DIGITAL SECURITY FOR SENIOR CITIZENS

2020-1-PL01-KA204-082121

Cadre de compétences en sécurité numérique

Ce projet a été financé avec le soutien de la Commission européenne. Cette publication reflète uniquement les opinions de l'auteur, et la Commission ne peut être tenue responsable de l'utilisation qui pourrait être faite des informations qu'elle contient.

Contributeurs

Cuiablue Ltd, Royaume-Uni

CWEP, Pologne

FyG Consultores, Espagne

eSeniors, France

Innovation Hub, Grèce

Contenu

Contexte

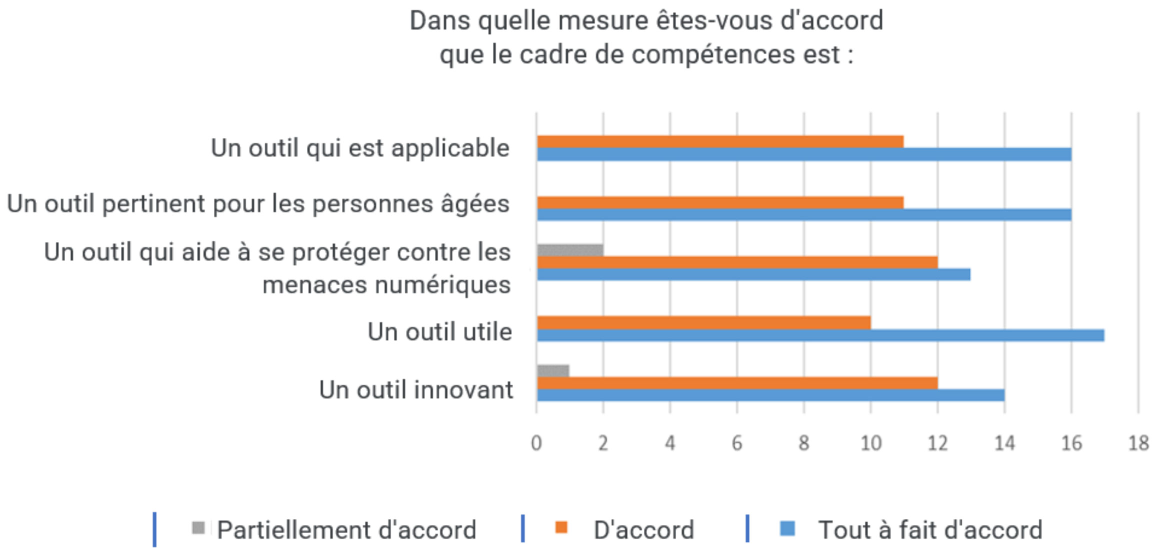
Ce cadre a été développé dans le cadre de la production intellectuelle (intellectual output) 1 du projet DiSC (Digital Security for Senior Citizens). Dans le cadre plus large du projet DiSC, ce résultat vise à soutenir le projet dans le renforcement de la capacité numérique des personnes âgées à reconnaître et à s'adapter de manière proactive aux menaces et aux menaces à la sécurité numérique, et à poser les bases de la la mise en œuvre et de l'adoption de politiques de sécurité numérique ciblées au niveau européen. Ce cadre est un petit pas vers ces deux objectifs.

Méthodologie

Le consortium a discuté et convenu de l'approche méthodologique pour l'élaboration du cadre lors de la réunion de lancement du projet en décembre 2020. Premièrement, un ensemble de questionnaires pour les réunions de consultation des parties prenantes et un modèle pour la recherche documentaire ont été développés, peaufinés et modifiés. En conséquence, afin que les partenaires puissent commencer à recueillir des informations à la pointe de la technologie sur les informations, les conseils, les orientations et les politiques actuelles en matière de sécurité numérique au niveau national dans chaque pays représenté. Alors que le consortium a entrepris des recherches documentaires, la première version du cadre a été élaborée. Après avoir résumé et analysé les résultats de la recherche documentaire et pris en considération les commentaires reçus des réunions de consultation des parties prenantes, la deuxième itération du cadre a été développée pour les commentaires et les réactions du consortium. Une fois les commentaires et les contributions intégrés, la version finalisée du cadre a été traduite et testée avec des groupes de parties prenantes plus larges et des utilisateurs finaux.

