Appel à candidatures pour le projet Stop phishing par SMS

dans le cadre du

Plan national pour la reprise et la résilience
Axe 2 Transformation numérique

Composante 2.1. Cybersécurité

Personne de contact : **Streel Yves** Senior Project Manager

(yves.streel@ccb.belgium.be)

TABLE DES MATIÈRES

Table des matières

1. Contexte

La cybercriminalité est le délit économique le plus courant en Belgique. Que ce soit par l'utilisation de menaces d'hameçonnage (phishing), de logiciels malveillants ou encore par l'intermédiaire de scannage de réseaux. Près de deux-tiers des organisations belges ont été victimes de criminalité économique au cours des deux dernières années. Les défis de la cybersécurité sont multiples et complémentaires. Il faut faire preuve de vigilance et mettre en œuvre des outils et services de protection. Enfin et surtout, il est indispensable de protéger nos données et en garantir la souveraineté nationale. L'hameçonnage est une menace majeure pour la société numérique et un réel frein à la confiance dans l'économie numérique. C'est en effet le moyen le plus utilisé par les cybercriminels afin de tromper une victime. L'hameçonnage a souvent de graves conséquences pour les victimes, comme la perte de données privées, l'accès aux comptes de la victime, l'infection par un logiciel de rançon, la fraude financière, le vol d'identité, l'intrusion dans un système informatique d'une entreprise, d'un hôpital, d'une université, ou le vol de propriété intellectuelle.

L'hameçonnage est un fléau qui ne cesse de croître en Europe et en Belgique. Le 7 janvier 2021, le Centre pour la Cybersécurité Belgique annonçait que « plus de 3,2 millions d'internautes belges ont signalé des fraudes d'hameçonnage à suspicious@safeonweb.be (contre 1,9 million en 2019). Cela a permis d'identifier 667 356 liens vers des sites Internet frauduleux. »

Dans le rapport IOCTA 2020, Europol déclare que « l'ingénierie sociale (hameçonnage) continue de représenter une menace majeure pour faciliter d'autres formes de cybercriminalité. L'ingénierie sociale et l'hameçonnage, qui sont axés sur la faiblesse humaine dans la chaîne de sécurité, ont un impact majeur sur la société et conduisent à la plupart des cybercrimes, allant de la fraude et de l'extorsion à l'acquisition d'informations sensibles et l'exécution d'attaques avancées sur les logiciels malveillants ».

Dans son rapport intitulé « Cyber threat landscape 2020 », l'ENISA, l'Agence de l'Union européenne pour la cybersécurité, confirmait que l'hameçonnage est la troisième plus grande menace et indiquait que « il y aura une nouvelle norme pendant et après la pandémie de COVID-19, qui reposera davantage sur un cyberespace sûr et fiable. Le nombre de victimes d'hameçonnage dans l'UE continue d'augmenter, des acteurs malveillants utilisant le thème de la COVID-19 pour les attirer. Le Business Email Compromise (BEC) et les attaques sur le thème de la COVID-19 sont utilisés par les cyber-escrocs qui entraînent des pertes de millions d'euros pour les citoyens et les entreprises de l'UE. Les petites et moyennes entreprises (PME) européennes ont également été victimes de ces menaces à un moment où beaucoup d'entre elles connaissent de graves difficultés financières en raison de la perte de revenus. »

Défis : Détecter et bloquer les messages d'hameçonnage envoyés par SMS avant qu'ils ne soient délivrés à leurs victimes. Le but étant d'améliorer la résilience nationale à l'hameçonnage (phishing) et à la fraude sur les réseaux de télécommunications afin de protéger nos citoyens, nos entreprises et les acteurs publics.

2. Objet et nature de l'accord de partenariat

Le projet Stop Phishing vise à détecter et à bloquer les tentatives d'hameçonnage et de fraude sur les réseaux de télécommunications grâce à l'introduction de plateformes anti-hameçonnage et antifraude avec les opérateurs de télécommunications belges, en étroite collaboration avec le Centre pour la Cybersécurité Belgique et le régulateur belge des télécommunications (IBPT).

