



Réponse conjointe du Ministre des Affaires intérieures, Léon Gloden et de la Ministre de la Justice, Elisabeth Margue, à la question parlementaire N° 3691 du 24 février 2026 de l'honorable Député Yves Cruchten et de l'honorable Député Mars Di Bartolomeo au sujet de l'évolution et la lutte contre le phishing, les appels frauduleux et l'usurpation de numéros au Luxembourg.

Il est rappelé que la Police grand-ducale publie chaque année les chiffres de la délinquance, qui seront présentés cette année le 23 avril 2026 à la Chambre des Députés et à la presse.

L'observatoire de la cybersécurité du Luxembourg National Cybersecurity Competence Centre « NC3 », publie d'ailleurs régulièrement des statistiques par rapport aux menaces, dont le phishing, sur son site internet (<https://observatory.nc3.lu/>).

1) Quelle a été l'évolution, entre 2023 et 2025, du nombre d'affaires enregistrées au Luxembourg en matière de phishing, de plaintes relatives à des « ping calls » ou autres appels frauduleux, ainsi que de cas d'usurpation de numéros luxembourgeois (« spoofing ») ?

Les cyberattaques et la cybercriminalité augmentent en nombre et en sophistication depuis quelques années au Luxembourg ainsi que dans toute l'Europe, avec une tendance qui devrait encore d'avantage s'accroître à l'avenir.

Le nombre de plaintes en matière de phishing déposées auprès de la Police a augmenté au Luxembourg pendant la période demandée.

Entre août et décembre 2023 : 114 plaintes

En 2024 : 247 plaintes

En 2025 : 367 plaintes

Le nombre de cas d'usurpation de numéros luxembourgeois, dit Spoofing, a connu une évolution vers le bas en 2025, grâce à des mesures préventives prises par les opérateurs téléphoniques.

En 2023 : 55 cas

En 2024 : 98 cas

En 2025 : 32 cas

Le phénomène des ping calls est connu par la Police, mais il n'y a pas eu de plaintes en la matière pour la période demandée. Il s'agit d'une arnaque téléphonique consistant à faire sonner brièvement le téléphone avec un numéro inconnu, souvent surtaxé ou étranger, afin d'inciter les destinataires à rappeler.



2) Le Gouvernement dispose-t-il de statistiques concernant le recours par les victimes aux plateformes de signalement, notamment BeeSecure, et ces données sont-elles centralisées et exploitées de manière coordonnée avec celles de la Police grand-ducale ?

Le Gouvernement ne centralise pas tous les recours par les victimes aux plateformes de signalement.

BEE SECURE transmet les contenus potentiellement illégaux signalés à la Stopleveline à la Police ou à d'autres autorités compétentes. La Stopleveline de BEE SECURE permet de signaler anonymement trois catégories de contenus :

- les abus sexuels sur mineurs (CSAM) ;
- la discrimination, le racisme, le révisionnisme et le discours de haine ; et
- le terrorisme.

3) Combien d'enquêtes relatives à ces phénomènes ont abouti à l'identification des auteurs, à l'engagement de poursuites judiciaires, à des condamnations et, le cas échéant, à une indemnisation des victimes ?

A l'heure actuelle, le service de police judiciaire mène 88 enquêtes relatives à ces phénomènes. Les identités de 117 auteurs présumés ont pu être confirmées et 45 personnes ont été arrêtées.

Concernant les statistiques des autorités judiciaires, il convient d'abord de relever que celles-ci sont établies sur la base des qualifications pénales des infractions en cause. Les faits délictueux visés par la question parlementaire tombent ainsi sous différentes qualifications pénales (p.ex. escroquerie, blanchiment etc.), sachant que le « phishing », le « spoofing » ou les « ping calls » ne constituent pas des qualifications prévues en tant que telles par le Code pénal. Vu que les qualifications en cause, comme p.ex. l'escroquerie, concernent également d'autres fraudes, étrangères aux modes opératoires visés par la question parlementaire, on ne peut pas fournir des statistiques précises et exactes sur les affaires de phishing, ping calls ou spoofing.

En prenant en considération les qualifications pénales des infractions en cause, on peut affirmer que, depuis l'année dernière, environ 26 enquêtes préliminaires sont en cours auprès des parquets, 80 dossiers ont été confiés à des juges d'instruction, à Luxembourg et à Diekirch. Il convient toutefois de préciser qu'un seul dossier peut regrouper plusieurs victimes, ce qui explique l'écart entre le nombre de plaintes et celui des enquêtes.

Depuis l'année 2023, plusieurs affaires de ce type ont donné lieu à des condamnations pénales par les chambres correctionnelles du Tribunal d'arrondissement de Luxembourg. Des peines d'emprisonnement, des amendes et des confiscations ont été prononcées. Des parties civiles se sont vu allouer des dommages-intérêts.

4) Combien de personnes sont actuellement affectées, au sein de la Police grand-ducale, des parquets et des unités spécialisées en cybersécurité ou en fraude numérique, au traitement de ces dossiers ?



