Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

Communiqué de presse

Luxembourg, le 10 décembre 2024

Lutte contre les fraudes financières en ligne : bons réflexes et outils à disposition

Face à la multiplication et la sophistication des tentatives de fraudes financières en ligne, l'Association des Banques et Banquiers Luxembourg (ABBL) et ses membres continuent leur travail de sensibilisation en rappelant l'existence d'un certain nombre d'outils et de services, ainsi que des bons réflexes à adopter.

Fraudes financières en ligne : un défi de taille

Une voix synthétique, imitant à la perfection les vraies voix, permet à des criminels de dérober des centaines de milliers d'euros, des appels affichant frauduleusement le numéro de téléphone de votre banque, alors que des escrocs se trouvent à l'autre bout de la ligne, des copies presque parfaites de sites Internet, de faux *chatbots*, ou encore des mails d'escrocs qui s'insèrent dans la suite d'échanges de mails que vous avez eus avec des personnes de confiance … les scénarios utilisés par les criminels financiers deviennent de plus en plus inventifs et sophistiqués. L'utilisation de l'intelligence artificielle a rendu courantes des pratiques telles que l'usurpation d'identité (*deepfakes*) S'il est difficile de chiffrer l'ampleur du phénomène, on peut néanmoins relever que, selon le Ministère de l'Intérieur, le nombre de cas de phishing (fraudes par messages trompeurs pour voler des données personnelles) signalés à la Police aurait explosé entre 2020 et 2023, passant de 28 affaires il y a trois ans à 1.310 l'an dernier.

Quelques rappels utiles

En cette période de fin d'année, une période au cours de laquelle les tentatives de fraudes sont en recrudescence, l'ABBL et ses membres rappellent ainsi quelques consignes de sécurité :

Mode de fonctionnement des escrocs :

La majorité des scénarios de fraude et d'escroquerie en ligne visent à vous amener à communiquer vos données personnelles ou bancaires ainsi que vos identifiants. Nous vous rappelons que jamais un établissement financier (ni aucune institution ou organisme public) ne vous demandera par mail, par SMS ou via un appel téléphonique de communiquer vos identifiants ou de vous connecter à votre online-banking en utilisant un lien envoyé par mail ou sms.

Un réflexe prioritaire : contactez le *helpdesk* de votre établissement financier, la hotline de Worldline 491010 ou celle de LuxTrust 24 550 550

En cas de question ou de doute sur une tentative de fraude, veuillez contacter le helpdesk de l'établissement financier auprès duquel vous êtes client pour bloquer votre carte bancaire et/ou suspendre/révoquer votre certificat LuxTrust.

En dehors de ses heures d'ouvertures, si vous avez ou pensez avoir été victime d'une fraude et si vous êtes client d'un des établissements financiers suivants : Banque de Luxembourg, Banque Internationale à Luxembourg (BIL), Banque Raiffeisen, BGL BNP Paribas, POST Luxembourg ou Spuerkeess vous pouvez contacter immédiatement Worldline Financial Services au +352 49 10 10 (service assuré 24h/24 ; 7j/7). Une procédure spécifique a été mise en place permettant de :

- clarifier avec vous les circonstances de la fraude ;
- bloquer vos cartes bancaires ;
- être mis en relation avec LuxTrust pour suspendre ou révoquer vos certificats ;
- informer l'établissement financier auprès duquel vous êtes client de l'incident.

Le Service Client de LuxTrust vous offre également du support pour suspendre ou révoquer votre certificat LuxTrust :

- par téléphone au +352 24 550 550, via une ligne anti-phishing dédiée. Le service est disponible 24/7.
- en personne, dans ses locaux à Capellen (IVY Building, 13-15 Parc d'activités, L-8308 Capellen, Luxembourg) du lundi au vendredi, du 8h à 18h.
- sur le site LuxTrust - www.luxtrust.com, dans l'espace My LuxTrust sur Suspendre temporairement mon certificat ou Révoquer définitivement mon certificat.

Rappel de quelques bonnes pratiques :

Faites preuve de discernement et demandez conseil

- Prenez le temps d'analyser l'e-mail ou l'SMS qui vous a été envoyé.
- Ne cliquez jamais sur un lien ou une pièce jointe reçue par SMS, e-mail ou d'autres canaux qui vous semblent suspects.
- Lisez attentivement les informations demandées à chaque étape d'autorisation d'une opération et prenez le temps de vérifier tous les détails pour assurer le bon déroulement de votre opération.
- Consultez des personnes de confiance pour obtenir un avis extérieur.
- Rappelez-vous que les employés d'aucun établissement financier se rendent au domicile des clients pour récupérer des cartes de paiement ou leurs codes secrets.
- Ils n'appellent pas non plus leurs clients en les mettant sous pression, ni en leur demandant d'ouvrir un e-mail prétendument envoyé par un établissement financier, de cliquer sur un lien ou de suivre des instructions pour bloquer une opération frauduleuse.

Faites des recherches complémentaires

- Recherchez des informations supplémentaires pour confirmer la légitimité des démarches qu'on vous demande d'effectuer via le mail ou le SMS que vous avez reçu.
- Effectuez une recherche sur Internet avec les mots clés annoncés par le fraudeur suivi du mot « arnaque ».

Protégez vos données

- Traitez vos données personnelles et bancaires comme vous le faites avec vos papiers d'identité ou vos clés. En les protégeant, vous vous protégez.
- Gardez vos identifiants strictement confidentiels, qu'il s'agisse de vos moyens de paiement ou de la connexion à vos comptes à distance. Ne communiquez jamais vos identifiants LuxTrust. Pas même à votre conseiller bancaire !

