Module 4 :
Sécurité sur le Net

Kit pédagogique pour l'enseignant

Quelques mots d'explication sur le thème

Internet est un très bel instrument pour rechercher et partager des informations, pour se connecter avec d'autres personnes, pour faire plein de chouettes activités. C'est un univers où les enfants d'aujourd'hui sont de plus en plus présents. Ils sont d'ailleurs très compétents en la matière mais ne mesurent pas toujours les risques auxquels ils pourraient être exposés.

Dans le module « Sécurité sur le Net », nous mettons en évidence un certain nombre de risques liés à l'utilisation d'internet et expliquons comment alerter les enfants sur ce qui pourrait mal tourner en ligne.

Objectifs

Ce module poursuit les objectifs suivants :

1. Expliquer les risques de contamination des ordinateurs, tablettes et smartphones
2. Apprendre comment protéger les ordinateurs et les réseaux sociaux
3. Sensibiliser aux comportements assertifs en ligne
4. Fournir des moyens pour signaler le cyberharcèlement

Compétences en matière de TIC

Ce module vise à faire acquérir aux élèves les compétences suivantes en matière de TIC :

- Les élèves utilisent les TIC de manière sûre, responsable et efficace.
- Les élèves sont capables d'utiliser les TIC pour communiquer de manière sûre, responsable et efficace.

De plus, une attention particulière est accordée à plusieurs compétences transversales :

- Les élèves sont capables de se protéger vis-à-vis d'autres enfants et d'adultes en utilisant des signaux compréhensibles et acceptables par les autres.

Groupe cible

- Troisième degré de l'enseignement primaire
- Premier degré de l'enseignement secondaire

Matériel

- Min. 5 ordinateurs/ ordinateurs portables avec système d'exploitation Windows 10
- Logiciel antivirus Windows Defender
- Accès internet et navigateur internet
- Module diggit « La sécurité d'abord »

Durée

2 heures de cours (2 x 50')

Préparation

- Charger les ordinateurs/ ordinateurs portables
- Préparer des informations factices pour la création d'un compte Facebook
- Préparer le module diggit « La sécurité d'abord » sur le tableau interactif

Notions importantes

Ci-dessous une liste de définitions et de termes importants relatifs à une utilisation d'internet en toute sécurité.

Ver informatique

Un ver est un programme informatique qui se multiplie. Des copies de ce ver se propagent à travers le réseau informatique sans l'intervention d'un utilisateur. Ce qui occasionne des dégâts considérables à tous les appareils connectés à ce réseau.

Contrairement à un virus, le ver se propage de lui-même sur internet, alors que le virus est incapable de le faire. Un virus a besoin d'un hôte, comme un fichier ou un e-mail, pour se propager. (Voir également : Virus)

Firewall ou pare-feu

Un firewall est un système de sécurité qui protège un réseau informatique local contre des intrusions non autorisées.

Hacking ou piratage informatique

Le piratage informatique consiste à pénétrer dans le(s) ordinateur(s) d'une autre personne ou d'une entreprise en contournant les dispositifs de sécurité. L'intention des pirates n'est pas toujours de collecter des informations de façon illégale. La plupart du temps, leur objectif vise simplement à démontrer que le réseau n'est pas suffisamment sécurisé.
Les entreprises ont souvent recours à des pirates éthiques pour découvrir des failles dans la sécurité de leurs réseaux informatiques. Ces pirates veulent ainsi contribuer à la lutte contre la cybercriminalité et sont donc les « anges gardiens » d'internet.

Troll

Dans le langage internet, un troll est une personne qui publie volontairement des messages anonymes sur internet pour semer le trouble. Parfois, ces messages sont plutôt anodins, mais souvent, ils sont bien moins innocents, voire carrément provocants.

Notions importantes

Ci-dessous une liste de définitions et de termes importants relatifs à une utilisation d'internet en toute sécurité.

Malware

Nom collectif des **logiciels malveillants et/ou nuisibles**. Ce mot est une contraction de l'expression anglaise « malicious software » (logiciel malveillant).
Exemples de malware : virus, ver informatique, cheval de Troie et logiciel espion.

