Appel à candidatures pour le projet Stop phishing par e-mail

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. En 2021, 4.500.000 messages ont été transférés à l'adresse suspect@safeonweb.be. En 2022, ce chiffre a encore grimpé pour atteindre 5,5 millions de messages, ce qui a permis la détection de plus de 1,5 millions d'URL suspects, soit une moyenne de 15.000 messages analysés par jour.

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 2022 », l'ENISA, l'Agence de l'Union européenne pour la cybersécurité, confirmait que l'hameçonnage est le vecteur d'attaque le plus utilisé pour obtenir une première entrée dans une organisation. L'ingénierie sociale et en particulier le phishing restent une technique populaire pour les attaquants pour mener leurs activités malveillantes. 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 suite au Covid-19 et en raison de la crise énergétique actuelle. »

Défis : Détecter et bloquer les messages d'hameçonnage envoyés par e-mail 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 et les fournisseurs d'accès à internet, 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. La première composante , à savoir la composante anti-phishing pour les SMS (smishing) est en cours d'implémentation, la deuxième composante qui traite de l'anti-phishing pour les e-mail, est abordée dans cet appel. Les 2 autres parties, à savoir 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.

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 les personnes qui possède une adresse de messagerie électronique (e-mail), proposée et gérée par un opérateur de télécommunication ou fournisseur d'accès internet qui offre un service d'accès à l'internet sur le territoire belge.

Période de mise en œuvre du projet

Le projet débutera début 2023 par l'appel à candidature et devra être finalisé fin du premier trimestre 2024.

3. Exigences

3.1. Critères d'admissibilité

Qui peux participer à ce projet ?

Chaque candidat désireux de participer au projet Stop Phishing par e-mail devra :

- Être actif en tant qu'opérateur ou fournisseur internet sur le marché belge et notifié auprès de l'IBPT conformément à l'art. 9 de la LCE : Loi du 13 juin 2005 relative aux communications électroniques;
- Proposer le service e-mail sur le marché intérieur aux citoyens que ce soit via une adresse privée ou de société ;
- Posséder au moins 1 e-mail Gateway opérationel afin de délivrer le trafic e-mail aux utilisateurs ;
- Fournir une description des plateformes actuelles (équipement et interconnexion) ainsi que des outils anti-fraude statique/réactif et dynamique/proactif (voir paragraphe 3.2) existants pour combattre le hameçonnage par e-mail;
- Être désireux d'investir dans une nouvelle plateforme de détection de messages e-mail frauduleux ou dans l'extension par l'ajout de nouvelles fonctionalités de leur plateforme actuelle afin d'en améliorer la détection ;
- Si au moment de la soumission, le candidat a déjà effectué l'analyse des différentes solutions et réalise le test d'une solution potentielle, par exemple au travers d'un pilote à grande échelle, il le précisera dans sa candidature. Cela n'aura pas d'impact sur l'admissibilité du projet.
- Le demandeur doit démontrer qu'il respecte l'ensemble de la législation applicable, notamment en matière de protection de la vie privée.
- Le demandeur doit soumettre une proposition réaliste de collecte de données statistiques pour mesurer l'efficacité de la solution.

3.2. Exigences techniques et opérationnelles

Actuellement les opérateurs et les fournisseurs d'internet qui propose le service de messagerie e-mail ont déjà des solutions en place, mais celles-ci sont encore insuffisantes par rapport à l'ingéniosité développée par les cyber criminels. Cet appel à candidature répond à une volonté d'améliorer de manière efficace et significative les systèmes anti-fraude aux e-mail en utilisant les dernières techniques proposées par les fournisseurs experts dans le domaine.

Actuellement on distingue 2 types de systèmes :

- Statique (réactif) :

- permet la détection réactive des campagnes de phishing connues (uniquement)
- basé sur les empreintes digitales (fingerprints) / indicateurs de compromission (IoCs-Indicators of Compromise) / résultats de hashage (hashes) …
- utilise uniquement des listes (de domaines/adresses/…) connus et des scores de réputation externes préalablement provisionnés et n'essaie pas de révéler des clusters de messages similaires avec de légères variations

- Dynamique (proactif) :

Permet une détection instantanée des

- campagnes de phishing émergentes et variation de contenu
- des scores de réputation dynamiques basés sur les similarités entre les messages (contenu/métadonnées)

Le nouveau système devra être capable de détecter de manière autonome des campagnes de phishing émergentes et jusque-là inconnues, en utilisant les techniques les plus avancées, élaborées par l'intelligence artificielle en utilisant toutes ou en partie les techniques suivantes :

- Approche basée sur le comportement (Behavioral based approach)
- Analyse comportementale basée sur la découverte (Heuristics based behavioral analysis)
- Algorithmes d'apprentissage automatique (Machine learning algorithms)
- Analyse et technique de la Vision par ordinateur (Computer Vision)

L'algorithme de détection des messages frauduleux doit se baser sur l'analyse des éléments suivants :

A. Analyse de l'adresse e-mail de l'envoyeur

Le demandeur doit préciser les méthodes utilisées pour identifier et analyser l'expéditeur du message.

