to the content, reliability, timeliness, integrity or accuracy of information from a third party and indicated as such.

The Client expressly acknowledges that no advice shall be given online by the Bank with regard to information published via the E-Banking Services, and undertakes to obtain advice relating to their investments and portfolio management directly from an adviser of their choice at the Bank.

The Client undertakes to respect the confidential nature of the information available via the E-Banking Services and to refrain from passing this information to a third party, from publishing or disseminating it by any means or for whatever reason, and from reproducing the E-Banking Services in part or in full. Notwithstanding any written information to the contrary, the Client authorises the Bank to send them any promotional material via the E-Banking Services or by email.

5. Consulting Accounts Available Online

The Client may consult the Accounts Available Online via the E-Banking Services as well as pending trades on these accounts, where applicable. The Client authorises the Bank to send them information online about the Accounts Available Online as well as operations on these accounts. This does not affect any agreements that the Client may have with the Bank pertaining to correspondence to be held at the Bank's premises on behalf of the Client.

If the Client has opted to consult their Accounts Available Online (of which they are the account holder or representative) solely via the E-Banking Services, they shall undertake to consult these accounts at least once per quarter. If the Client has not consulted their Accounts Available Online for a continuous period of six months, the Bank shall revoke their access to the E-Banking Services and shall forward to the Client any account statements and correspondence relating to the Accounts Available Online to the address provided in the account-opening application form or other address provided by the Client.

The Bank reserves the right to deny the Client access to one or more of their Accounts Available Online via the E-Banking Services if it deems it has a valid reason to do so.

6. Electronic orders

The Client may use the E-Banking Services to submit to the Bank orders for credit transfers and trades on financial instruments (hereinafter "Electronic Orders"), which will be executed according to the same conditions applied to their other orders. Using the E-Banking Services, the Client may also electronically sign documents submitted to them by the Bank; this electronic signature shall have the same weight as a handwritten signature.

With regard to Electronic Orders submitted to the Bank, the Client undertakes to provide the specific information required for the proper execution of that order. The Bank will display the information that the Client has entered on screen.

Unless the Bank has authorised the Client to do so by granting them an overdraft facility, the Client may only execute transactions when the account balance is positive and such transactions are limited to sufficient coverage in their account. The Client undertakes to ensure that there is a sufficient positive balance in the current account to cover Electronic Orders, within the set usage limits. The Client acknowledges that in the event that the account is not sufficiently funded, debit interest will apply as provided for under article 15 of the Bank's General Terms and Conditions. The Bank reserves the right to refuse any Electronic Order if the account is not sufficiently funded.

The Client shall be responsible for all orders signed off using their identifiers until the Bank receives notice from the Client not to trust such orders (as per the procedure set out in article 3.3 above) and the Bank is in a position to refuse such orders.

The Client is responsible for all Electronic Orders submitted via the E-Banking Services by the Client, their attorney or their representative, even in the event that the power of attorney granted to the attorney or representative has been revoked.

The parties acknowledge that Electronic Orders submitted and documents electronically signed via the E-Banking Services shall have the probative value of a private agreement in accordance with articles 1322 et seq. of the Civil Code, and that they are binding on both the Client and the Bank regardless of the amount or scope.

6.1. Orders involving financial instruments

Orders to purchase or sell financial instruments are presumed to be instructed for execution and/or for reception and transmission as execution-only orders, as referred to in Article 12 of the Bank's General Terms and Conditions.

6.2. Transfer orders

6.2.1. Declaration of acceptance of risks

The Client declares that they are aware of the risks inherent to executing transfer orders via the E-Banking Services as set out in the appendix entitled "Notice concerning the risks inherent to credit transfers made via the E-Banking (online banking) Services".

The Client hereby states that they are aware of the risk of loss involved in making transfers via the E-Banking Services and that such risks are greater if transfer limits are raised. Moreover, they are aware that if more than one account is linked to a BL Web User, the maximum limit of the BL Web User will be the total sum of the limits defined for each account.