Le projet Stop Phishing est divisé en quatre parties différentes. Seul le premier, à savoir la composante anti-phishing pour les SMS (smishing), est abordée dans cet appel. Les trois autres parties, à savoir la partie anti-hameçonnage pour les emails, la plate-forme anti-fraude pour les appels téléphoniques générés par des machines et pour détecter les messages de signalisation frauduleux dans les réseaux mobiles seront abordées plus tard.

Ce projet contribue grandement à la transition numérique en augmentant la confiance dans l'économie numérique. Cette confiance accélère la transition numérique : les citoyens utilisent les services publics numériques et le commerce électronique en toute confiance ; les PME développent

leur transition numérique et sont mieux protégées contre les menaces de blocage par des logiciels malveillants ; les services publics et les administrations fournissent des services en ligne plus sûrs ; les universités et les secteurs de la recherche protègent leur propriété intellectuelle et les secteurs clés sont mieux protégés contre les acteurs de la menace.

Le cadre légal afin de permettre aux opérateurs de télécommunications de détecter et de bloquer les messages SMS et MMS frauduleux a été modifié et publié au Moniteur en date du 31 décembre 2021.

Sous le contrôle du Comité de pilotage, le Centre pour la Cybersécurité Belgique (CCB) et l'IBPT coordonnent les actions avec les opérateurs de télécommunications. La gestion administrative et le suivi de ce projet sera assurée par le CCB pour le compte de la Ministre des Télécommunications.

Public-cible :

Les bénéficiaires de ce projet sont l'ensemble de la population belge, les secteurs publics et les entreprises, y compris les petites entreprises et les indépendants.

Période de mise en œuvre du projet

Le projet débutera dès janvier 2022 et sera finalisé mi-2023 (au plus tard).

3. Exigences

3.1. Critères d'accès

Qui peux participer à ce projet ?

Chaque opérateur désireux de participer au projet Stop Phishing par SMS devra :

- Être actif en tant qu'opérateur mobile sur le marché belge et notifié auprès de l'IBPT conformément à l'art. 9 de la LCE ;
- Posséder au moins 1 SMS-C opérationel afin de délivrer le trafic SMS aux utilisateurs mobiles belges ;
- Proposer le service SMS et MMS (optionel) sur le marché intérieur ;
- Fournir une description des plateformes actuelles (équipement et interconnexion) ainsi que des outils anti-fraude existants (par exemple : pare-feu) ;
- Être désireux d'investir dans une plateforme de détection de messages SMS et MMS (optionel) frauduleux ;
- Exigences légales : Dans sa demande, le demandeur doit démontrer qu'il respecte l'ensemble de la législation applicable, notamment en matière de protection de la vie privée, en particulier l'article 1251 de la loi relative aux communications électroniques « LCE » en abrégé. Le demandeur doit soumettre une proposition réaliste de collecte de données statistiques pour mesurer l'efficacité de la solution.

[1] « 7° lorsque les actes sont accomplis par les opérateurs dans le but exclusif de combattre la fraude commise au moyen de messages utilisant des numéros de téléphone, comme des messages SMS ou MMS, et aux conditions suivantes :

a) les actes restent limités à l'examen mécanique des messages afin d'établir la fraude ; l'intervention humaine est autorisée exclusivement pour vérifier le bon fonctionnement des algorithmes informatiques ;

b) les opérateurs sont transparents vis-à-vis des utilisateurs finaux, afin qu'il soit clair pour eux que les messages sont susceptibles d'être examinés mécaniquement dans le cadre de la lutte contre la fraude ;

c) les données concernées ne peuvent être traitées que par des personnes chargées par l'opérateur de lutter contre la fraude ;

d) le traitement des données concernées est limité aux actes et à la durée nécessaires pour lutter contre la fraude ou jusqu'à la fin de la période durant laquelle une action en justice est possible.

3.2. Exigences techniques et opérationnelles

Le candidat au partenariat doit démontrer dans son dossier de candidature que la solution proposée permet de déterminer avec un très haut degré de fiabilité un score final qui est une indication fiable de la probabilité qu'un message soit frauduleux.

L'algorithme de détection des messages frauduleux doit être composé de trois éléments, chaque élément se voyant attribuer un score avec une pondération spécifique pour obtenir un score final.