B. Analyse de l'adresse IP

Le demandeur doit préciser les méthodes utilisées pour identifier et analyser l'adresse IP de l'envoyeur.

C. Analyse du contenu des e-mail

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.

D. 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).

E. L'analyse des métadonnées

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

F. L'analyse des pièces jointes

Le demandeur devra clarifier les méthodes utilisées pour l'analyse des pièces jointes (fichier pdf, fichier word, fichier d'archive, …), qui sont des indicateurs de messages frauduleux.

G. L'analyse des images

Le demandeur devra clarifier les méthodes utilisées pour l'analyse des images (QR code, image basée sur du texte et logo), qui sont des indicateurs de messages frauduleux.

Ces analyses doivent également répondre aux exigences suivantes de la plateforme :

1) la plateforme fonctionnera en temps réel (**Real Time**), les compteurs dynamiques et les scores de réputation seront calculés par la solution, au lieu de ce qui se fait dans un système statique (réactif) via des listes (de domaines et adresses connus…) et des scores de réputation externes préalablement provisionnés ;

2) la plateforme fonctionnera en mode de détection automatique (**Automatic Detection**), mais certaines interventions manuelles du candidat 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**) ;

Il faut également indiquer comment le personnel autorisé du candidat peut effectuer un réglage manuel sur la base des informations actuelles.

Le candidat doit définir 3 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 :

Catégorie	Score correspondant (max. 100 - à titre indicatif)	Y a-t-il une fraude ?	Action
A	>80	Certainement	Effacer le message (et donc ne pas le remettre à l'utilisateur final)
B	>40 et <80	Probablement	Placez le message dans le dossier "Courrier indésirable" ou "Spam" et ajoutez un avertissement clair à l'objet du message
C	> 20 et < 40	Doute	Placer le message dans le dossier "Boîte de réception" avec un avertissement "danger"

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 e-mail.

Les informations détaillées recueillies à la suite des différentes analyses (scan) telle que décrites ci-dessus doivent être détruites dès que possible. Bien sûr cela n'exclut pas que sur la base du scan des informations statistiques sous forme agrégées soient conservées afin d'alimenter l'algorithme.

Le candidat au partenariat doit démontrer dans son dossier de candidature que la solution proposée permet de lutter efficacement contre le hameçonnage par e-mail.

3.3. Aspects financiers

Le candidat doit démontrer qu'il prendra en charge au moins 50 % des coûts d'achat et d'exploitation du nouveau système (nouvelle plateforme ou extension de fonctionnalités) mis en place 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. Dans son dossier de candidature, le candidat devra fournir tous les coûts ventilés et démontrés en détail. En d'autres termes, le candidat doit indiquer le prix de revient total pour la mise en place et l'exploitation de sa plateforme pendant 3 années, ventilé sur les différentes années 2023-2024-2025-2026 pour chaque type de dépense (software, hardware, personnel, maintenance et autres).

3.4. Planning du projet

L'opérateur de télécommunications belge ou le fournisseur d'accès à l'internet mettra en œuvre la plateforme anti-phishing et anti-fraude « de pointe » au sein de son réseau 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 e-mail 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, de la définition à l'implémentation et l'exploitation complète.

3.5. Objectifs – résultats attendus

L'objectif du projet est de réduire de manière significative les messages e-mail frauduleux reçus par les utilisateurs.

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.

Le candidat devra proposer dans sa réponse un moyen de mesurer les éléments suivants :

- 1) Nombre de e-mail bloqués sur une période donnée par rapport au nombre total de e-mail 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 Phishing 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 Phishing 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 candidats 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 dès le lancement de la plateforme et le groupe de pilotage du projet procédera à une évaluation régulière.

4. 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.

5. Propriétés des résultats

Chaque candidat sélectionné e candidat 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.