The Client hereby declares that they accept that all transfers made on the E-Banking Services using their personal access codes be executed at their own risk and hereby releases the Bank of any liability resulting from negligent or wrongful behaviour on their part, or non-compliance with the rules of conduct described in this document and its appendices.

6.2.2. Consent and revocation of transfer orders, execution period

A transfer order shall be considered to have been authorised if the Client has consented to the execution through the means of authentication and validation required by the E-Banking Services. In the absence of such consent, the transfer order shall be considered unauthorised.

The provisions concerning the timeframes for receiving and revoking payment orders and the execution deadline, set out in article 9 of the Bank's General Terms and Conditions, shall apply in full.

6.2.3. The Client's liability for unauthorised transfers

Until the theft, loss or fraudulent use of their E-Banking Services identifiers has been reported, the Consumer Client may be held liable for losses of up to EUR 50 linked to unauthorised transfers resulting from the misuse of their E-Banking Services identifiers. This clause does not apply if the loss, theft or fraudulent use of the access rights could not be detected by the Client prior to the payment, unless the Client has acted fraudulently or the loss was due to actions or negligence on the part of an employee, agent or branch of the Bank, LuxTrust or another authentication solution provider.

The maximum liability is set at EUR 50. This shall not apply to non-Consumer Clients.

Both the consumer Client and non-consumer Client shall be liable for all losses resulting from unauthorised transfers if such losses result either from fraudulent action on their part, or from the fact that they have not complied, either intentionally or following gross negligence, with the security provisions and/or obligations set out in article 3 of these terms and conditions. In this scenario, the maximum amount listed above does not apply. The following shall be considered cases of gross negligence: (i) the Client writes down their personalised security details, such as their personal identifier or any other code, in an easily recognisable form, (ii) the Client discloses such details to a third party, (iii) the Client saves such details to the hard drives of one or more unsecured devices, and (iv) the Client fails to notify the central cancellation service of the theft or loss as soon as they become aware of it. All factual circumstances shall be taken into account in order to assess the extent of the negligence.

Should the Bank reimburse the Client for an amount corresponding to an unauthorised transaction and subsequently have reason to believe that the Client has acted fraudulently or failed to meet one of the obligations set forth above, either intentionally or as a result of gross negligence, the Bank reserves the right to debit this amount from the Client's account and inform the Commission de Surveillance du Secteur Financier (CSSF), headquartered at L-1150 Luxembourg, 283 route d'Arlon.

6.2.4. Right to repayment, notification and correction of unauthorised or incorrectly executed transfers

The right to repayment, notification and correction of unauthorised or incorrectly executed transfers is governed by the relevant provisions set out in article 9 of the Bank's General Terms and Conditions.

6.3. Book entries linked to Electronic Orders

Electronic Orders are executed by means of a book entry and analogous to the operations described in articles 9 and 12 of the Bank's General Terms and Conditions. The Bank must be notified immediately of any book entry linked to an unauthorised transaction, or any error or other irregularity in the management of the account.

The Bank undertakes to keep a log of all the Electronic Orders signed by the Client on a durable medium and for a period of 10 years, while ensuring that the records remain unchanged. The Client expressly agrees that the records of their Electronic Orders kept by the Bank shall be proof of their existence, content, and precise date and time, and that these details be valid before a court of law. The Bank shall provide the Client with a copy of all such records upon request.

7. Complaints by the Client

The complaint procedures, including the extrajudicial recourse options available to the Client, are indicated in article 7 of the Bank's General Terms and Conditions.

8. Account aggregation service

The account aggregation service corresponds to the account information service provided for in PSD 2[1]. It consists in providing, via the internet, consolidated information on the payment account(s) held by and identified by the Client with one or more payment service providers identified by the Client. This information includes the balance on such accounts and the payment operations executed over the last 90 days using the payment account(s) identified.