Ces éléments sont les suivants :

A. Analyse du contenu des SMS

Le demandeur doit préciser les méthodes utilisées pour identifier le contenu des logiciels malveillants et les mots-clés dans le message texte. Outre le texte, il convient également d'identifier la présence de raccourcis URL, d'adresses e-mail, de numéros de téléphone, etc.

B. Analyse de l'URL

Le demandeur doit préciser les méthodes utilisées pour analyser les URL et les noms de domaine associés menant à des pages web frauduleuses, si celles-ci sont incluses dans le message. Au minimum, une analyse de fiabilité doit être effectuée sur la base, entre autres, du nom de domaine de premier niveau utilisé, de l'ancienneté du nom de domaine et de l'apparition du nom de domaine sur des listes d'anti-hameçonnage. Il faut également vérifier si un fichier malveillant est téléchargé lors de l'appel de l'URL. Pour ce faire, la plateforme utilise notamment des listes de réputation d'URL (URL reputation lists).

C. L'analyse des métadonnées

Le demandeur devra clarifier les méthodes utilisées pour l'analyse des métadonnées (numéro de téléphone, nombre de messages, etc.), qui sont des indicateurs de messages frauduleux.

Cette analyse et la détermination du score final doivent également répondre aux exigences suivantes de la plateforme :

1) la plateforme fonctionnera en temps réel (**Real Time**) ;

2) la plateforme fonctionnera en mode de détection automatique (**Automatic Detection**), mais certaines interventions manuelles de l'opérateur seront acceptées afin d'améliorer continuellement l'apprentissage automatique, en particulier dans les premières semaines/mois du déploiement de la plateforme ;

3) la plateforme sera capable de traiter des messages dans toutes les langues (**Language Independant**) ;

4) la plateforme devra utiliser l'apprentissage automatique avec l'adaptation des algorithmes (**Machine Learning**) afin d'améliorer les performances grâce à l'expérience acquise.

En outre, il convient d'indiquer comment éviter les résultats faussement positifs.. La possibilité d'établir une « liste blanche » doit être incluse.

Il faut également indiquer comment le personnel autorisé de l'opérateur peut effectuer un réglage manuel sur la base des informations actuelles.

L'opérateur doit définir 4 catégories dans lesquelles les messages doivent être classés. Chacune de ces catégories correspond à une fourchette/plage définie en fonction du score final. Les actions suivantes peuvent être prises en fonction du score final :

« Si l'examen visé à l'alinéa 1er, 7°, a), révèle une fraude, les opérateurs prennent des mesures concrètes pour lutter contre la fraude, comme le blocage des messages ou le remplacement dans les messages des URL renvoyant à un site Internet frauduleux par un message d'avertissement ou une URL avec un message d'avertissement.

Avant le 1er février, les opérateurs fournissent à l'Institut un rapport annuel reprenant au moins les mesures qu'ils ont prises au cours de l'année écoulée pour lutter contre la fraude, leur efficacité ainsi que l'évolution de la fraude. »

Catégorie	Score correspondant (max. 100 - à titre indicatif)	Y a-t-il une fraude ?	Action
A	>80	Certainement	Effacer le message
B	>60 et <80	Très probable	Supprimer l'URL
C	>40 et <60	Probablement	Remplacer l'URL par l'URL d'avertissement
D	> 20 et < 40	Doute	Action à déterminer : par exemple, ajouter un avertissement au message (ne pas supprimer l'URL, le texte ou le numéro de téléphone).

Les opérateurs doivent s'engager à convenir, dans la mesure du possible, d'une norme commune pour effectuer la catégorisation.

L'algorithme utilisé pour déterminer le score final et les actions prises ne doivent pas entraîner de retards significatifs (sauf en cas d'intervention manuelle) dans la distribution des messages SMS (MMS est optionnel)

3.3. Aspects financiers

Le candidat doit démontrer qu'il prendra en charge au moins 50 % des coûts d'achat et d'exploitation de la plateforme pendant les trois premières années. À cette fin, le demandeur doit fournir toutes les informations relatives aux coûts du prestataire de services qu'il a retenu dans le dossier de demande.

3.4. Objectifs – résultats attendus

L'objectif du projet est de réduire de manière significative les messages SMS (MMS optionnel) frauduleux reçus par les utilisateurs mobiles.

