COMMUNIQUÉ DE PRESSE
PRESSEMITTEILUNG
PRESS RELEASE

Luxembourg, le 7 septembre 2025

Notre priorité : protéger nos clients et protéger la banque contre les fraudeurs

À la lumière des récentes vagues de fraudes bancaires touchant l'ensemble du secteur financier, la Banque Internationale à Luxembourg (BIL) réaffirme son engagement dans la lutte contre la cybercriminalité. Depuis des années, la Banque investit dans des technologies avancées. Elle continuera d'agir avec détermination sur deux fronts : protéger ses clients et les accompagner lorsqu'ils sont victimes, tout en renforçant sans relâche son infrastructure déjà robuste.

« Nous savons que derrière chaque cas de fraude, il y a des victimes, dont certaines se retrouvent en grande difficulté. Nous faisons tout notre possible pour les accompagner au mieux et pour éviter que ces situations ne se reproduisent », déclare Jeffrey Dentzer, CEO de BIL.

Une menace croissante et organisée
En 2024, la Police Grand-Ducale a enregistré près de 6 400 cas de fraude au Luxembourg, un chiffre qui ne cesse d'augmenter. Les fraudeurs sont de plus en plus organisés et utilisent des méthodes sophistiquées : faux sites internet imitant ceux des banques, fausses factures, liens sponsorisés trompeurs sur les moteurs de recherche, SMS, appels téléphoniques de faux conseillers… Bien que les mesures de sécurité soient régulièrement adaptées et renforcées et que les campagnes de sensibilisation se multiplient, elles ne suffisent pas à empêcher les clients de tomber victimes de ces tentatives de fraude.

Mesures prises par la BIL
Pour chaque cas détecté, la Banque met rapidement en œuvre une série de mesures :

- **Blocage des comptes clients** : dès qu'une fraude est détectée, la BIL bloque les comptes concernés, les cartes et le certificat LuxTrust.
- **Blocage des fonds sortants** : la Banque bloque les virements vers les comptes des fraudeurs.
- **Rappel de fonds** : la Banque contacte les banques vers lesquelles l'argent a été transféré afin de récupérer les fonds.
- **Signalement systématique** : chaque faux site est signalé aux hébergeurs et aux moteurs de recherche pour qu'il soit rapidement désactivé.

Lorsque les fonds n'ont pas pu être rappelés

Dans certains cas, malgré toutes les démarches engagées, les fonds transférés frauduleusement ne peuvent être récupérés, car ils ont déjà été retirés par les fraudeurs. Dans le cas de la campagne de « malvertising » qui a eu lieu en juillet par exemple, les trois quarts des virements tentés par les fraudeurs ont été bloqués avant exécution avec succès. Nous avons également pu rappeler une partie des fonds qui avaient déjà été transférés sur les comptes des fraudeurs. Pour d'autres clients, malheureusement, ce rappel n'a pas fonctionné. L'argent avait été déplacé trop rapidement et n'était plus sur le compte, souvent à l'étranger, utilisé par les fraudeurs.

La BIL suit chaque cas de près. Des procédures judiciaires et bancaires sont en cours. Comme elles impliquent plusieurs juridictions et institutions financières, ces procédures sont longues et complexes, et ne garantissent pas la récupération des fonds.

« Nous comprenons que cette incertitude est difficile à vivre pour les victimes. C'est pourquoi nous mettons tout en œuvre pour y apporter un suivi rigoureux. Nous travaillons étroitement avec les autorités et la place financière luxembourgeoise », a ajouté Nicolas Remarck, Responsable de la Cybersécurité.

Dépôt de plainte auprès du Parquet

La BIL, qui est aussi une victime dans cette affaire, a décidé de porter plainte auprès du Parquet du Tribunal d'Arrondissement de Luxembourg, tout en se réservant le droit de se constituer partie civile. Il appartient désormais à la justice de mener son enquête. Nous avons également déposé des réclamations auprès des établissements bancaires étrangers vers lesquels l'argent a été frauduleusement transféré et auprès du site de recherche qui a été la porte d'entrée de cette attaque.

Notre engagement

Consciente de l'impact financier et psychologique de ces fraudes sur les victimes, la BIL a lancé une revue de son processus de gestion des dossiers de fraude afin de :

- Réduire le délai de réponse pour les victimes.
- Améliorer la communication et le suivi personnalisé avec les clients.
- Rendre les démarches plus claires et plus simples pour les clients.