Consultation des parties prenantes

Dans le cadre de l'approche de co-création du projet DiSC pour les résultats du projet, vous trouverez ci-dessous un résumé des contributions pertinentes recueillies lors des premières réunions de consultation des parties prenantes au début de 2021 par tous les partenaires du projet. Les déclarations relatives au cadre de compétences sont résumées ci-dessous. Les parties prenantes ont ensuite été invitées à commenter leur décision ou à ajouter leurs réflexions sur le cadre.



Les parties prenantes ont ensuite été invitées à donner suite aux réponses quantitatives en répondant à la question « Avez-vous des commentaires ou des recommandations qui nous aideraient à améliorer le Cadre de compétences en sécurité numérique ? » et ont reçu une zone de texte ouverte pour donner des commentaires, des réflexions ou des impressions générales sur le concept qu'ils avaient.

Les recommandations spécifiques comprenaient la garantie d'un vocabulaire pertinent à comprendre pour les personnes âgées et l'accent mis sur les exigences de base réalisables pour garantir l'accessibilité et l'adoption. Une autre recommandation de ce type consistait à fournir aux utilisateurs les moyens et les ressources nécessaires pour développer chaque compétence, ce qui répond au besoin d'IO2 et d'IO3.

La recommandation la plus fréquemment reçue était que le cadre prenne en compte les développements technologiques les plus récents et les plus rapides et les problèmes de cybersécurité associés ; la crypto-monnaie et les centaines d'approches créatives en constante évolution que les cybercriminels utilisent pour tenter de voler de telles devises en sont un bon exemple. C'est dans ce contexte que le consortium DiSC fait face au plus grand défi dans la conception du cadre : il doit être suffisamment complet pour couvrir le large éventail de compétences et de connaissances différentes requises, mais aussi suffisamment flexible pour s'adapter aux innovations futures.

Recherche documentaire

La deuxième phase entreprise par le consortium s'est concentrée sur la collecte d'informations, de conseils, d'orientations et de documents de politique nationale pertinents qui aideraient à encadrer le contexte dans lequel le cadre de compétences en sécurité numérique se situe à la fois au niveau national dans chacun des pays partenaires, mais également au niveau européen. Au total, le consortium a analysé 10 documents pertinents, deux de Pologne, du Royaume-Uni, de Grèce, de France et d'Espagne ; ceux-ci sont résumés ci-dessous. Toutes les recherches documentaires se trouvent en annexe à la fin de ce document.

La stratégie nationale de cybersécurité de la Grèce 2020-2025 : consiste en un plan national pour la période 2020-2025 comprenant les objectifs stratégiques, les priorités, les politiques et les mesures réglementaires visant à garantir un niveau élevé de sécurité pour les systèmes de communication et d'information numériques au niveau national. La campagne de cybersécurité de la division grecque de la cybercriminalité sur les logiciels malveillants mobiles présente des informations et des idées pertinentes sur les formes de menaces numériques et comment les pirates pourraient violer les données personnelles des citoyens.

En France, les deux documents examinés étaient le site internet Cyber Malveillance, publié en 2021 par le gouvernement français, et un document concis de la CNIL (Commission nationale de l'informatique et des libertés) intitulé « 10 astuces de la CNIL pour rester net sur le net ». Les deux documents sont publiés dans le but de sensibiliser et de renforcer les capacités de tous les citoyens à faire face aux cybermenaces. Les deux documents diffèrent en termes de conception et de niveau et de profondeur des informations qu'ils transmettent, et s'alignent donc bien avec le projet DiSC en termes de ce que nous visons à réaliser et de la manière dont le consortium du projet DiSC s'engagera et présentera les informations aux utilisateurs finaux.

