Référentiel

Sécuriser l'environnement et les pratiques numériques

Développer ses compétences numériques en cybersécurité

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

pix

Version 1.0 - Mars 2022

Avant-propos

La dématérialisation croissante de la société fait de la maîtrise des compétences en sécurité numérique un enjeu majeur, tant au niveau individuel que collectif. Mesurer la maîtrise de ses compétences doit permettre à chacun et à chacune de se positionner sur le continuum des connaissances, pratiques, enjeux et savoir-faire en matière de cybersécurité, essentiel pour évoluer de manière sécurisée dans sa vie personnelle, professionnelle et citoyenne.

Pour répondre à cet enjeu de société, Pix a développé en partenariat avec l'ANSSI, la référence en France en matière de cybersécurité, et Cybermalveillance.gouv.fr, des outils à destination des professionnels et du grand public pour accompagner le développement des compétences nécessaires à la sécurité numérique de tous, de débutant à confirmé.

Pix, l'ANSSI et Cybermalveillance.gouv.fr ont ainsi mené un travail conjoint d'expertise sur le contenu pédagogique de la plateforme Pix en matière de sécurité numérique, et ont développé dans ce domaine de nouveaux défis ludiques pour tous les niveaux. À cette occasion, ce présent référentiel des compétences numériques dédié à la cybersécurité a également été co-créé.

Initié en 2016, Pix est un Groupement d'intérêt public à but non lucratif, réunissant des acteurs engagés dans les domaines de l'éducation et de la formation. Pix.fr est un service public en ligne ouvert à tous – élèves, étudiants, professionnels, demandeurs d'emplois, retraités, etc. – permettant de tester, développer et certifier ses compétences numériques.

L' Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique. Acteur majeur de la cybersécurité, l'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises et assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

Créé en 2017 dans le but de lutter contre les actes de cybermalveillance, Cybermalveillance.gouv.fr rassemble dans le GIP ACYMA (Groupement d'intérêt public "Actions Contre la Cybermalveillance") des acteurs publics et issus de la société civile autour de trois missions communes : sensibiliser et prévenir au risque numérique, venir en aide aux victimes, et observer la menace afin de mieux l'anticiper.

Sommaire

Pourquoi un référentiel sur la sécurité de l'environnement et des pratiques numériques ?

L'objectif de ce référentiel est de proposer une vision précise et structurée des compétences en sécurité numérique, afin de donner aux acteurs de la formation des éléments permettant de cadrer et de nourrir leurs enseignements et pratiques d'évaluation.

Ce référentiel entend couvrir le champ de la sécurité numérique dans toutes ses dimensions, qu'elles soient techniques, comportementales ou procédurales : bonnes pratiques, comportements de prudence, utilisation des outils de sécurité, mais aussi connaissance des menaces, compréhension des mécanismes de protection et de réaction, participation à l'effort collectif de sécurisation de l'espace numérique.

Ce référentiel a été élaboré dans le cadre d'un partenariat entre l'Agence nationale de sécurité des systèmes d'information (ANSSI), Cybermalveillance.gouv.fr (GIP ACYMA) et Pix, le service public en ligne pour évaluer, développer et certifier ses compétences numériques.

À qui s'adresse ce référentiel ?

Les compétences en sécurité du numérique sont mises en œuvre pour accompagner chaque dimension de la vie numérique. Par nature transversales et liées à d'autres compétences numériques, elles concernent tous les utilisateurs de services et d'équipements numériques, acteurs et citoyens (élèves, étudiants, professionnels, demandeurs d'emploi, retraités…) à partir de 13 ans. Ces compétences ont été spécifiées, regroupées, et hiérarchisées dans le présent référentiel qui a vocation à être utilisé principalement dans une visée pédagogique par les enseignants et les formateurs.

Il ne concerne pas une pratique, une situation, une formation, un métier ou un niveau d'étude en particulier. Il n'est donc pas adapté pour évaluer les compétences nécessaires pour exercer un poste spécialisé en cybersécurité. Il ne vise en effet pas à décrire des niveaux d'expertise professionnelle même s'il peut contribuer, le cas échéant, à définir des prérequis dans l'accès à des formations de spécialisation. Sa visée est englobante et générale.