Pour répondre à des scénarios de fraude en ligne en constante évolution, la BIL s'engage également à continuer :

- L'amélioration son accompagnement client.
- La sensibilisation régulière du public aux différents scénarios de fraude.
- Ses investissements dans la cybersécurité.

La lutte contre la fraude est collective : elle implique les banques, les autorités judiciaires et policières. Elle nécessite aussi la vigilance de chacun. Protéger nos clients contre les fraudeurs reste notre priorité absolue.

Annexe-Comment fonctionne la fraude et comment s'en protéger

Au cours des derniers mois, de nombreuses tentatives de fraude ont visé des résidents et des entreprises au Luxembourg. Comme d'autres banques, la BIL a constaté que les fraudeurs utilisent des techniques de plus en plus sophistiquées pour tromper les clients : faux sites internet imitant ceux des banques, fausses factures, liens sponsorisés sur les moteurs de recherche, SMS, appels de faux conseillers… L'objectif de ces groupes malveillants : tromper les clients pour obtenir leurs données personnelles ou codes d'accès à la banque en ligne, accéder à leur compte bancaire et effectuer des virements.

Chaque cas de fraude est spécifique. S'il nous est impossible de tous les détailler, nous pouvons tenter d'expliquer la complexité des scénarios mis en place. Prenons l'exemple d'une campagne de malvertising, c'est-à-dire une campagne de publicité en ligne mise en place pour attirer les clients vers un faux site bancaire.

Les étapes d'une campagne de malvertising

1. **Phase préparatoire**

Pour tenter d'obtenir les identifiants des clients, les fraudeurs développent et activent un faux site internet, copiant la page de connexion dans les moindres détails. L'URL utilisée contient tout ou partie du nom de l'entreprise ciblée.

Remarque : il est impossible pour une entreprise d'acquérir tous les noms de domaine contenant son nom. Un changement de lettre ou de signe de ponctuation est généralement utilisé, mais les combinaisons sont infinies.
Pour attirer les clients vers ce site, les fraudeurs mettent en place un lien sponsorisé sur les moteurs de recherche afin d'être affichés en tête des résultats de recherche, augmentant ainsi leur visibilité et attirant des utilisateurs non méfiants vers un site frauduleux.

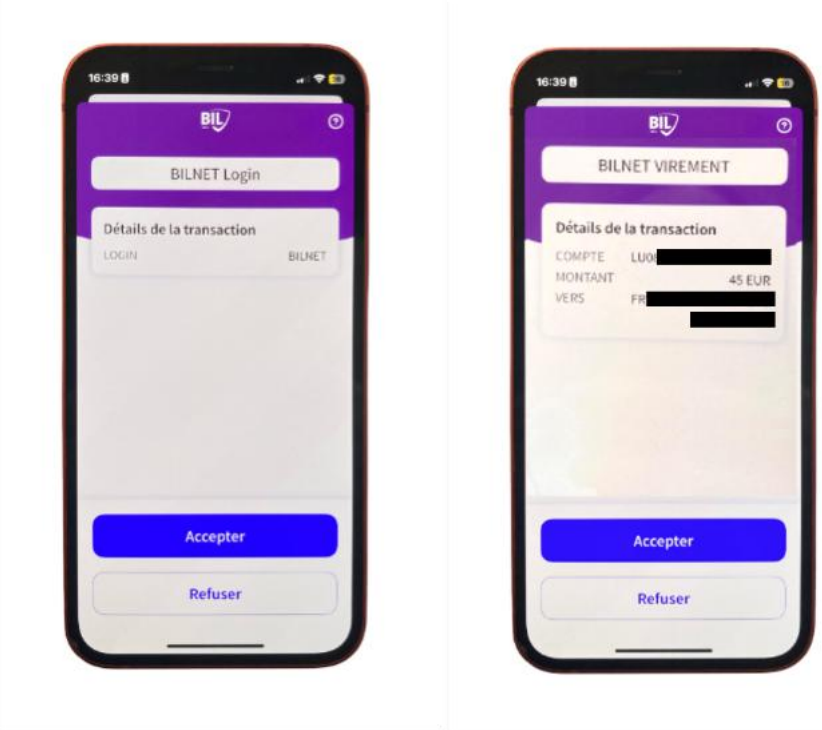
2. **Matérialisation de la fraude**

Le lien sponsorisé est publié. Sur son ordinateur ou sa tablette, le client utilise un navigateur web et un moteur de recherche pour trouver le site de la Banque. Il clique sur le lien sponsorisé placé en haut des résultats et arrive sur le faux site.