The Bank cannot supply the Client with information provided by the payment service provider(s) identified by the Client; it cannot be held liable for any lack of information for which this/these payment service provider(s) is/are responsible.

The account aggregation service is not dependent upon the existence of contractual relations between the Bank and the other payment service providers. It is supplied on the basis of the Client's express consent and adequate authentication with respect to other payment service providers, on the condition that the accounts identified are accessible online and the Client is the account holder of the Accounts Available Online with the Bank. The Client's consent will be requested when they access the account aggregation service for the first time; it will expire and require renewal 90 days later.

As part of the account aggregation service, the Client expressly authorises the Bank to use their personalised security details in order to enable the Client to identify themselves securely with respect to the payment service providers identified by the Client. The Bank ensures that the Client's personalised security details are not accessible to any parties other than the Client and the issuer of these details and uses safe and effective means of transferring such details.

The Bank only accesses information derived from the accounts identified by the Client and associated payment operations. In accordance with data protection rules, the Bank does not use, view or store these details for any purposes other than the account aggregation service.

1 Directive (EU) 2015/2366 of the European Parliament and Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

9. Processing and protection of personal data

In order to grant access to the E-Banking Services, the Bank will need to process the personal data of the Client for the purposes of executing this contract and managing the client relationship and any related services.

The information collected by means of this E-Banking Services Application Form may be stored on any medium and saved by the Bank in a computer file, and processed for the purposes of authenticating and managing access to the E-Banking Services, managing accounts and transactions, and ensuring their regularity.

In order to meet its regulatory obligations, particularly with regard to anti-money laundering and anti-terrorist financing legislation, the Bank may have to verify the authenticity of the data provided by the Client and transfer this data to the public authorities and competent courts.

The Bank may store personal data for a period not to exceed that necessary for its purposes, and in accordance with its General Terms and Conditions.

The Bank transfers the Client's personal data to LuxTrust and/or any other provider of the authentication solution chosen by the Client and recognised by LuxTrust in order to execute this agreement and provide the E-Banking Services. It also transfers the Client's personal data to LuxHub, which manages the interface (API), for the purposes of providing the account aggregation service. The Client expressly consents to these companies processing their data for these purposes. The Client has the right to request access to their personal data as well as its correction, erasure and portability. They also have the right to object to or restrict its processing.

The Client may consult and/or modify their personal data via the E-Banking Services. The Client requests that any changes of which the Bank is notified in this way be considered in the same way as any other notification of a change in personal data.

The Client undertakes to provide correct and accurate information to the Bank, to inform the Bank as soon as possible of any change in their personal information, and to communicate on request any document or additional information that the Bank deems necessary within the framework of the banking relationship or that may be required by legal or regulatory provisions.

10. Accessibility of the E-Banking Services

The Bank reserves the right to temporarily suspend access to the E-Banking Services, including for technical reasons.

Should the Bank expect that access to the E-Banking Services may become temporarily unavailable, it will make every effort to give the Client advance notice, using all appropriate means, including a message displayed via the E-Banking Services.

The Client discharges the Bank from any liability arising from the temporary inability to access the E-Banking Services, for whatever reason, and from consequences arising from a breakdown or malfunction of the E-Banking Services, from the Bank's IT infrastructure, from the E-Banking Services being disconnected or from any other technical incident, even in case this is through the fault of the Bank.

11. Message confidentiality

The parties acknowledge that messages sent using the E-Banking Services shall be considered to be of the nature of private correspondence.

12. Place of communication

Communications between the Bank and the Client, as well as any operations initiated or completed using the E-Banking Services shall be considered as having been conducted at the Bank, at the date and time indicated on the Bank server and confirmed by the Bank's connection log.

13. Destruction of identifiers and certificates

In the event that the Client no longer has access to their Accounts Available Online via the E-Banking Services, they undertake to destroy all means of authentication provided by the Bank.