Les messages frauduleux doivent être compris comme tous les messages qui ont pour but de nuire au destinataire (par exemple financièrement) de manière déloyale ou illégale, y compris les messages qui ont pour but d'installer (indirectement ou non) des logiciels malveillants.

Les modules proposés par les fournisseurs dans le seul but de détecter les SIM boxes et les routes grises sans que les utilisateurs finaux ne soient victimes de fraude ne peuvent être subventionnés.

L'opérateur devra proposer dans sa réponse un moyen de mesurer les éléments suivants :

- 1) Nombre de SMS bloqués sur une période donnée par rapport au nombre total de SMS sur la même période (en tenant compte du trafic exclu). Les opérateurs devront soumettre ce qu'est le trafic exclu.

- 2) Comme la plateforme qui sera mise en œuvre sera basée sur l'apprentissage automatique supervisé, les analystes de la fraude devront « entraîner » l'algorithme en y introduisant des décisions dans la phase initiale après la mise en œuvre. L'opérateur devra proposer un KPI pour que le délai moyen par campagne de smishing soit automatiquement détecté et traité.

- 3) En termes de plaintes : l'opérateur devra indiquer le « nombre de plaintes pour lesquelles aucune action n'a été entreprise » pour une période donnée. C'est-à-dire des plaintes liées à des campagnes de smishing non identifiées par la plateforme.

- 4) L'opérateur devra fournir des chiffres pour mesurer l'efficacité de la plateforme, car l'analyse manuelle des données sera réduite au minimum. Ces mesures devraient permettre d'espérer une amélioration de la précision et de l'efficacité de l'algorithme au cours des premier(e)s semaines/mois.

- 5) Tout autre chiffre pertinent que la plateforme peut présenter chaque semaine ou chaque mois pour démontrer le succès du lancement de la plateforme.

Tou(te)s les KPI/mesures proposé(e)s seront évalué(e)s (par tous les opérateurs et le Comité de pilotage) pendant la période d'évaluation et serviront de base à la définition de KPI communs obligatoires que les opérateurs devront respecter après une période à convenir.

Le projet produira des résultats mesurables dans chaque phase de mise en œuvre. Nous ne devons donc pas attendre que le projet soit terminé. Le groupe de pilotage du projet procédera à une évaluation régulière.

4. Planning du projet

L'opérateur de télécommunications belge mettra en œuvre la plateforme anti-phishing et anti-fraude « de pointe » au sein de son réseau de télécommunications en suivant une approche par projet, notamment :

(1) en évaluant l'état de l'art et les techniques les plus avancées pour la détection et le blocage des messages SMS frauduleux ;
(2) en évaluant le marché et sélectionnant le fournisseur ;
(3) en implémentant la solution sélectionnée ;
(4) en utilisant cette plateforme et en évaluant les résultats.

Les opérateurs devront partager un plan détaillé de mise en œuvre incluant toutes les phases du projet, le projet devra couvrir les phases suivantes :

- appel à candidats (RFP)

- évaluation des réponses

- sélection d'un ou de deux candidat(s)

- test de la ou des solution(s) retenue(s) (PoC)

- sélection de la solution finale

- définition du design final

- mise en œuvre

- validation en environnement de test (trafic limité)

- évaluation

- mise en production

5. Comité de pilotage

Le Comité de pilotage est composé de :

- **La Ministre des Télécommunications**, représentée par Monsieur Gertjan Boulet ;
- **L'IBPT,** représenté par Monsieur Jan Vannieuwenhuyse ;

- **Le CCB,** représenté par Monsieur Miguel de Bruycker et Madame Phédra Clouner et **le chef de projet** : Yves Streel ;

Le Comité de pilotage se réunit pour valider et évaluer les différentes phases du projet, en tenant compte des jalons établis en concertation avec les opérateurs.

6. Propriétés des résultats

Chaque opérateur devra partager les résultats obtenus grâce à la mise en œuvre de cette nouvelle plateforme dans toutes les phases du projet, ainsi qu'un rapport mensuel à partir du lancement officiel afin d'évaluer le retour sur investissement dans les mois et années à venir.

Les données et les modalités exactes de partage (type d'information, granularité et unité) sera déterminée par le Comité de pilotage et les opérateurs au cours du projet, après sélection de la solution retenue par l'opérateur.