En Pologne, la recherche s'est concentrée sur un guide officiel de cybersécurité pour les citoyens, développé et publié par le gouvernement polonais « Comment se protéger des cyberattaques ». Le document fournit une base de référence de ce qui pourrait être considéré comme des connaissances essentielles sur l'utilisation d'internet et en particulier des réseaux sociaux et pourrait donc être pris en considération lors de l'élaboration du cadre et potentiellement adapté et inclus. Le second est un guide développé dans le cadre d'un autre projet de l'UE. Le document fournit des conseils sur les connaissances et la sensibilisation essentielles que tous les citoyens pourraient avoir au niveau de base afin qu'elles puissent être prises en compte lors de l'élaboration du cadre et potentiellement adaptées et incluses. Les informations des deux documents contiennent des informations pertinentes qui ont de la valeur dans l'application DiSC et qui s'appliquent à de nombreux contextes individuels et familiaux différents.

La recherche espagnole a conduit les partenaires à la stratégie nationale de cybersécurité 2019 publiée par le Conseil national de sécurité du gouvernement espagnol, qui fixe des directives dans les lignes générales d'action pour relever le défi que représente la vulnérabilité du cyberespace pour le pays. La deuxième publication de la recherche est« Vivre un internet sûr : il n'est jamais trop tard pour profiter d'un internet plus sûr » par Organización de Consumidores y Usuarios (OCU). Il contient une série de guides pratiques pour différents membres de la société, notamment les enfants, les parents, les adultes et les personnes âgées. Pour les seniors, le guide propose des recommandations pour apprendre à profiter de tous les avantages d'internet, sans préjudice de leur âge.

La recherche britannique s'est concentrée sur la Site Web national de conseils et d'orientation du Centre National de Cybersécurité du Royaume-Uni. Les informations fournies s'inscrivent dans l'objectif plus large de protection du Royaume-Uni et s'adressent donc à tous les citoyens, ce qui est reflété dans le contenu. Le deuxième document est la stratégie nationale de cybersécurité du gouvernement britannique 2016-2021 qui fournit un aperçu complet des menaces stratégiques pour le gouvernement, les entreprises et le public et donc, bien qu'il soit pertinent pour le projet DiSC, il ne couvre que marginalement les domaines abordés par ce projet. La liste complète des types de menaces est très pertinente pour le cadre et le projet dans son ensemble.

En résumé, la recherche documentaire a éclairé l'élaboration du cadre en présentant les problèmes de cybersécurité, les menaces et la terminologie utilisée dans chacun des contextes nationaux. La présentation et l'analyse des différentes formes d'informations utilisées pour différents groupes cibles ont également eu une forte incidence sur l'orientation du cadre de compétences, car certaines terminologies et la présentation des informations sont importantes pour les seniors ; mis en évidence dans des documents similaires au niveau national. Tous les pays partenaires fournissent un certain type d'informations aux personnes âgées dans le contexte national, soit spécifiquement, soit dans le cadre d'une campagne de sensibilisation plus large destinée à des groupes sociaux. Pourtant, une fois achevé, le cadre sera autonome puisqu'il fournira un ensemble de compétences applicables nécessaires pour accroître la capacité personnelle à atténuer les cybermenaces.

Introduction au cadre

Un cadre de compétences est une méthode efficace pour évaluer, maintenir et surveiller les connaissances, les compétences et les attributs des groupes cibles en matière de sensibilisation, de réactivité et de proactivité à la cybersécurité. Le cadre DiSC a été conçu pour s'appuyer sur le Cadre de compétences numériques Digcomp qui ne couvre pas explicitement la sécurité contre les cyberattaques agressives, les spams et les escroqueries utilisées pour voler les données et les informations des personnes en ligne.

Plus largement, ces compétences et aptitudes sont basées sur les sections 4.1 et 4.2 du cadre DigComp 2.1 :

4.1 Protection des appareils - Pour protéger les appareils et le contenu numérique, et pour comprendre les risques et les menaces dans les environnements numériques. Connaître les mesures de sûreté et de sécurité et tenir dûment compte de la fiabilité et de la confidentialité.