14. Liability

In its role as E-Banking Services provider, the Bank's responsibility shall only extend to due diligence and best efforts with regards to the Client. In accordance with article 21 of the Bank's General Terms and Conditions, the Bank shall only be liable for gross negligence.

The Bank cannot be held liable in cases of force majeure or where it is bound by other applicable legal obligations.

Should the Client access the E-Banking Services in another country, they undertake to abide by the legal regulations and requirements in force in the country in which the access takes place. The Bank will not be held liable in the event of the failure of the authentication solutions provided by the supplier of the authentication solution chosen by the Client.

15. Amendment to the Terms and conditions for accessing and using the E-Banking Services

The Bank may amend these Terms and conditions for accessing and using the E-Banking Services by notifying the Client in writing by any means, including via a message sent by or displayed on the E-Banking Services, as set out in article 23 of the General Terms and Conditions.

The Client shall be deemed to have accepted this amendment if they use the E-Banking Services after receiving notification of the amendment.

Should any of the clauses of these Terms and conditions for accessing and using the E-Banking Services become inapplicable or void, this shall not affect the validity of the other clauses which shall remain in force unless any of their provisions are rescinded.

16. Term and termination of the agreement

The Terms and Conditions for accessing and using the E-Banking Services is concluded for an indefinite term.

16.1. Termination by the Client

The Client may terminate their access to the E-Banking Services at any time, free of charge and without having to give a reason. The fact that the Client being account holder has terminated their access does not automatically result in the termination of access granted to their attorneys or representatives. Furthermore, the Client is liable for all transac-

tions which have yet to be recorded in the form of a book entry when their access is terminated, whether they were ordered by the Client themselves or by their representative or attorney.

Should an attorney or representative terminate their access to the E-Banking Services, this will not result in the termination of the access granted to the Client being account holder or, where applicable, to the other attorneys or representatives. The Client being account holder has the right to terminate the access granted to their attorneys or representatives. In such cases, the Client being account holder remains jointly and severally liable for the operations carried out by this attorney or representative until their access is terminated.

16.2. Termination by the Bank

The Bank may terminate the Client's access to the E-Banking Services at any time, with immediate effect, free of charge and without having to give a reason. For the consumer Client, the Bank may terminate their access with at least two months' notice.

When the Bank terminates the Client's access, it shall inform the Client by any means the Bank deems appropriate.

The Client is liable for all transactions that have yet to be recorded in the form of a book entry when their access is terminated.

17. Acceptance of the LuxTrust general terms and conditions

Clients having opted for the LuxTrust access mode state that they are aware and approve of the LuxTrust general terms and conditions and any other terms and conditions binding them or the Bank to LuxTrust, with regards to the access mode. Please check www.luxtrust.lu for more information. Clients having opted for another access mode recognised by LuxTrust state that they are aware and approve of the general terms and conditions of their provider and any other terms and conditions binding them or the Bank to the provider, with regards to the access mode.

Appendix: Notice concerning the risks inherent to credit transfers made via online banking on the E-Banking website

Notice concerning the risks inherent to credit transfers made via online banking on the E-Banking website

This notice is intended to provide a non-exhaustive list of some of the risks involved in electronic credit transfers.

Phishing

"Phishing" is a technique used by online fraudsters (scammers), pretending to represent the Bank in a bid to collect personal details about clients.

phishing email or text message:

This is a technique that computer hackers use to mimic emails or institutional websites to collect confidential data relating to your bank accounts, such as your account number and access codes. The victim receives a scam email or text message from a bank or official organisation. The messages pretend that a technical upgrade of the bank's website is needed or that your personal details need to be verified. By clicking on a link in the message, the victim is redirected to a site mimicking the bank's official website and then invited to enter their identifiers and personal passwords.

The emails may also consist of emails about fictitious lotteries, informing the victim that they have won. In order to pay out the winnings, the scammers request the victims' personal banking details.