Logiciel espion

On appelle logiciel espion un programme informatique qui collecte des informations sur un utilisateur d'ordinateur et les transmet à une autre personne. Le but d'un logiciel espion est généralement lucratif. Un logiciel espion est également appelé « spyware », contraction du terme anglais « spy », qui signifie espion, et du suffixe « ware » (de software), indiquant qu'il s'agit d'un logiciel.

Cheval de Troie

C'est un **programme informatique** qui a l'air plus vrai que nature alors qu'il n'en est rien. Un cheval de Troie introduit des virus et des vers informatiques en douce dans le système informatique, des programmes invisibles qui collectent des données confidentielles sauvegardées sur un ordinateur pour ensuite les transférer à l'expéditeur du cheval de Troie, dont les intentions ne sont probablement pas amicales.

Virus

Un virus est un programme informatique capable de se fixer dans un fichier de votre ordinateur. Il y rentre incognito, en se servant d'un « hôte », par exemple un fichier ou un e-mail infecté. Il est dangereux parce qu'il occupe de l'espace sur le disque dur et monopolise des ressources d'ordinateur. Dans les cas graves, un virus peut aussi effacer des informations sensibles ou les diffuser. Et dans les cas les plus graves, l'utilisateur peut même perdre totalement le contrôle de son ordinateur.

Liens intéressants

https://www.childfocus.be/fr/prevention/securite-en-ligne/professionnels
https://www.childfocus.be/fr/prevention/clicksafe-tout-sur-la-securite-en-ligne
http://www.policelocale.be/5283/questions/criminalite-sur-internet

Scénario

5’	**Partie 1 : Introduction**
15’	**Partie 2 : Démarreurs de conversation**
15’	**Partie 3 : Sécuriser votre ordinateur**
45’	**Partie 4 : Créer un mot de passe fort**
30’	**Partie 5 : Se protéger en ligne**

Partie 1 : Introduction

1. Présenter le contexte : internet est un très bel instrument, mais il comporte aussi quelques risques.
2. Expliquer l'objectif du cours.

Partie 2 : Démarreurs de conversation

Les élèves sont souvent très actifs dans le monde du digital. Il est donc important qu'ils puissent partager leurs expériences : que font-ils en ligne ? Qu'est-ce qui les intéresse ? Qu'est-ce qui fonctionne bien ou moins bien ? Entamer une conversation supervisée en classe est un premier pas pour sensibiliser encore plus les élèves aux côtés plus sombres du digital. Vous trouverez ci-dessous quelques questions qui peuvent servir de « démarreurs de conversation » sur le thème de la sécurité sur le Net.

- Supposons que quelqu'un vole vos mots de passe Facebook et Instagram. Qu'est-ce qui pourrait arriver de pire ?
- Un « faker » est une personne qui se fait passer pour quelqu'un d'autre. Parfois pour vous manipuler et vous demander de faire des choses bizarres devant la webcam. Comment reconnaît-on un « faker », par exemple sur Facebook, Instagram ou WhatsApp ? Comment réagir dans de telles situations ?
- Il peut arriver que des enfants fassent une petite incursion sur le compte de leurs amis pour publier un post amusant sur la page Facebook de l'un d'entre eux. L'intention n'est évidemment pas de nuire. Cependant, s'introduire sur le compte d'une personne est punissable. Pour vous, quelle est la différence entre une petite blague et un comportement criminel sur internet ? Quand un comportement va-t-il trop loin ?

Partie 3 : Sécuriser votre ordinateur

> **Quelques mots d'explication**
> Les ordinateurs qui sont connectés à un réseau, quelle que soit leur taille, sont vulnérables aux logiciels malveillants. Les utilisateurs doivent prendre conscience que la façon dont ils gèrent leurs ordinateurs, fichiers et e-mails peut avoir une grande influence sur la façon dont ils s'exposent à ces influences négatives.
> Dans cette partie du cours, nous allons analyser les risques de contamination des ordinateurs, tablettes et smartphones.

Étape par étape

Description étape par étape des informations, captures d'écran et illustrations comprises.