- Ne conservez pas vos identifiants sur des supports non sécurisés, qu'ils soient physiques « papier » ou informatiques de type messagerie électronique, disque dur, téléphone portable ; utilisez un gestionnaire de mot de passe sécurisé.
- Pensez à contrôler régulièrement votre liste de bénéficiaires enregistrés dans votre application bancaire.

Ecoutez les conseils de l'établissement financier auprès duquel vous êtes client et aidez-la à vous protéger

- Consultez régulièrement la rubrique sécurité du site Internet ou de l'application de votre établissement financier, elle est souvent mise à jour pour tenir compte des types et modalités de fraude récentes et les plus courantes
- Informez votre établissement financier de tout changement de coordonnées (téléphone, adresse de courrier électronique…) via le canal habituel préconisé par ce dernier, pour être joignable rapidement en cas de problème.
- Pensez à mettre régulièrement à jour votre application bancaire pour profiter des mises à jour de sécurité.

Passez à l'application LuxTrust Mobile

Pour répondre aux exigences de sécurité croissantes, **le Token LuxTrust sera désactivé le 31 décembre 2024.** En effet, les évolutions technologiques et les impératifs de sécurité incitent LuxTrust et ses partenaires à revoir régulièrement leurs dispositifs pour mieux vous protéger.

Si vous utilisez le Token comme principal dispositif de connexion, vous pouvez l'associer gratuitement à l'application LuxTrust Mobile et ainsi continuer à accéder aux services en ligne.

L'application LuxTrust Mobile offre une sécurité renforcée par rapport au Token pour plusieurs raisons :

1. Affichage des détails des transactions : l'application présente les informations complètes de chaque transaction avant validation, permettant ainsi de vérifier les montants et les destinataires.

2. Authentification biométrique : l'application LuxTrust Mobile utilise des méthodes d'authentification avancées telles que le code PIN, l'empreinte digitale (Touch ID) ou la reconnaissance faciale (Face ID), offrant une couche de sécurité supplémentaire.

Près de 90% des utilisateurs du Token sont déjà passés à l'application a LuxTrust Mobile. Sautez le pas également et n'attendez pas le dernier moment pour renforcer la protection de vos transactions en ligne !

Pour savoir comment procéder : https://www.luxtrust.com/fr/desactivation-du-token.

Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

6 techniques courantes d'escroquerie à connaître pour mieux les déjouer :

- Phishing (par e-mail) : Un e-mail frauduleux imite une institution officielle (administration fiscale, la police, la caisse maladie) ou votre établissement financier ou assurance ou LuxTrust pour vous inciter à cliquer sur un lien ou partager vos identifiants.
- Smishing (par SMS) : Un SMS alarmant ou urgent contient un lien ou un numéro à appeler pour vérifier ou confirmer vos données personnelles ou bancaires.
- Vishing (par téléphone) : Un escroc se fait passer pour un employé d'un établissement financier ou de LuxTrust ou une autorité pour obtenir vos informations sensibles ou vous manipuler en vue d'effectuer des transactions frauduleuses.
- Spoofing : Les escrocs usurpent un numéro de téléphone ou une adresse e-mail officielle pour masquer leur identité réelle et gagner votre confiance.
- Quishing : Une nouvelle forme de phishing utilisant des codes QR frauduleux pour vous rediriger vers des sites malveillants ou voler vos informations.
- Deepfake : Les escrocs utilisent des vidéos ou des enregistrements audio manipulés pour imiter une personne de confiance et vous inciter à réaliser une action frauduleuse, comme transférer de l'argent ou partager des données sensibles.

Quelques liens utiles :

- Sécher am Internet https://learn-ebanking.fondation-abbl.lu/fr/accueil/ : site développé par la Fondation ABBL pour l'Education financière pour vous permettre de mieux appréhender le monde de la banque en ligne.
- Letzfin.lu https://www.letzfin.lu : site d'éducation financière développé par la Commission de Surveillance du Secteur Financier (CSSF) avec le soutien de la Fondation ABBL pour l'Education financière.
- BeeSecure https://www.bee-secure.lu/fr/ : initiative gouvernementale opérée par le Service national de la jeunesse (SNJ) et le Kanner-Jugendtelefon (KJT), en partenariat avec Luxembourg House of Cybersecurity, la Police Lëtzebuerg ainsi que le Parquet général du Grand-Duché de Luxembourg visant à sensibiliser le grand public à une utilisation plus sûre et responsable des technologies numériques.

A propos de l'ABBL

La mission de l'ABBL est de promouvoir le développement durable de services bancaires réglementés, innovants et responsables. L'ABBL est la plus grande et la plus ancienne association professionnelle du secteur financier. Elle représente le secteur bancaire au sens large, à savoir la majorité des banques établies au Luxembourg, ainsi que les intermédiaires financiers réglementés et autres du secteur y compris les cabinets d'avocats, les cabinets de conseil, les auditeurs, les infrastructures de marché, la monnaie électronique et les établissements de paiement.

L'ABBL fournit à ses membres les informations, les ressources et les services dont ils ont besoin pour opérer sur un marché financier dynamique et dans un environnement réglementaire de plus en plus complexe. Elle est une plateforme ouverte pour discuter des problématiques clés de l'industrie et pour définir des positions communes à l'ensemble du secteur.

Contact presse : Paul Wilwertz, +352 46 36 60-322, paul.wilwertz@abbl.lu