COMMUNIQUÉ DE PRESSE
PRESSEMITTEILUNG
PRESS RELEASE

Luxembourg, September 7, 2025

Our priority: protecting our clients and protecting the Bank against fraudsters

In light of the recent waves of banking fraud affecting the entire financial sector, Banque Internationale à Luxembourg (BIL) reaffirms its commitment to the fight against cybercrime. For years, the Bank has been investing in advanced technologies and expertise, and it will continue to act with determination on two fronts: protecting its clients and supporting them when they are victims, while relentlessly strengthening its already robust infrastructure.

“We know that behind every fraud case there are victims, some of whom find themselves in great difficulty. We are doing everything we can to support them as best as possible and to prevent these situations from happening again,” commented Jeffrey Dentzer, CEO of BIL.

A growing and organized threat

In 2024, the Grand Ducal Police recorded close to 6,400 cases of fraud in Luxembourg[1], a number that continues to rise. Fraudsters are increasingly well-organised and they use sophisticated methods: fake websites imitating banks websites, fake invoices, misleading sponsored links on search engines, text messages, phone calls from fake advisors... While security measures are regularly adapted and strengthened and awareness campaigns are multiplying, they still do not prevent clients from falling victim to these fraud attempts.

Measures implemented by BIL when a case is detected

For each case detected, the Bank quickly implements a series of measures:

- **Blocking client accounts**: as soon as fraud is detected, BIL blocks the affected accounts, cards, and the LuxTrust certificate.
- **Blocking outgoing funds**: the Bank blocks transfers to the fraudsters’ accounts.
- **Funds recall**: the Bank contacts the banks to which the money was transferred to recover the funds.
- **Systematic reporting**: each fake website is reported to the website hosts and search engines so it can be quickly deactivated.

When the fund couldn’t be recalled

In some cases, despite all the measures taken, the funds transferred by the fraudsters cannot be recovered because they have already been transferred elsewhere.
In the case of the malvertising campaign that took place in July, for example, three quarters of the transfers attempted by the fraudsters were successfully blocked before execution. We were also able to recall part of the funds that had already been transferred to the fraudsters’ accounts. For other clients, unfortunately, this recall did not work. The money was moved too quickly and was no longer in the account, often abroad, used by the fraudsters.

[1] Rapport d’activités 2024, Police Grand ducale

BIL closely monitors each case. Judicial and banking proceedings are underway. As they involve several jurisdictions and financial institutions, these proceedings will be long and complex, and do not guarantee the recovery of funds.

“We understand that this uncertainty is difficult for victims. That’s why we are doing everything we can to provide rigorous follow-up. We are working closely with the authorities and the Luxembourg financial sector,” added Nicolas Remarck, Head of Cybersecurity.

Filing a complaint with the Public Prosecutor
BIL, which is also a victim in this matter, has decided to file a complaint with the Public Prosecutor Office of the Luxembourg District Court, while reserving the right to bring a civil case. It is now up to the justice system to conduct its investigation. We have also filed complaints with the foreign banks to which the money was fraudulently transferred to and with the search engine that was the entry point for this attack.

Our commitment
Aware of the financial and psychological impact of these frauds on the victims, BIL has launched a review of its fraud case management process in order to:

- Shorten the response time for victims.
- Enhance communication and personalised follow-up with clients.
- Make the steps clearer and easier for clients to follow.

To respond to constantly evolving digital fraud scenarios, BIL is also committed to continue:

- Improving its support to clients.
- Raising regularly public awareness on the different fraud scenarios.
- Investing in cybersecurity.

The fight against fraud is a collective one: it involves banks, judicial and police authorities. It also requires the vigilance of everyone. Protecting our clients against fraudsters is our absolute priority.

Annexes - How fraud works and how to protect yourself from it

In recent months, numerous fraud attempts have targeted residents and businesses in Luxembourg. Like other banks, BIL has observed that fraudsters are using increasingly sophisticated techniques to deceive clients: fake websites imitating those of banks, fake invoices, sponsored links on search engines, text messages, calls from fake advisors... The goal of these malicious groups: to trick clients to get their personal data or online banking passcodes, access their bank account and make transfers.

Each case of fraud is specific. While we cannot detail them all, we can try to explain the complexity of the scenarios put in place. Let's take the example of a malvertising campaign, in other words, an online advertising campaign set up to lure clients to a fake banking website.

The stages of a malvertising campaign

1. Preparatory phase

To try to obtain clients' login details, fraudsters develop and activate a fake website, copying the login page of a bank in every detail. The URL used contains all or part of the name of the targeted company.