Contenu par étape	Travail en classe	Média
Tâche : Cherchez la définition des mots suivants • Malware • Cheval de Troie • Piratage • Virus • Troll	Travail en petits groupes + discussion en classe	Google search

Contenu par étape	Travail en classe	Média
Explication : Un ordinateur peut être contaminé de différentes façons : Par des sites internet ordinaires eux-mêmes contaminés. **1.** Par des logiciels qui ne sont pas mis à jour : mettez donc toujours bien à jour les logiciels de votre ordinateur, tablette et/ou smartphone dès que vous êtes invité à le faire. **2.** Par des pièces jointes infectées d'un e-mail : **a.** L'e-mail vous est envoyé automatiquement par des membres de la famille ou des amis dont l'ordinateur est lui-même infecté. **b.** Vous recevez l'e-mail d'un expéditeur souvent inconnu et il est accompagné d'une pièce jointe sur laquelle il faut cliquer. **3.** Par des comptes de réseaux sociaux mal sécurisés. **4.** Parce que vous n'utilisez pas de programme antivirus ou de firewall. **5.** Tapez « Windows Defender » dans le champ de recherche à gauche au bas de votre écran et appuyez sur Enter. **6.** Voilà à quoi ressemble Windows Defender. **7.** Si vous voyez « Désactivé », cliquez sur « Paramètres » dans le coin supérieur droit et cochez « Activer la protection en temps réel (recommandé) ». Cliquez ensuite sur « Enregistrer les modifications ». **8.** Retournez dans le premier onglet, à la « Page de démarrage » et cliquez sur « Analyser maintenant ». Le programme identifie alors les fichiers infectés que vous pouvez supprimer. **9.** Votre ordinateur ne comporte plus aucun fichier infecté.	En classe	Annexes 1 et 2

Contenu par étape	Travail en classe	Média
Tâche : Essayez maintenant d'appliquer cette procédure sur l'ordinateur de la classe.	Travailler en petits groupes sur l'ordinateur	
Question et réponse : Que pouvez-vous faire maintenant pour mieux sécuriser votre ordinateur ? **Conseils et astuces :** **1.** N'ouvrez jamais un e-mail ou une pièce jointe qui vous semble bizarre. Par exemple : un titre qui n'a pas de sens, un e-mail sans objet, un expéditeur inconnu, des fautes dans le texte. Faites preuve de bon sens et demandez éventuellement conseil à un adulte. **2.** Dans un e-mail ou un post sur un réseau social, ne cliquez jamais sur un lien qui vous semble bizarre. Demandez toujours à l'expéditeur si c'est bien lui qui l'a envoyé. **3.** Si vous devez introduire des données personnelles sur un site internet, vérifiez toujours si https:\\ figure dans le lien, en haut dans la fenêtre du navigateur. Si c'est bien le cas, vous êtes sûr que le site est sécurisé et que vos données sont entre de bonnes mains.	Question et réponse + Conclusion en classe avec les astuces	

Partie 4 : Créer un mot de passe fort

> **Quelques mots d'explication**
> Le choix d'un mot de passe fort est un aspect très important de la sécurité en ligne. De cette manière, les cybercriminels ont beaucoup plus de mal à s'introduire dans votre ordinateur, tablette et/ou smartphone. Certains sites internet et applications vont encore plus loin en instaurant une vérification en deux étapes.
> Dans cette partie du cours, nous allons vous expliquer la meilleure approche à l'aide de trucs et astuces.

Étape par étape

Contenu par étape	Travail en classe	Média
Question : Selon vous, qu'est-ce qu'un mot de passe FAIBLE ? **Explication :** Un mot de passe faible est un mot de passe qui est facile à deviner **1.** Votre propre nom **2.** Le nom de votre animal de compagnie **3.** Votre date de naissance **4.** Le nom de votre rue et votre numéro de maison **5.** Des séries logiques comme « abcdefg » ou « 12345678 » Ou encore : un mot de passe que vous avez noté quelque part est aussi un mot de passe faible **1.** Conseil n° 1 : n'écrivez jamais votre mot de passe sur un bout de papier, un post-it ou dans votre agenda. **2.** Conseil n° 2 : ne confiez jamais votre mot de passe à personne, même pas à votre meilleur(e) ami(e).	Travail en petits groupes + discussion en classe	Google search

Contenu par étape	Travail en classe	Média
Question : Qu'appelle-t-on alors un mot de passe FORT ? **Explication :** **1.** Un mot de passe fort se compose d'au moins 12 caractères. **2.** Il se compose d'un mélange de majuscules, minuscules, chiffres et caractères spéciaux. **3.** Il est original : MonChien@boie20Fois ! **4.** Vous le retenez par cœur. **5.** Il n'est pas unique pour toutes vos applications : vous en utilisez plusieurs. En cas de problème avec l'un d'entre eux, le mot de passe concerné ne peut pas être utilisé pour s'introduire sur vos réseaux sociaux, dans votre messagerie, vos apps, etc.	Discussion en petits groupes en classe + liste des "choses à faire"	diggit: phase 2