7. Dossier de candidature et engagements

Le candidat doit démontrer dans son dossier de candidature qu'il ou le cas échéant que le fournisseur envisagé répond à tous les critères décrits au chapitre 3.1.

En outre, le candidat doit fournir une description détaillée des systèmes SMS et MMS (optionnel) (à la fois fonctionnels et architecturaux) dont il dispose à la date du 1er avril 2022. Une description complète du pare-feu et des systèmes antifraude existants doit également être fournie.

Le candidat doit décrire comment il répondra, aux critères proposés au chapitre 3.2 (exigences techniques et opérationnelles), au chapitre 3.3 (exigences légales) et au chapitre 3.4 (aspects financiers).

Le candidat doit fournir des éléments supplémentaires qu'il juge importants pour atteindre l'objectif du projet et qui démontrent l'expertise du candidat, le cas échéant du prestataire envisagé (par exemple, des mises en œuvre à l'étranger).

Le candidat doit présenter un plan de projet détaillé dans le but de rendre le système antifraude pleinement opérationnel.

Il est également demandé à l'opérateur de désigner un seul point de contact dans le cadre de ce projet.

Le candidat devra s'engager à fournir de manière hebdomadaire l'état d'avancement de son projet en collaboration avec le chef de projet.

8. Critères d'évaluation

Un opérateur qui ne répond pas à un ou plusieurs critère(s) d'accès (voir chapitre 3.1) ou qui ne respecte pas l'article 125 de la LCE (voir chapitre 3.3) ne peut pas participer au projet.

Pour qu'une candidature soit prise en compte pour évaluation, l'opérateur devra répondre complètement aux exigences et aux engagements (voir chapitre 7).

Une évaluation des candidatures sera effectuée sur la base des réponses fournies, le candidat devant obtenir au moins 60 points sur 100 pour pouvoir bénéficier des subsides selon le schéma suivant :

a. Exigences techniques et opérationnelles : 60 points.
L'évaluation sera faite suivant les règles d'attributions suivantes :

Critères	**Points**
Real-time platform	5
Automatic detection	5

Language independant	5
Machine Learning	5
Possibilité d'intervention manuelle	5
Analyse le contenu des SMS	5
Analyse de L'URL	5
Analyse des Métadonnées	5
Utilisation d'un algorithme de détection de message frauduleux	10
Description détaillée de la matrice de décision	10

b. Aspects financiers : 20 points.
L'évaluation sera faite suivant les règles d'attributions suivantes :

Critères	**Points**
Présentation détaillée de tous les coûts afférents au projet sur 3 ans	20

c. Informations et rapports statistiques : 20 points.
L'évaluation sera faite suivant les règles d'attributions suivantes (explications sur les infos à présenter voir chapitre 3):

Critères	**Points**
Rapport 1 : Nombre de SMS bloqués sur une période donnée par rapport au nombre total de SMS sur la même période (en tenant compte du trafic exclu)	3
Rapport 2 : KPI pour que le délai moyen par campagne de smishing soit automatiquement détecté et traité	3
Rapport 3 : le « nombre de plaintes pour lesquelles aucune action n'a été entreprise » pour une période donnée	3
Rapport 4 : mesure de l'efficacité de la plateforme	6
Rapport 5 : chiffre pertinent que la plateforme peut présenter chaque semaine ou chaque mois pour démontrer le succès du lancement de la plateforme	5

Dans une phase ultérieure, s'il est sélectionné, le candidat négociera avec la ministre en vue de conclure un accord de partenariat. Ce n'est qu'après la conclusion d'un tel accord que le candidat pourra bénéficier de subsides (voir chapitre suivant).

9. Mécanisme d'attribution des subsides

Dans le cadre de son budget, le gouvernement fédéral dispose d'une enveloppe maximale estimée à 2.295.000 € pour la réalisation de ce projet avec les différents opérateurs télécom qui seront retenus.

Dans les limites budgétaires ci-avant précisées, l'Etat fédéral financera jusqu'à maximum 50 % des coûts totaux d'investissements, de mise en œuvre et d'exploitation de chaque plateforme anti-phishing et antifraude par SMS pour les années 2022-2023-2024. Les 50 % restants ou plus demeureront à charge de chaque opérateur télécom.