6. Dossier de candidature et engagements

Le candidat doit démontrer dans son dossier de candidature qu'il répond à tous les critères d'admissibilité décrits au chapitre 3.1.

En outre, le candidat doit fournir une description détaillée des systèmes e-mail (à la fois fonctionnels et architecturaux) dont il dispose à la date du 1er novembre 2022. Une description des systèmes antifraude e-mail statique et/ou dynamique (voir paragraphe 3.2) 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 (aspects financiers), au chapitre 3.4 (planning du projet) et au chapitre 3.4 (résultats attendus).

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 au candidat 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.

7. Critères d'évaluation

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	3
Automatic detection	3
Language independant	3
Behavioral based approach	3
Heuristics based behavioral analysis	3
Machine Learning	3
Computer Vision	3
Analyse de l'adresse de l'expéditeur	4

Analyse de l'adresse IP	4
Analyse le contenu des e-mail	4
Analyse des pièces jointes (fichier pdf et word, fichier d'archive)	4
Analyse de ou des URL	4
Analyse des images (QR code, image basée sur du texte et logo)	4
Analyse des Métadonnées	4
Utilisation d'un algorithme de détection de message frauduleux	4
Description détaillée de la matrice de décision	4
Possibilité d'intervention manuelle	3

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. Aspects projet : 10 points.

L'évaluation sera faite suivant les règles d'attributions suivantes :

Critères	**Points**
Présentation d'un plan de projet détaillé dans le but de rendre le système antifraude pleinement opérationnel.	10

d. Informations et rapports statistiques : 10 points.

Ce qui sera évalué ici est la façon d'élaborer le rapport et le format de celui-ci. L'évaluation sera faite suivant les règles d'attributions suivantes :

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

Dans une phase ultérieure, s'il est sélectionné, le candidat conclura avec la Ministre des Télécommunications 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).

8. Mécanisme d'attribution des subsides

Dans le cadre de son budget, le gouvernement fédéral dispose d'une enveloppe maximale estimée à : 2.992.500€ pour la réalisation de ce projet avec les différents opérateurs et acteurs 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 e-mail pour les années 2023-2024-2025-2026. Les 50 % restants ou plus demeureront à charge de chaque opérateur télécom.

L'intervention totale s'élève ainsi à un maximum de 50% du coût total du projet sur les années 2023-2025. Toutefois, les subsides fournis par l'Etat fédéral devront être affectés aux dépenses effectuées par les opérateurs en 2023 et 2024, 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 de télécommunications belge ou le fournisseur d'accès à l'internet sur la base des données relatives au coût du projet (investissements, mise en œuvre et exploitation) fournies par les opérateurs dans le dossier de candidature.

Si 50 % des coûts totaux des candidatures retenues s'avère supérieur au budget total prévu, une clé de répartition des subsides entre les candidats retenus pour ce projet sera appliquée : chaque candidat sélectionné recevra une part des subsides proportionnellement aux nombres de connexions haut débit par le nombre total de connexions haut débit de toutes les parties sélectionnées à la date du 1er janvier 2023.

La compensation de service public sera libérée comme suit :

- une première tranche de 40 % des coûts éligibles estimés après la conclusion du protocole;

- une deuxième tranche de 40 % des coûts éligibles estimés à la mise en service de la plateforme de blocage de messages e-mail;

- une troisième tranche dont le montant correspond à 50% des coûts réels éligibles moins le montant déjà réglé au travers des première et deuxième tranches, lorsque le candidat sélectionné démontre que la plateforme de blocage de messages e-mail répond totalement aux résultats attendus tels que décrits dans le protocole et au plus tard le 31 mars 2024