Ce référentiel n'est pas propre à des savoirs ou des savoir-faire liés au contexte français, il peut donc avoir une portée internationale.

Quel est le périmètre de ce référentiel ?

La thématique de la sécurité informatique (ou cybersécurité) peut être abordée selon différents axes :

- **l'axe temporel :** la prévention puis l'identification d'une attaque, la réaction à une attaque, et enfin les conséquences d'une attaque et leur mitigation
- **les types d'équipements :** ordinateur, téléphone multifonctions, tablette, objets connectés ;
- **les types d'usages :** connexion, gestion de données, navigation web, communication… ;
- **les notions conceptuelles :** authentification, chiffrement, ingénierie sociale… Le travail effectué pour concevoir et proposer ce référentiel s'est établi au croisement de ces différentes approches.

Il comprend :

- **des connaissances** sur les risques, les types d'attaques, les moyens de les reconnaître, les outils de protection… ;
- **des savoir-faire**, notamment la maîtrise de bonnes pratiques de sécurité informatique dans des situations courantes ;
- **des enjeux** : la prise de conscience des risques, des menaces, des moyens d'actions.

Le présent référentiel s'inscrit dans le référentiel Pix, format opérationnel du cadre de référence des compétences numériques (CRCN), inspiré du cadre européen (DigComp).

Il est composé de deux parties :

- **La première partie** définit les sujets principaux en matière de sécurité numérique et correspond à la compétence **"4.1. Sécuriser l'environnement numérique"** dans le référentiel Pix.
- **La seconde partie** définit les sujets connexes en matière de cybersécurité présents dans d'autres compétences du référentiel Pix.

Les sujets abordés dans la compétence 4.1 Sécuriser l'environnement numérique du référentiel de Pix

4.1 Sécuriser l'environnement numérique — Thématique 1 :

Identification et réaction face aux principales menaces

Panorama des menaces

Menaces
#logiciel malveillant #virus #rançongiciel #injection #DDoS #MITM #forcebrute #rançongiciel

Techniques de piraterie informatique
#hacker #cyberattaques #hacktiviste #défacement

Sources d'infection
#pièce-jointe infectée #support infecté #botnets

Niveaux 1-2 — Novice — Autonomie

- Connaître les comportements et pratiques de prudence élémentaires face au risque de malveillance numérique.
- Réaliser des actions élémentaires en réponse aux différentes techniques de pirateries informatiques et/ou aux différentes sources d'infections.
- Connaître la notion de pirate informatique.

Niveaux 3-4 — Indépendant — Autonomie

- Connaître les principales sources d'infection d'un équipement informatique ainsi que les principales techniques de piraterie existantes.

Niveaux 5-6 — Avancé — Initiative

- Identifier un type précis de menace (parmi des attaques, logiciels malveillants, techniques de piraterie) et comprendre les enjeux associés.

Niveaux 7-8 — Expert — Innovation

- Vérifier l'absence de menace dans un contenu avant action.*
- Analyser une source d'infection et élaborer une solution technique originale pour y répondre.*
- Analyser une source d'infection et évaluer les risques associés.*

* À venir dans Pix

Thématique 1 :

Identification et réaction face aux principales menaces

Ingénierie sociale

Ingénierie sociale
#escroquerie #usurpation d'identité #faux support informatique

Hameçonnage
#phishing #mail #SMS #hameçonnage #données personnelles #typosquatting

Niveaux 1-2 — Novice — Autonomie

- Connaître la notion d'hameçonnage.
- Repérer des tentatives d'hameçonnage ou d'usurpation d'identité.

Niveaux 3-4 — Indépendant — Autonomie

- Reconnaître une tentative d'hameçonnage ou d'attaque par ingénierie sociale dans différents contextes.
- Réagir à une tentative d'escroquerie par ingénierie sociale.

Niveaux 5-6 — Avancé — Initiative

- Connaître et identifier différentes formes d'ingénierie sociale et d'hameçonnage.

Niveaux 7-8 — Expert — Innovation

- Mettre en œuvre une stratégie de protection contre l'ingénierie sociale et le hameçonnage.*

Thématique 2 :

Authentification sécurisée

Mots de passe

Robustesse des mots de passe
#mot de passe sûr #identifiant #longueur #caractères spéciaux #données personnelles

Bonnes pratiques relatives aux mots de passe
#couple identifiant/mot de passe #divulgation #fuite mots de passe #mail

Niveaux 1-2 — Novice — Autonomie

- Connaître les bonnes pratiques de bases concernant le choix et l'utilisation des mots de passe.