Dans son dossier de candidature, chaque opérateur devra fournir tous les coûts ventilés et démontrés en détail (voir chapitre 4.3). En d'autres termes, l'opérateur doit indiquer le prix de revient total pour

la mise en place de sa plateforme et la ventilation sur les différentes années 2022-2023-2024 pour chaque type de dépense (software, hardware, personnel, maintenance et autres).

L'intervention totale s'élève ainsi à un maximum de 50% du coût total du projet sur les années 2022-2024. Toutefois, les subsides fournis par l'Etat fédéral devront être affectés aux dépenses effectuées par les opérateurs en 2022, et le cas échéant en 2023, et être justifiés par des pièces justificatives (voir plus loin).

Les subventions peuvent couvrir tous les aspects/coûts liés au projet. Les fonds seront alloués à l'opérateur télécom sur la base des données relatives au coût du projet (investissements, mise en œuvre et exploitation) fournies par les opérateurs au moment de répondre à la demande.

Si 50 % des coûts totaux des candidatures retenues s'avère supérieur au budget total prévu, une clé de répartition des subsides entre les opérateurs télécom sera appliquée : chaque candidat sélectionné recevra une part des subsides proportionnellement au nombre de cartes SIM actives sur son réseau divisé par le nombre total de cartes SIM actives de tous les participants (ayant une date de référence au 31 décembre 2021 et notifiés à l'IBPT conformément à l'article 137 de la loi du 13 juin 2005 relative aux communications électroniques et à l'article 14, § 2, 2° de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges. Les cartes SIM actives pour la communication de données uniquement et l'IoT (M2M) sont exclues).

L'allocation des fonds sera basée sur le principe suivant :

1/ **Paiement 1**: préfinancement de 40% de la subvention totale acceptée après signature du protocole d'accord

2/ **Paiement 2** : financement de 40% de la subvention totale acceptée à la mise en service de la plateforme

3/ **Paiement 3** : financement des 20% restants à la fin du projet, une fois qu'il peut être démontré que la plateforme répond totalement aux résultats attendus (voir chapitre 3.5),

L'élaboration des subventions fera l'objet d'une décision d'octroi (arrêté royal) et d'un protocole d'accord avec La Ministre des télécommunications. Ils pourront être versés pendant les années 2022 et 2023.

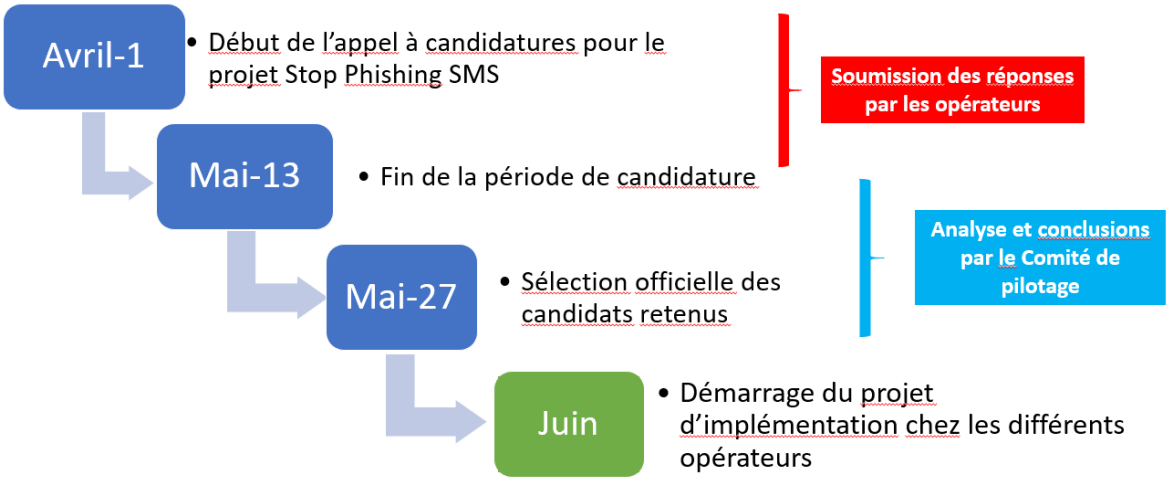
Afin d'effectuer les versements des deuxième et troisième paiement, il sera demandé aux opérateurs de fournir toutes les pièces justificatives nécessaires, cette partie sera décrite dans le protocole d'accord qui sera signé.