4.2 Protection des données personnelles et de la vie privée - Protéger les données personnelles et la confidentialité dans les environnements numériques. Pour comprendre comment utiliser et partager des informations personnellement identifiables tout en étant capable de se protéger et de protéger les autres contre les dommages. Comprendre que les services numériques utilisent une « Politique de confidentialité » pour informer de la manière dont les données personnelles sont utilisées.

Le consortium du projet DiSC a divisé les 4.1 dispositifs de protection et 4.2 la protection des données personnelles et de la vie privée en cinq sous-sections, qui ont été utilisées pour classer les compétences pertinentes en matière de sécurité numérique :

1. Connaissance des menaces : sensibilisation aux différents types de menaces pour la sécurité numérique
2. Compréhension des menaces : connaissance des risques associés aux menaces de sécurité numérique
3. Planification de l'atténuation : préparation contre
4. Détection des menaces : application de la pensée critique et analytique aux menaces potentielles de sécurité numérique

5. Contrer les menaces : résoudre les problèmes pour contrer les menaces et les violations

L'établissement du cadre de compétences en matière de sécurité numérique permettra au projet DiSC de définir les connaissances et les compétences en matière de cybersécurité requises pour faire face aux menaces potentielles, d'identifier les compétences spécifiques en matière de cybersécurité, sous la forme d'ensembles de sujets, et de soutenir le développement et la proposition de cours et d'opportunités de formation personnelle et professionnelle spécifiques pour les groupes cibles sur la base du cadre.

Les utilisateurs finaux visés du cadre de compétences sont les personnes âgées de 55 ans et plus. Le cadre devrait également être pertinent et intéressant pour les enseignants, les formateurs, les éducateurs et les praticiens des TIC en formation et en cours d'emploi travaillant dans le domaine du renforcement des capacités technologiques des seniors.

Le cadre de compétences en sécurité numérique vise à définir les aptitudes, les connaissances et les attitudes des compétences clés nécessaires aux seniors pour intégrer efficacement les protocoles de sécurité numérique dans leurs contextes localisés, ainsi qu'à fournir un cadre de référence de l'UE pour développer et évaluer les compétences en sécurité numérique.

Champ d’application

Pour définir le périmètre du cadre, les partenaires ont identifié le dispositif, la démarche et les méthodes envisagées pour appliquer le Cadre de Compétences Numériques. Cela aidera à différencier les autres types d'activités criminelles qui ne sont pas couverts par les compétences du cadre.

Appareils : l'appareil utilisé pour contacter la victime

- Téléphones et Smartphones
- Ordinateurs fixes et portables
- Tablettes

Approche : la technique utilisée pour arnaquer la victime

- Hameçonnage : tentative frauduleuse d'obtenir des informations ou des données sensibles, telles que des noms d'utilisateur, des mots de passe et des détails de carte de crédit, en se faisant passer pour une entité digne de confiance dans une communication électronique.
- Vishing (Phishing vocal) : le phishing vocal est une forme de fraude téléphonique criminelle, qui utilise l'ingénierie sociale par le système téléphonique pour accéder à des informations personnelles et financières privées dans le but d'obtenir une récompense financière.
- Smishing (SMS Phishing) : activité qui permet aux criminels de voler l'argent ou l'identité des victimes, ou les deux en réponse à un message texte. Le smishing utilise votre téléphone mobile (soit un smartphone, soit un combiné traditionnel non connecté à internet) pour manipuler des personnes innocentes afin qu'elles prennent diverses mesures qui conduisent à une fraude.

- Fraude logicielle : Une activité dans laquelle le fraudeur utilise un logiciel faux ou copié tel qu'une application ou un programme pour accéder aux données sur un appareil numérique, qu'il utilise ensuite pour voler l'argent ou l'identité des victimes.
- Ingénierie sociale : terme utilisé pour un large éventail d'activités malveillantes accomplies par le biais d'interactions humaines. Il utilise la manipulation psychologique pour amener les utilisateurs à commettre des erreurs de sécurité ou à divulguer des informations sensibles.