- 5) **Des moyens humains ou techniques supplémentaires ont-ils été alloués depuis 2023 afin de faire face à l'augmentation du phénomène et, dans l'affirmative, lesquels ?**
- 6) **Le Gouvernement estime-t-il que les moyens actuellement déployés sont suffisants au regard de l'ampleur et de la complexité croissantes de ces infractions ?**

Comme expliqué dans la réponse à la question parlementaire n° 99 du 16 janvier 2024, chaque policier au sein de la Police grand-ducale peut prendre en charge des plaintes dans le cadre d'une affaire de phishing. Le traitement des dossiers est effectué, parmi d'autres, par les sections Criminalité Générale, Anti-Blanchiment et Cybercrime du Service de police judiciaire. Ces sections regroupent environ 90 enquêteurs et analystes. Le recrutement de la Police se poursuit.

Au courant de l'année 2025, une taskforce au sein de la Police a été créée pour lutter de manière plus ciblée contre le phénomène croissant du phishing. Celle-ci associe une quinzaine d'enquêteurs et d'experts du Service de police judiciaire qui, en cas de besoin, sont appuyés par d'autres services.

Dans le domaine des escroqueries, la prévention joue un rôle primordial. Par un effort constant et coordonné, la Police sensibilise au maximum les acteurs clés (banques, providers) et le grand public pour éviter de nouveaux faits et/ou en réduire les effets. Des conseils de prévention sont régulièrement diffusés via différents canaux (presse écrite, réseaux sociaux, bulletins communaux, campagnes de sensibilisation...) par la Police. Les efforts sont constamment adaptés pour atteindre les différents groupes d'âge.

Le ministre des Affaires intérieures a visité le 18 mars 2026 un projet innovant avec le « Maacher Lycée », qui implique la création de courtes vidéos de sensibilisation par les élèves, en vue de les diffuser sur les réseaux sociaux.

Afin de sensibiliser le public aux risques liés à la cybercriminalité, la Police a répertorié l'ensemble des escroqueries en ligne actuellement connues, ainsi que des conseils y associés, sur son site Internet, sous la rubrique « Prévention »¹.

Il est difficile de déterminer avec précision le nombre exact de magistrats qui, à un moment donné, sont amenés à traiter spécifiquement des dossiers liés au phishing. En effet, la répartition des dossiers varie en fonction de la charge de travail, de la complexité des affaires et des nécessités du service. Lorsqu'une telle infraction est portée à la connaissance des autorités judiciaires, le magistrat de permanence prend, le cas échéant, les mesures urgentes qui s'imposent afin de préserver les éléments de preuve et d'assurer le suivi adéquat du dossier.

Le traitement de ces affaires relève, en règle générale, du département de la criminalité économique et financière du Parquet. Ce département dispose d'une expertise particulière dans l'analyse des mécanismes financiers et des phénomènes criminels liés aux infractions économiques et financières. Il constitue l'un des trois piliers organisationnels du Parquet et joue un rôle central dans la poursuite de ce type d'infractions.

¹ <https://police.public.lu/fr/prevention/arnaques.html>



Actuellement, près de 40 % des effectifs du Parquet de Luxembourg sont affectés au département économique et financier.

Le Gouvernement a la ferme volonté de renforcer massivement les effectifs de la justice et de leur accorder des moyens supplémentaires. Ainsi, le programme pluriannuel de recrutement, adopté en 2024, a prévu la création de 94 nouveaux postes de magistrats de l'ordre judiciaire entre 2024/2025 et 2026/2027. Dans ce contexte, les Parquets, les cabinets d'instruction ainsi que la Cellule de renseignement financier (CRF) reçoivent un renforcement substantiel, traduisant la volonté de renforcer les capacités des autorités judiciaires, notamment dans les domaines spécialisés tels que la criminalité économique et financière.

Au fil des dernières années, les méthodologies de travail ont également été affinées afin de permettre un traitement efficace des dossiers, qu'il s'agisse de l'orientation procédurale ou de la poursuite des auteurs. Les autorités compétentes collaborent régulièrement et unissent leurs efforts. La Police grand-ducale, ainsi que BEE SECURE, lancent régulièrement des campagnes de sensibilisation sur le sujet du phishing.

7) Le Gouvernement dispose-t-il désormais d'une estimation des dommages financiers subis par les victimes au Luxembourg, notamment en ce qui concerne les appels surtaxés déclenchés par des « ping calls » ainsi que par d'autres formes de fraudes téléphoniques, telles que l'usurpation de numéros (« spoofing ») ou les appels frauduleux internationaux ?

La Police ne dispose pas de données pour évaluer le préjudice causé par les fraudes de type ping calls ou spoofing.

Quant au phénomène du phishing, la Police peut désormais estimer le préjudice à un montant de +/- 10.000.000 EURO depuis août 2023. Le préjudice réel risque néanmoins d'être plus élevé.

Luxembourg, le 15 avril 2026
Le Ministre des Affaires intérieures,
(s.) Léon Gloden