Les subsides ne peuvent être utilisés à d'autres fins que les adaptations nécessaires à la mise en œuvre de la plateforme antifraude.

10. Candidature, calendrier et confidentialité

Le projet débutera dès janvier 2022 et la plateforme devra être finalisée mi-2023 (au plus tard).

Les candidatures sont adressés moyennant le formulaire repris en annexe et doivent contenir toutes les informations stipulées dans le présent appel à candidatures et doivent être soumises **au plus tard le 13 mai 2022**.



Les réponses seront envoyées au chef de projet : Yves Streel

Par e-mail yves.streel@ccb.belgium.be

Toutes les informations fournies par le candidat seront traitées dans la plus stricte confidentialité par l'IBPT, le CCB et la Ministre des Télécommunications ou sa cellule stratégique.

Petra De Sutter (Signature)

Digitaal ondertekend door Petra De Sutter (Signature)
Datum: 2022.03.31 15:54:01 +02'00'

Vice-Première Ministre Petra De Sutter

Annexe : formulaire de candidature

1. Critères d'accès

Critères	Oui/ Non	Justificatif
Actif en tant qu'opérateur mobile sur le marché belge et notifié auprès de l'IBPT conformément à l'art. 9 de la LCE		
Posséder au moins 1 SMS-C opérationel afin de délivrer le trafic SMS aux utilisateurs mobiles belges		
Proposer le service SMS sur le marché intérieur		
Description des plateformes actuelles (équipement et interconnexion) ainsi que des outils anti-fraude existants (par exemple : pare-feu)		
Désireux d'investir dans une plateforme de détection de messages SMS et MMS (optionel) frauduleux		
Démonstration du respect de l'ensemble de la législation applicable, notamment en matière de protection de la vie privée, en particulier l'article 125 de la loi relative aux communications électroniques « LCE » en abrégé		
L'opérateur prend en compte le blocage des messages MMS frauduleux		

2. Exigences techniques et opérationnelles : 60 points.

Critères	Oui/ Non	Justificatif
Real-time platform		
Automatic detection		
Language independant		
Machine Learning		
Possibilité d'intervention manuelle		
Analyse le contenu des SMS		
Analyse de L'URL		
Analyse des Métadonnées		
Utilisation d'un algorithme de détection de message frauduleux		
Description détaillée de la matrice de décision		

3. Aspects financiers : 20 points.

Critères	Oui/ Non	Justificatif
Présentation détaillée de tous les coûts afférents au projet sur 3 ans		

4. Objectifs – résultats attendus (Informations et rapports statistiques) : 20 points.

Critères	Oui/ Non	Justificatif
Rapport 1 : Nombre de SMS bloqués sur une période donnée par rapport au nombre total de SMS sur la même période (en tenant compte du trafic exclu)		
Rapport 2 : KPI pour que le délai moyen par campagne de smishing soit automatiquement détecté et traité		
Rapport 3 : le « nombre de plaintes pour lesquelles aucune action n'a été entreprise » pour une période donnée		
Rapport 4 : mesure de l'efficacité de la plateforme		
Rapport 5 : chiffre pertinent que la plateforme peut présenter chaque semaine ou chaque mois pour démontrer le succès du lancement de la plateforme		

5. Autres informations requises.

Critères	Oui/ Non	Justificatif
Plan de projet détaillé (incluant toutes les phases) dans le but de rendre le système antifraude pleinement opérationnel		
Tous les coûts ventilés et démontrés en détail (voir chapitre 4.3), càd description du prix de revient total pour la mise en place de sa plateforme et la ventilation sur les différentes années 2022-2023-2024 pour chaque type de dépense		
Tout éléments supplémentaires importants pour atteindre l'objectif du projet et qui démontrent l'expertise du candidat, le cas échéant du prestataire envisagé (par exemple, des mises en œuvre à l'étranger)		
Un seul point de contact dans le cadre de ce projet		
S'engage à fournir de manière hebdomadaire l'état d'avancement de son projet en collaboration avec le chef de projet		