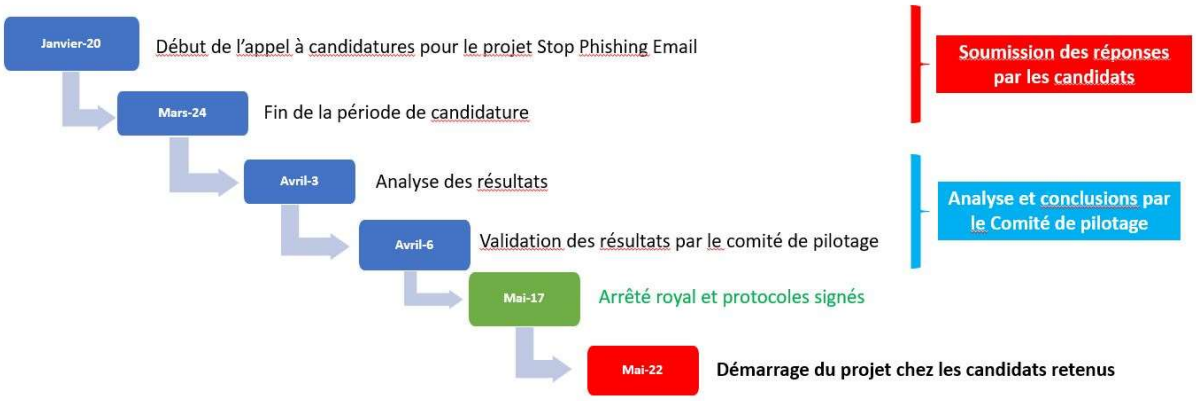
L'élaboration des subventions fera l'objet d'une décision d'octroi (arrêté royal) et d'un protocole d'accord avec La Ministre des télécommunications. Ils pourront être versés pendant les années 2023 et 2024.

Afin d'effectuer les versements du troisième paiement, il sera demandé aux candidats sélectionnés 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 nouvelle plateforme antifraude ou de l'extension de la plateforme actuel tels que défini au chapitre 3.

9. Candidature, calendrier et confidentialité

Les candidatures sont adressées moyennant le formulaire repris en annexe, doivent contenir toutes les informations stipulées dans le présent appel à candidatures et doivent être soumises **au plus tard le 24 mars**.



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.

Vice-Première Ministre Petra De Sutter

Annexe : formulaire de candidature

1. Critères d'admissibilité

Critères	Oui/ Non	Justificatif
Être actif en tant qu'opérateur ou fournisseur internet sur le marché belge et notifié auprès de l'IBPT conformément à l'art. 9 de la LCE : Loi du 13 juin 2005 relative aux communications électroniques		
Proposer le service e-mail sur le marché intérieur aux citoyens que ce soit via une adresse privée ou de société		
Posséder au moins 1 e-mail Gateway opérationel afin de délivrer le trafic e-mail aux utilisateurs		
Fournir une description des plateformes actuelles (équipement et interconnexion) ainsi que des outils anti-fraude statique/réactif et dynamique/proactif (voir paragraphe 3.2) existants pour combattre le hameçonnage par e-mail		
Être désireux d'investir dans une nouvelle plateforme de détection de messages e-mail frauduleux ou dans l'extension par l'ajout de nouvelles fonctionalités de leur plateforme actuelle afin d'en améliorer la détection		
Le candidat a déjà effectué l'analyse des différentes solutions et réalise le test d'une solution potentielle, par exemple au travers d'un pilote à grande échelle		
Le demandeur doit démontrer qu'il respecte l'ensemble de la législation applicable, notamment en matière de protection de la vie privée		
Le demandeur doit soumettre une proposition réaliste de collecte de données statistiques pour mesurer l'efficacité de la solution		

2. Exigences techniques et opérationnelles : 60 points.

Critères	Oui/ Non	Justificatif
Real-time platform		
Automatic detection		
Language independant		
Behavioral based approach		
Heuristics based behavioral analysis		
Machine Learning		
Computer Vision		
Analyse de l'adresse de l'expéditeur		
Analyse de l'adresse IP		
Analyse le contenu des e-mail		
Analyse des pièces jointes (fichier pdf et word, fichier d'archive)		
Analyse de ou des URL		

Analyse des images (QR code, image basée sur du texte et logo)		
Analyse des Métadonnées		
Utilisation d'un algorithme de détection de message frauduleux		
Description détaillée de la matrice de décision		
Possibilité d'intervention manuelle		

3. Aspects financiers : 20 points.

Critères	Oui/ Non	Justificatif
Présentation détaillée de tous les coûts ventilés et démontrés en détail, càd description du prix de revient total pour la mise en place de sa plateforme et la ventilation sur les différentes années 2023-2024-2025-2026 pour chaque type de dépense		

4. Plan projet : 10 points

Critères	Oui/ Non	Justificatif
Plan de projet détaillé (incluant toutes les phases) dans le but de rendre le système antifraude pleinement opérationnel		

5. Objectifs – résultats attendus (Informations et rapports statistiques) : 10 points.

Critères	Oui/ Non	Justificatif
Rapport 1 : Nombre de e-mail bloqués sur une période donnée par rapport au nombre total de e-mail 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		

6. Autres informations requises.

Critères	Oui/ Non	Justificatif
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		