Niveaux 3-4 — Indépendant — Autonomie

- Comprendre l'importance du couple identifiant-mot de passe.

Niveaux 5-6 — Avancé — Initiative

- Comprendre les facteurs contribuant à la robustesse des mots de passe (longueur, complexité) et à leur vulnérabilité.

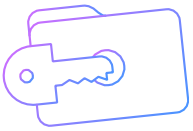
Niveaux 7-8 — Expert — Innovation

- Mettre en œuvre une stratégie avancée de gestion de l'authentification.*

Chiffrement et cryptographie

Notions de chiffrement
#chiffrement #symétrique #asymétrique

Notions de cryptographie
#secret #chiffrement #clé



Niveaux 1-2 — Novice — Autonomie

- Connaître la notion de chiffrement.
- Appliquer une méthode de chiffrement basique pour transmettre un secret.

Niveaux 3-4 — Indépendant — Autonomie

- Connaître des usages et l'importance du chiffrement en matière de sécurité.
- Appliquer une méthode de chiffrement poussée.

Niveaux 5-6 — Avancé — Initiative

- Comprendre les utilisations du chiffrement à des fins de sécurité.
- Comprendre le principe du chiffrement symétrique et asymétrique.

Niveaux 7-8 — Expert — Innovation

- Comprendre les enjeux et les limites du chiffrement en matière de sécurité.*
- Mettre en œuvre une stratégie de chiffrement pour protéger une information.*

Thématique 3 :

Utilisation d'Internet en sécurité

Accès à Internet en sécurité

Wifi sécurisé
#hotspot #box #wifi public

Niveaux 1-2 — Novice — Autonomie

- Reconnaître et se connecter à un accès wifi sécurisé.

Niveaux 3-4 — Indépendant — Autonomie

- Connaître les risques liés à un réseau wifi ouvert.
- Choisir de manière éclairée le réseau wifi le plus adapté lorsqu'un choix se présente.

Niveaux 5-6 — Avancé — Initiative

- Accompagner un tiers dans ses choix et la connexion de ses appareils à un réseau wifi sécurisé.
- Comprendre les principales modalités de sécurisation d'un réseau wifi.*

Niveaux 7-8 — Expert — Innovation

- Mettre en place un réseau wifi sécurisé à l'usage de tiers.*

Navigation sur Internet en sécurité

Sécurité d'un site web
#protocole #https #cadenas #certificat

Niveaux 1-2 — Novice — Autonomie

- Connaître l'existence du protocole HTTPS et reconnaître sa présence

Niveaux 3-4 — Indépendant — Autonomie

- Adapter son comportement sur Internet et configurer sa connexion en fonction de ses besoins et des enjeux associés.

Niveaux 5-6 — Avancé — Initiative

- Vérifier l'identité certifiée associée à un site web sécurisé.
- Évaluer la pertinence, et les conséquences possibles, de l'utilisation d'une connexion Internet non-sécurisée en fonction des usages.

Niveaux 7-8 — Expert — Innovation

- Détecter et réparer une faille sur un site web.*

Thématique 4 :

Protection des équipements informatiques

Outils de protection des équipements

Outils de prévention et protection
#antivirus #pare feu #firewall #fonctionnement #paramétrage

Utiliser un antivirus
#antivirus #quarantaine #base virale #console #freemium

Niveaux 1-2 — Novice — Autonomie

- Connaître le terme antivirus.
- Interpréter les messages d'alerte d'un antivirus.

Niveaux 3-4 — Indépendant — Autonomie

- Connaître un antivirus et ses principales fonctionnalités.
- Connaître les bonnes pratiques d'utilisation d'un antivirus.