Contenu par étape	Travail en classe	Média
Question : Imaginez un mot de passe efficace pour vous. **Explication : Vérification en deux étapes** : Différentes plateformes, comme Facebook et Instagram vont encore un peu plus loin pour limiter les risques de sécurité, grâce à une vérification en deux étapes. Tout ça semble plus compliqué que ça ne l'est en réalité. **Un exemple avec Facebook :** **1.** Connectez-vous à Facebook et cliquez en haut à droite sur la petite flèche. **2.** Choisissez maintenant « Paramètres » et ensuite « Sécurité ». **3.** Dans « Vérification en deux étapes », cliquez sur « Configurer » et ensuite sur « Activer ». **4.** Cochez « SMS » pour recevoir votre code de sécurité sur votre GSM et cliquez sur « Suivant ». **5.** Vous recevez alors un code au numéro de téléphone que vous avez communiqué. Introduisez-le ici. Cliquez sur « Suivant ». Votre vérification en deux étapes est à présent activée ! À partir de maintenant, vous recevrez toujours un code si vous ou quelqu'un d'autre se connecte à partir d'un smartphone ou d'un ordinateur inconnu.	Discussion en classe	Annexes 3, 4, 5, 6 et 7

Partie 5 : Se protéger en ligne

> **Quelques mots d'explication**
> Dans l'univers en ligne, les enfants sont confrontés à des personnes qui ne respectent pas leurs limites, qui se comportent grossièrement ou même qui leur demandent de l'argent. Il est important qu'ils puissent en parler et obtenir de l'aide au cas où ils seraient confrontés à de telles situations. Dans cette partie du cours, nous voulons sensibiliser les élèves à un comportement assertif en ligne et leur fournir des moyens pour lutter contre la cyberintimidation ou le cyberharcèlement.