Méthode : l'arnaque prévue

- Escroquerie par e-mail par hameçonnage
- Arnaque au « prince » riche
- Arnaque à la carte de voeux
- Arnaque au prêt bancaire ou à la carte de crédit
- Arnaque à la loterie
- Escroquerie par extorsion
- Arnaque de rencontres en ligne
- Faux logiciel antivirus
- Usurpation d'identité sur Facebook ou de profil piraté
- Arnaque « Gagnez de l'argent rapidement ! »
- Escroqueries de voyage
- Les escroqueries aux crypto-monnaies
    - Faux échanges Bitcoin
    - Schémas de Ponzi
    - Tentatives d'escroquerie au quotidien
    - Malware
- Arnaque aux fausses nouvelles
- Faux sites marchands
- Les arnaques aux offres d'emploi
- Arnaque SMS (Smishing)
- Arnaque de trop-payé en ligne
- Assistance technique Escroqueries en ligne

Remarque : les menaces numériques changent et évoluent constamment et, de par leur nature, il est impossible d'en dresser une liste exhaustive. Pour se tenir au courant des menaces, DiSC recommande de s'abonner à une organisation ou à un réseau de cybersécurité, tel que Sécurité Heimdal, par exemple, qui publie des mises à jour régulières sur les problèmes, les approches et les méthodes de cybersécurité, ou Les zones de tendances criminelles d'Europol page.

Le cadre

Compétences fondamentales	Niveaux de compétence		
Descripteurs	Fondamental L'individu comprend le concept de base, les compétences et les connaissances requises en matière de sécurité numérique et est prêt à atteindre le plus haut niveau de compétence dont il est capable.	Intermédiaire L'individu fait preuve d'un esprit critique lié à la sécurité numérique, peut différencier les menaces numériques sur tous les appareils et est capable de planifier et de mener à bien de manière indépendante des mesures d'atténuation pour s'en protéger.	Avancée L'individu fait preuve d'une pensée analytique envers la sécurité numérique et peut réagir aux menaces en temps réel en évaluant et en choisissant la réponse la plus efficace dans une situation à haute pression.

1. Sensibilisation aux menaces

Sensibilisation aux menaces	Fondamental	Intermédiaire	Avancée
Sensibilisation aux menaces spécifiques qui ciblent les appareils numériques.	Je suis conscient des menaces de sécurité numérique et leurs différentes approches utilisées.	Je suis conscient des menaces à la sécurité numérique et des approches moins courantes.	Je me tiens au courant des nouvelles approches de sécurité numérique au fur et à mesure qu'elles évoluent.
	Je suis conscient des menaces de sécurité numérique et de leurs différentes méthodes utilisées.	Je suis conscient des menaces à la sécurité numérique et des méthodes moins courantes.	Je me tiens au courant des nouvelles méthodes de sécurité numérique au fur et à mesure qu'elles évoluent.
	Je connais les activités de base de l'ingénierie sociale dans la sécurité numérique.	Je connais des techniques d'ingénierie sociale plus complexes.	Je connais différentes combinaisons de techniques, d'approches et de méthodes d'ingénierie sociale.

2. Compréhension des menaces

Compréhension des menaces	Fondamental	Intermédiaire	Avancée
Connaissance des caractéristiques et fonctions de chacune des menaces. Évaluer les menaces numériques et leur niveau de risque. Comprendre la nature changeante des menaces numériques. Être conscient de l'importance de sources d'informations de sécurité fiables, à jour et précises.	Je comprends les principales caractéristiques et fonctions des menaces de sécurité numérique les plus courantes.	Je comprends les principales caractéristiques et fonctions des menaces de sécurité numérique les plus rares et les plus inhabituelles.	Je mets à jour mes connaissances des menaces numériques grâce à des sources d'informations de sécurité fiables, à jour et précises.
	Je comprends le niveau de risque et les conséquences potentielles associés aux simples menaces de sécurité numérique.	Je comprends le niveau de risque et les conséquences potentielles associés aux menaces de sécurité numérique et ses multiples facettes.	Je comprends le niveau de risque et les conséquences potentielles associés aux menaces complexes de sécurité numérique.