Niveaux 5-6 — Avancé — Initiative

- Maîtriser le fonctionnement de l'antivirus.
- Optimiser l'utilisation de l'antivirus et utiliser son potentiel en cas de menaces.*

Niveaux 7-8 — Expert — Innovation

- Mettre en place un système de protection pour les équipements de tiers.*

Thématique 4 :

Protection des équipements informatiques

Bonnes pratiques de protection des équipements

Installation sûre d'un logiciel
#store #application #éditeurs officiels de logiciel

Accès aux équipements
#verrouillage #gestion session administrateur #cache webcam #câble de verrouillage #anti-reflet #nomadisme

Niveaux 1-2 — Novice — Autonomie

- Installer une application en sécurité.
- Protéger l'accès à ses équipements, personnels ou partagés.

Niveaux 3-4 — Indépendant — Autonomie

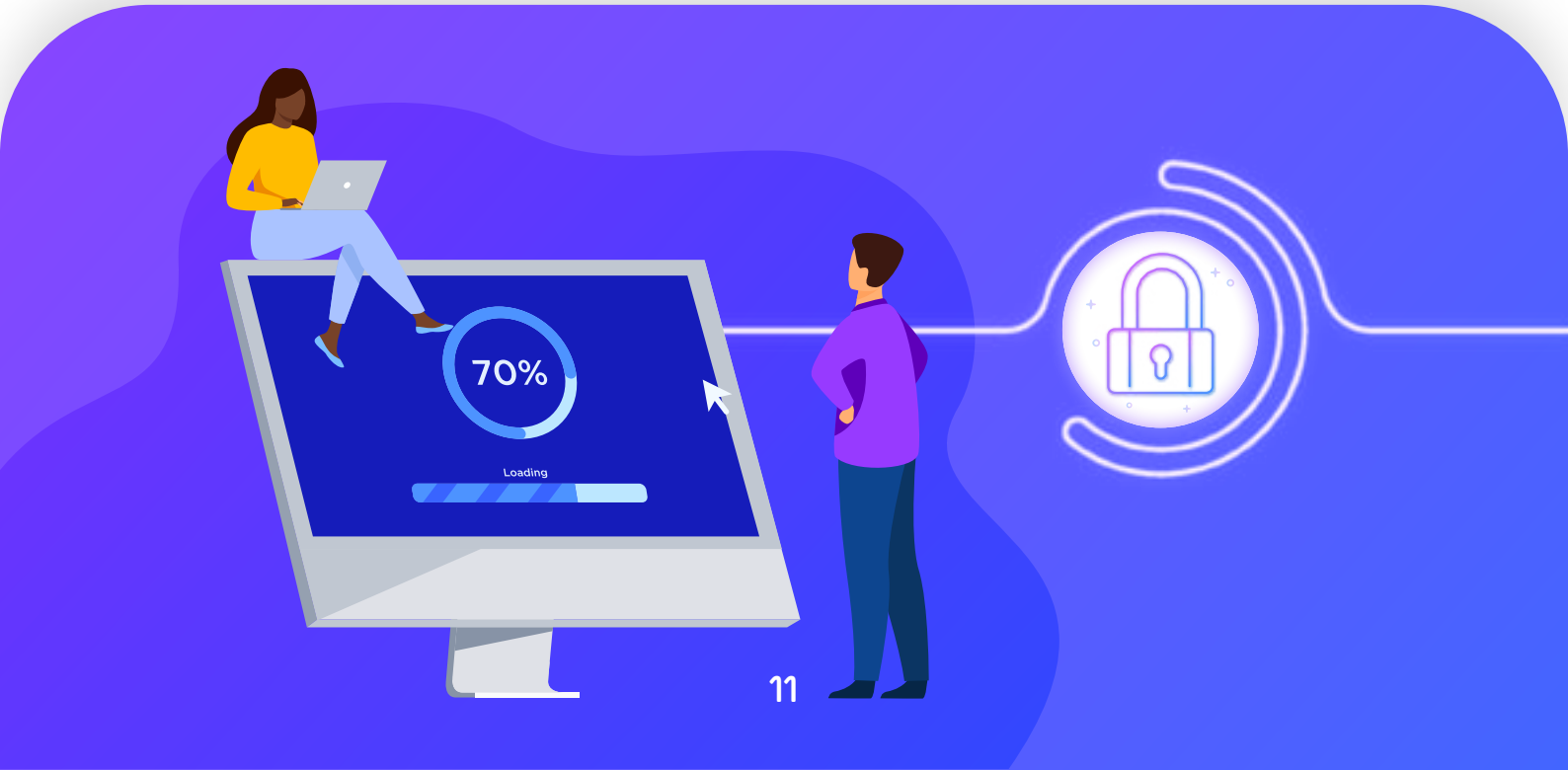
- Installer un logiciel en minimisant les risques.