Étape par étape

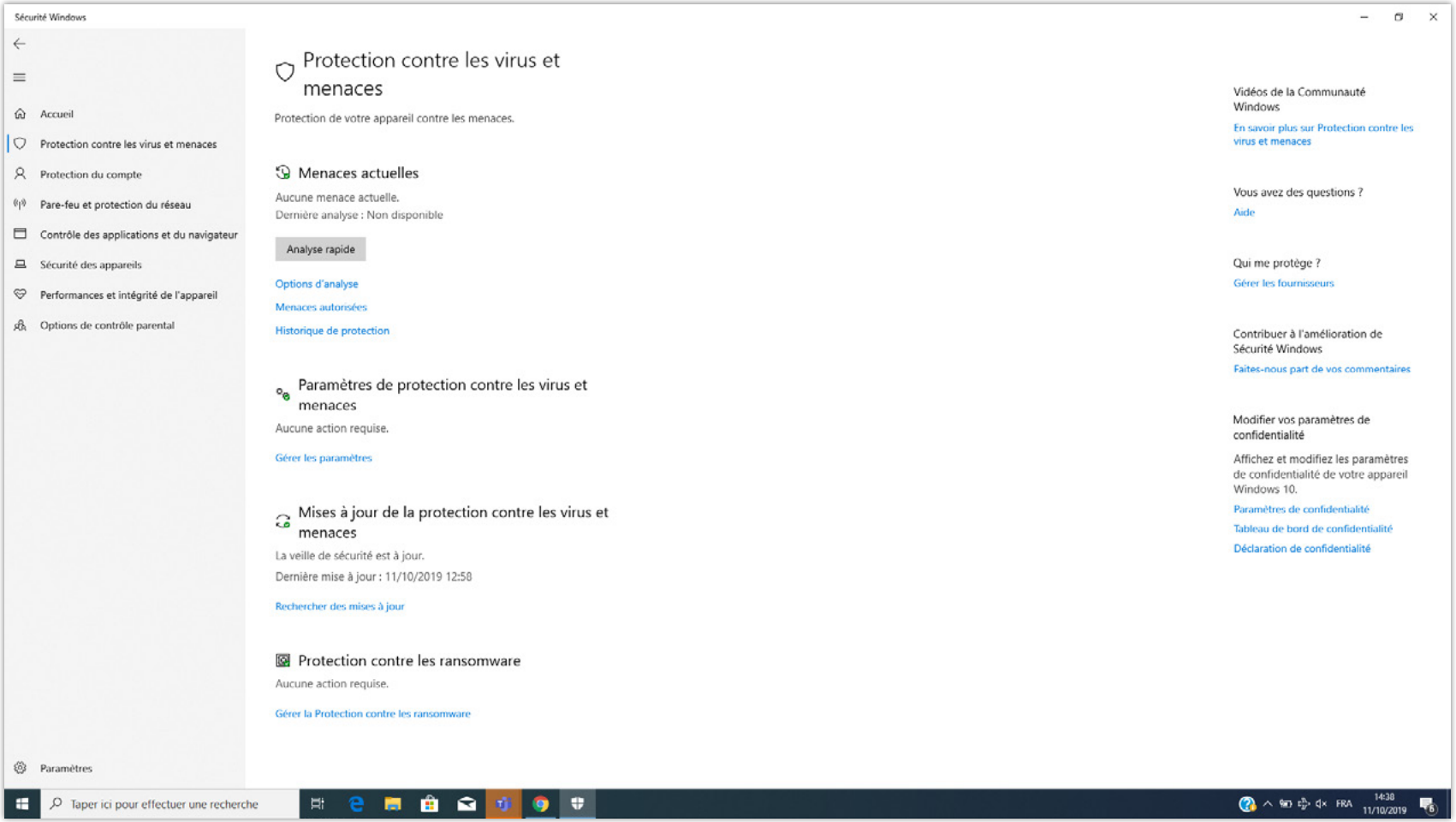
Contenu par étape	Travail en classe	Média
Question : Dans des films comme Batman et Superman il y a toujours un héros et un méchant. Le bien contre le mal. Et pour vous, sur internet qu'est-ce qui est 'bien' et qu'est-ce qui est 'mal' ? **Explication :** En ligne, vous n'avez aucune obligation, envers personne, même pas envers quelqu'un que vous avez ajouté à votre liste d'amis sur vos réseaux sociaux. En cas de doute, demandez toujours conseil à une personne en qui vous avez confiance, comme vos parents ou un professeur.	Discussion en classe + liste des "choses à (ne pas) faire"	

Contenu par étape	Travail en classe	Média
Quelques conseils et astuces supplémentaires : **1.** N'envoyez jamais de photos ou de vidéos inappropriées même si quelqu'un vous le demande (même une personne que vous connaissez très bien). **2.** Méfiez-vous des fausses informations (les fameuses « fake news »). **3.** Faites toujours preuve de bon sens quand vous lisez quelque chose qui vous semble incroyable sur les réseaux sociaux ou dans un e-mail. **Petit conseil :** Si quelque chose vous semble trop beau pour être vrai, ce n'est sans doute effectivement pas vrai !		
Question : Comment définiriez-vous le cyberharcèlement ?	Travail en petits groupes	
Tâche : Surfez sur le site de Child Focus et cherchez comment signaler un cas de cyberharcèlement.	Travail en petits groupes sur ordinateur 1 groupe fait une proposition, les autres peuvent compléter cette proposition.	

Contenu par étape	Travail en classe	Média
Explication : Il existe différentes possibilités pour signaler un cyberharcèlement : **1.** Vous trouverez une oreille attentive et une personne de confiance chez Child Focus : sur leur site internet, en téléphonant au numéro gratuit 116000, par e-mail ou sur leur compte Facebook. **2.** Sur le site internet www.103ecoute.be vous pouvez envoyer un e-mail ou chatter avec quelqu'un. Vous pouvez aussi leur téléphoner au numéro gratuit 103. **3.** Vous pouvez aussi surfer sur les plateformes des réseaux sociaux. Sur Facebook, par exemple, vous pouvez non seulement signaler les comportements de harcèlement, mais aussi demander de l'aide à un parent, un ami ou un professeur.	En classe	Annexes 8, 9 et 10