3. Atténuation

Atténuation	Fondamental	Intermédiaire	Avancée
Compétences et expérience permettant de prendre des décisions éclairées concernant la protection contre les menaces numériques. Connaissance et compréhensi on des	Je peux identifier des outils de protection numérique adaptés pour atténuer les menaces de sécurité numérique.	Je peux utiliser mes expériences et compétences passées pour éclairer mes décisions sur la protection contre les menaces de sécurité numérique.	Je peux utiliser mon expérience et mes compétences pour analyser les impacts potentiels de différents risques et choisir des stratégies de protection adaptées en conséquence.
	Je peux suivre les instructions de sécurité numérique de base pour atténuer les	Je peux décider des outils de sécurité numérique de base les plus appropriés pour	Je peux analyser et évaluer les menaces à la sécurité numérique et adapter ma stratégie de

différents outils et ressources pour se protéger contre les menaces.	menaces de sécurité numérique.	atténuer les menaces de sécurité numérique.	protection en fonction de la menace à la sécurité numérique.
	Je sais comment configurer un appareil numérique pour assurer une protection contre les menaces de sécurité numérique de base.	Je sais comment vérifier et mettre à jour un appareil numérique pour assurer une protection appropriée contre les menaces de sécurité numérique les plus courantes.	Je sais comment installer des outils et des logiciels de protection sur des appareils pour atténuer les menaces numériques.

4. Détection des menaces

Détection des menaces	Fondamental	Intermédiaire	Avancée
Capacité à reconnaître les menaces numériques et les risques spécifiques posés Connaissances pour pouvoir catégoriser les menaces numériques par niveau de risque	Je peux reconnaître et identifier les menaces de sécurité numérique les plus courantes pour mes données et informations personnelles.	Je peux reconnaître et identifier les menaces de sécurité numérique les plus rares et inhabituelles pour mes données et informations personnelles.	Je reste activement conscient des menaces à la sécurité numérique grâce à des sources d'informations de sécurité fiables, à jour et précises.
	Je peux reconnaître des risques et des menaces clairs et évidents dans les environnements numériques.	Je peux reconnaître des menaces de sécurité numérique plus cachés.	Je peux reconnaître les risques et menaces complexes dans les environnements numériques.
	Je peux utiliser mes connaissances pour évaluer les menaces de sécurité potentielles et décider si elles sont suspectes.	Je peux utiliser mon approche analytique de la sécurité numérique pour mettre en évidence les menaces numériques.	Je peux utiliser mes capacités de pensée critique pour analyser, comparer et évaluer l'étendue d'une menace numérique et le niveau de risque associé.

5. Contrer les menaces

Contrer les menaces	Fondamental	Intermédiaire	Avancée

Prendre des décisions positives et efficaces tout en restant calme sous pression. Force mentale pour faire face à l'incertitude, au stress et aux situations difficiles.	Je suis flexible et bien préparé aux menaces de sécurité numérique.	J'utilise l'adaptabilité pour contrer les menaces à la sécurité numérique.	J'anticipe activement les menaces de sécurité numérique et leurs risques et m'entraîne à m'adapter pour les contrer.
	Je reste positif face aux menaces ou atteintes à la sécurité numérique.	Je peux utiliser mes propres expériences pour aborder les menaces et les violations potentielles avec optimisme et confiance.	Je peux expliquer comment une attitude, des comportements et des actions positives envers la sécurité numérique ont contribué à ma sécurité numérique.
	Je peux réfléchir aux expériences passées avec des menaces numériques pour en tirer des leçons.	Je peux réfléchir aux expériences passées et changer mon comportement et mon attitude envers les menaces numériques pour me rendre plus résilient face à elles.	Je peux réfléchir aux expériences passées avec des menaces numériques et changer mon comportement et mon attitude dans la vie pour devenir une personne plus résiliente.