Some emails seek the victim's assistance in order to transfer funds. The sender will ask to use the victim's account for the transmission of a very large sum, promising a percentage. These requests are scams and should be ignored.

phone phishing:

You receive a phone call from someone pretending to represent the Bank.

This person explains that, due to technical problems, your account will be closed if you do not disclose personal information such as your account number and password.

Identity theft

A malevolent person knowingly uses the identity of another person in order to carry out fraudulent actions.

To use someone else's identity, a scammer needs to have obtained in advance the personal and confidential information of the scam victim.

Identity theft can have serious consequences including the constitution of false papers, use of bank accounts and execution of fraudulent transactions.

For example, by stealing your email address, the fraudster has access to all your emails and can write to your contacts using your email address and your style of communicating and betray the trust of those close to you.

Malware

Malware is a computer program developed to intentionally harm a computer system, or collect data without the user's knowledge.

It comes in many forms: viruses, worms or Trojan horses are the most widely known examples (a Trojan horse is a virus installed when you access a hacked website or open an attachment in an email or text message; for example, it may collect details of the keys that are pressed and then automatically transfer these to the fraudsters).

Such programs are becoming increasingly sophisticated with advances in technology.

What can you do to reduce risk? Review of best security practices on the internet

Never tell anyone your password or your personal identifiers!

The Bank will never ask its clients for their access codes (passwords, one-time passwords or any other confidential information) by email, phone, text message or any other means of communication.

How can I protect my password?

Choose a secure password (composed of at least 8 characters, including numbers and special characters) and change it regularly. Use different passwords for every website you visit (online banking access to other banks' online banking, email, online shopping, social networks, forums, etc.).

How can I protect my device?

To protect your access to the E-Banking website or BL-Mobile app, always use a device (computer, smartphone, tablet, etc.) you trust and know is secure; avoid public computers.

We recommend that you:

– install antivirus and antispyware software on your computer which update automatically on a regular basis
– install recent updates of your operating system and internet browser
– only install trustworthy programs
– activate the firewall.

How can I check that I really am on the Bank's online banking website?

Go directly to the Bank's website by entering https://www.banquedeluxembourg.com in the address bar of your internet browser, having checked the address for typos, or access it from your Favourites if you have saved the address there previously. Never click on a link in an email or text message.

– Click on "MY ACCOUNT ONLINE" then select your authentication mode:
– Check that the address starts with "https"
– Check that there is a padlock symbol at the bottom and/or top of the secure page and that the padlock is closed
– Double-click on the padlock
– A screen representing the Bank's digital certificate appears
– Check that the name on the certificate actually says "BANQUEDELUXEMBOURG.COM"

How can I log off securely and check when I last connected to the online banking site?

After checking your accounts online, always terminate the connection on your personal area of the E-Banking Services using the "Logout" button and close the window of your browser. The date and time of your last connection using your identifiers are shown under the log out button. Remember to check movements on your accounts.

How can I protect against phishing?

This is a technique that computer hackers use to mimic emails or institutional websites to collect confidential data such as your credit card number, identifier, password, name, first name, date of birth, address, phone number, etc.

In most cases, this scam uses fake emails from banks or official organisations. The messages use the pretext of a technical upgrade of the site in question or say that your personal details need to be verified. By clicking on a link contained in the email, you are redirected to a site that mimics the institutional site and invited to enter your personal data.

To protect against phishing, be vigilant concerning any such message or call, its content, and the address of the sender.

Remember that the Bank and other financial institutions in general will never ask a client for their password, identifier or OTP by email or phone.

What can I do if I've lost my access codes and who can I contact if I have a question?

If you have lost your access codes, please contact LuxTrust (www.luxtrust.lu) or the provider of your authentication method as soon as possible. For any other questions regarding your account or problems the BL Mobile Banking application, please telephone BL-Support (+352) 26 20 26 30, open Monday to Friday from 8am to 6pm.