Il saisit ses identifiants sur le faux site, qui sont collectés en temps réel par les fraudeurs. Simultanément, les fraudeurs utilisent ces identifiants et le mot de passe pour se connecter au compte du client sur le vrai site de la Banque.

Le client, toujours sur le faux site, valide la connexion des fraudeurs avec l'application LuxTrust Mobile, pensant valider sa propre connexion. Le fraudeur, désormais connecté au compte du

client, crée un nouveau bénéficiaire pour effectuer un virement. Il prépare le virement, qui doit être validé avec LuxTrust Mobile.
Pendant ce temps, le client est toujours sur le faux site. Un message lui indique qu'en raison d'un problème technique, il doit valider à nouveau sa connexion. L'application LuxTrust Mobile présente un nouveau message au client. Cette fois, le message affiche l'IBAN du compte bénéficiaire et le montant de la transaction. Le client ne lit pas ce message et valide le virement.



Une validation LuxTrust équivaut à une signature manuscrite. Si les avancées technologiques permettent de remplacer la saisie d'un code (comme c'était le cas avec le Token physique) par la reconnaissance faciale ou l'empreinte digitale, il s'agit toujours d'une validation ayant une valeur légale.
Il est donc extrêmement important d'être vigilant lorsque vous validez une action sur LuxTrust et de lire attentivement les détails de cette action. Si l'information vous paraît suspecte, annulez l'opération et en cas de doute, contactez immédiatement la Banque ou Worldline.

Découverte de la fraude et mise en place des mesures de protection
Les clients, réalisant qu'ils viennent d'être victimes d'une fraude, appellent la BIL au 45 90 5000 pendant les heures d'ouverture ou le service Worldline au 49 10 10 le soir et le week-end. Ce numéro est un service partagé par les banques luxembourgeoises.

Après analyse de la situation et du scénario, la Banque et Worldline mettent en place des mesures de protection supplémentaires : blocage du compte, désactivation du certificat

LuxTrust, blocage des virements vers les comptes bénéficiaires utilisés par les fraudeurs, signalement du lien sponsorisé au moteur de recherche et du site frauduleux à l'hébergeur, et rappel des fonds.

Procédure de rappel des fonds

Lorsque les virements ont pu être stoppés directement, la transaction est annulée et n'impacte pas le client. Si la transaction a été effectuée, la Banque suit la procédure de rappel des fonds, qui est rapidement et automatiquement mise en œuvre. L'établissement du bénéficiaire peut prendre jusqu'à 4 semaines pour répondre. Si ces tentatives aboutissent, les fonds sont restitués aux clients.

Comment se protéger

Rappelons quelques bonnes pratiques pour prévenir la fraude :

- Utilisez l'application mobile de la BIL.
- Si vous utilisez un navigateur web sur votre ordinateur ou tablette, n'utilisez pas de moteur de recherche. Saisissez vous-même l'adresse complète du site de la banque, www.bil.com, et enregistrez-la dans vos favoris.
- Vérifiez toujours le message de votre application LuxTrust pour confirmer votre connexion ou valider une opération. Cela équivaut à votre signature.
- Ne communiquez jamais vos identifiants bancaires à une personne que vous ne connaissez pas. Votre banque ne vous les demandera jamais, ni par email, ni par SMS, ni par téléphone.
- En cas de doute, appelez la BIL au 45 90 5000 pendant les heures d'ouverture ou Worldline au 49 10 10 le soir et le week-end.

Nous encourageons également les clients à signaler activement toute tentative de fraude (comme des emails de phishing, des faux sites internet ou des messages suspects) directement à la Banque, afin que nous puissions agir rapidement pour protéger tout le monde.

À propos de la Banque Internationale à Luxembourg (BIL)
Fondée en 1856, la Banque Internationale à Luxembourg (BIL) est la plus ancienne banque universelle du Grand-Duché. Depuis sa création, elle joue un rôle actif dans les principales phases du développement de l'économie luxembourgeoise. Elle exerce aujourd'hui les métiers de banque de détail, banque privée et banque des entreprises et participe aux marchés de capitaux. Avec plus de 1900 collaborateurs, la Banque est présente au Luxembourg, en Suisse, en France et en Chine.
www.bil.com

Pour plus d'informations, veuillez contacter :

Banque Internationale à Luxembourg SA
69, route d'Esch • L-2953 Luxembourg
E-mail : mediarelations_BIL@bil.com