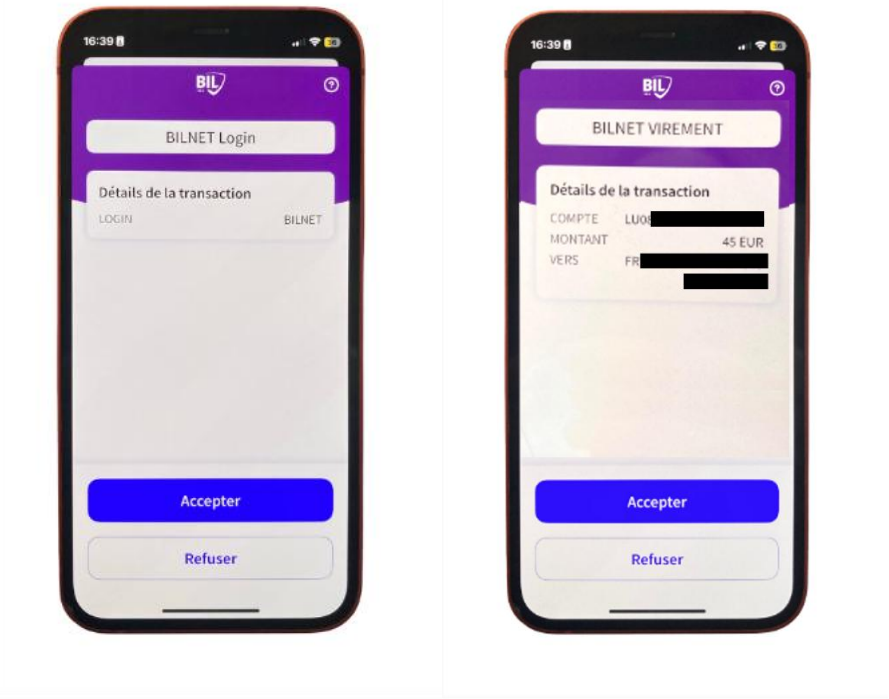
It is impossible for a company to acquire all domains containing its name. A change of a letter or a punctuation mark is generally used, but the combinations are limitless.

To attract clients to this website, fraudsters set up a sponsored link on search engines to ensure being listed at the top of search results, thereby increasing visibility and luring unsuspecting users to a fraudulent website.

1. Materialisation of the fraud

On their computer or tablet, the client uses a web browser and a search engine to find the Bank's website. The client clicks on the sponsored link placed at the top of the results and lands on the fake website.
The client enters their login details on the fake site, which are collected in real time by the fraudsters. Simultaneously, the fraudsters use these credentials and password to log in to the client's account on the Bank's real website.
The client, still on the fake website, approves the fraudsters' login with the LuxTrust Mobile app, thinking they are approving their own connection. The fraudster, now connected to the client's account, creates a new beneficiary to make a transfer. They prepare the transfer, which must be validated with LuxTrust Mobile.
Meanwhile, the client is still on the fake website. A message tells them that due to a technical problem, they must approve their connection again. The LuxTrust Mobile app presents a new

message to the client. This time, the message shows the IBAN of the recipient account and the transaction amount. The client does not read this message and approves the transfer.



A LuxTrust validation is equivalent to a handwritten signature. While technological advances allow the entry of a code (as was the case with the physical Token) to be replaced by faceID or fingerprint, it remains a validation with legal value.
It is therefore extremely important to be vigilant when you approve an action on LuxTrust and to carefully read the details of this action. If the information is suspicious, cancel the operation and if in doubt, contact the Bank or Worldline immediately.

Discovery of the fraud and implementation of protection measures

Clients, realizing they have just been victims of fraud, can call BIL at 45 90 5000 during opening hours or the Worldline service at 49 10 10 on evenings and weekends. This number is a service shared by banks in Luxembourg.
After analyzing the situation and the scenario, the Bank and Worldline implement additional protection measures: account blocking, deactivation of the LuxTrust certificate, blocking of transfers to recipient accounts used by fraudsters, reporting of the sponsored link to the search engine and of the fraudulent website to the host, and recalling the funds.

Funds recall procedure

When the transfers could be stopped directly, the transaction is void and does not impact the client. If the transaction went through, the Bank follows the fund recall procedure, which is

quickly and automatically implemented. However, the beneficiary's institution can take up to 4 weeks to respond. If these attempts succeed, the funds are returned to the clients.

How to protect yourself

Let's recall some good practices to prevent fraud:

- Use BIL's mobile banking app.
- If you use a web browser on your computer or tablet, do not use a search engine. Type the full address of the bank's website yourself, www.bil.com and save this address in your favorites.
- Always check the message from your LuxTrust app to confirm your login or to approve a transaction. This is equivalent to your signature.
- Never give your banking credentials to a someone you don't know. Your bank will never ask for them, neither by email, nor by SMS, nor by phone.
- If in doubt, call BIL at 45 90 5000 during opening hours or Worldline at 49 10 10 during evenings and week-ends.

We also encourage clients to actively report any fraud attempts (such as phishing emails, fake websites, or suspicious messages) directly to the Bank, so that we can act quickly to protect everyone.

About Banque Internationale à Luxembourg (BIL):
Founded in 1856, Banque Internationale à Luxembourg (BIL) is the oldest multi-business bank in the Grand Duchy. It has always played an active role in the main stages of development of the Luxembourg economy. It currently operates in retail, private and corporate banking, as well as on financial markets. Employing more than 1,900 people, BIL is present in the financial centres of Luxembourg, Switzerland, and China.
www.bil.com

For more information, please contact :
Banque Internationale à Luxembourg SA
69, route d'Esch • L-2953 Luxembourg
E-mail : mediarelations_bil@bil.com