Niveaux 5-6 — Avancé — Initiative

- Analyser les risques associés aux téléchargements de logiciels et s'en prémunir.*

Niveaux 7-8 — Expert — Innovation

- Maîtriser, parfois restreindre, l'accès à ses équipements et à ses données, aux personnes autorisées.*
- Vérification de l'intégrité cryptographique d'un logiciel.*



2e PARTIE

La sécurité numérique abordée dans les autres compétences du référentiel de Pix

1. 1 Mener une recherche et une veille d'information

Adresse web en pratique
Identifier, utiliser et analyser une adresse web (URL)

De nombreux pièges peuvent être évités lorsque l'on comprend et maîtrise la manipulation des URL.

1. 2 Gérer les données

Enregistrement
Enregistrer un document

Pratique de sauvegarde
Choisir la bonne localisation des fichiers pour prévenir leur perte

Sauvegarde et synchronisation
Dupliquer et synchroniser des fichiers

Sauvegarder ses données de façon robuste et maîtrisée permet de réduire la vulnérabilité à de nombreux incidents et attaques mais aussi de se protéger des menaces liées aux rançongiciels.

2.3 Collaborer

Droits d'accès à un document en ligne
Gérer les droits d'accès à un document en ligne

La maîtrise du paramétrage des documents que l'on partage est essentielle pour limiter les risques de diffusion accidentelle d'informations sensibles et certaines attaques par ingénierie sociale.

2.4 S’insérer dans le monde numérique

Charte informatique

Connaître la notion de charte informatique et les règles usuelles qu’elle recouvre

Le respect des règles d’usage des équipements informatiques au sein d’une organisation est nécessaire pour prendre la mesure des risques spécifiques à l’organisation et tenir une conduite adaptée aux équipements mis à disposition.

Choix identifiant

Maîtriser son identité numérique à travers le choix d’un identifiant (pseudo, adresse électronique…)

Le choix d’identifiants et la maîtrise des enjeux liés à l’identité numérique permet de réduire la vulnérabilité à des attaques par ingénierie sociale, comme l’usurpation d’identité.

Paramètres de confidentialité

Paramétrer la visibilité de ses publications sur un réseau social

Maîtriser la visibilité de ses publications permet de réduire et prendre connaissance de sa vulnérabilité à des attaques par ingénierie sociale.

4.2 Protéger les données personnelles et la vie privé

Accès d’une application aux données

Maîtriser l’accès à ses données lors de l’installation d’une application

Maîtriser l’accès à ses données lors de l’installation d’une application permet de réduire le volume de données qui peuvent fuiter si l’application en question se fait pirater.

5.1 Résoudre des problèmes techniques

Messages de mise à jour

Interpréter des messages liés à la mise à jour de logiciels (système d'exploitation, application, plugin, ...)

L'interprétation des messages de mise à jour permet d'une part, de garder ses équipements informatiques à jour, ce qui réduit leur vulnérabilité, et d'autre part, d'être capable de distinguer les vrais messages de mise à jour des faux, par exemple dans le cadre d'une arnaque au faux support informatique.

Mot de passe oublié

Réagir en cas d'oubli de mot de passe

Savoir utiliser la réinitialisation de mot de passe permet d'utiliser des mots de passe forts avec plus de sérénité et d'éviter d'avoir un post-it avec ses mots de passe.

5.2 Construire un environnement numérique

Périphériques et composants

Connaître les différentes parties d'un ordinateur ou d'un smartphone (périphériques et composants)

Avoir une bonne compréhension de la composition d'un ordinateur et de ses périphériques est nécessaire pour être capable d'en évaluer la dangerosité et/ou résoudre des problèmes de sécurité lorsqu'ils surviennent

Contacts

GIP Pix
www.pix.fr
communication@pix.fr

Agence nationale de la sécurité des systèmes d'information (ANSSI)
www.ssi.gouv.fr
communication@ssi.gouv.fr

GIP ACYMA
www.cybermalveillance.gouv.fr
contact@cybermalveillance.gouv.fr