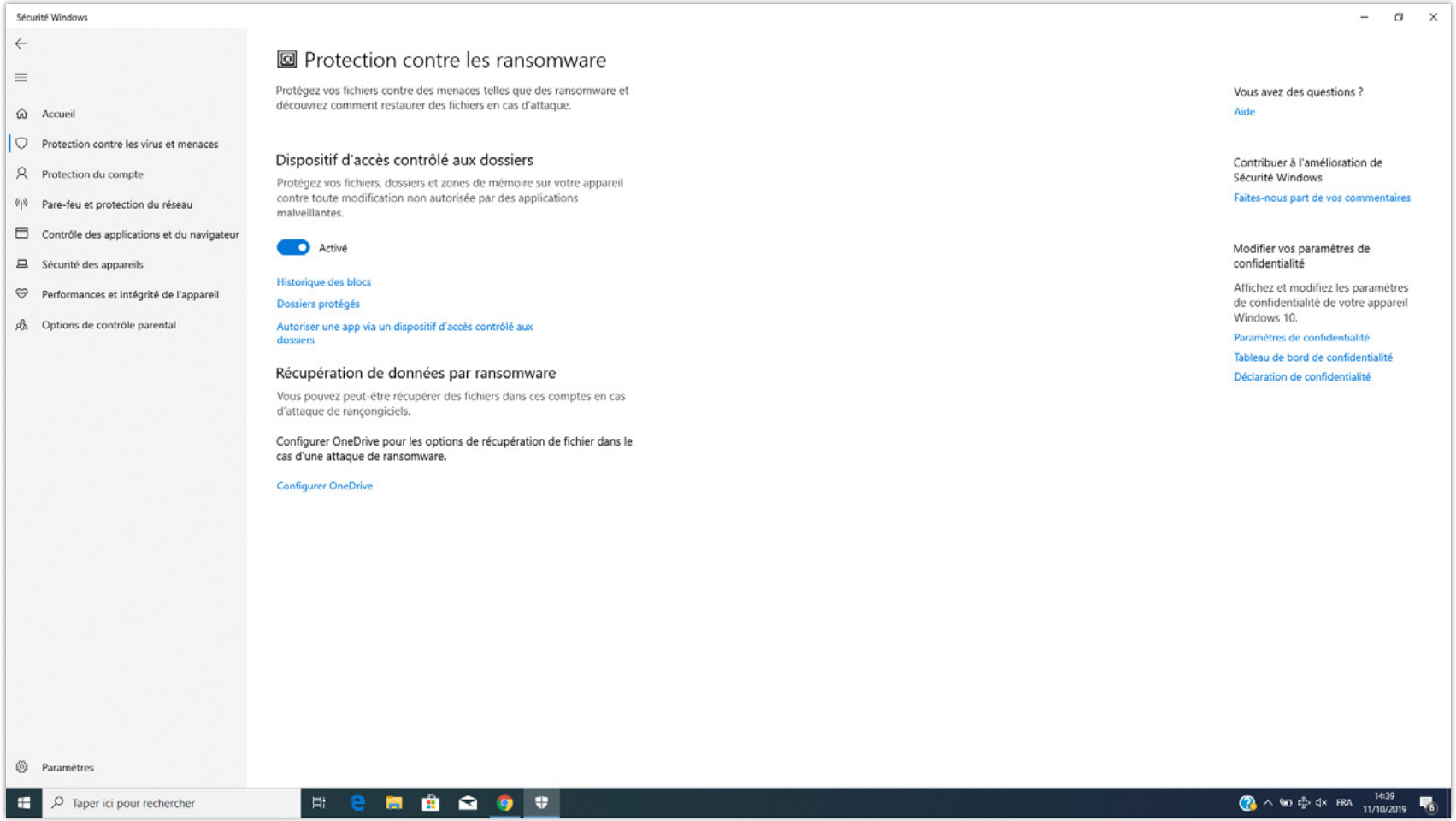
Annexes

1.


Sécurité Windows
Accueil
Protection contre les virus et menaces
Protection du compte
Pare-feu et protection du réseau
Contrôle des applications et du navigateur
Sécurité des appareils
Performances et intégrité de l'appareil
Options de contrôle parental
Paramètres
Protection contre les virus et menaces
Protection de votre appareil contre les menaces.
Menaces actuelles
Aucune menace actuelle.
Dernière analyse : Non disponible
Analyse rapide
Options d'analyse
Menaces autorisées
Historique de protection
Paramètres de protection contre les virus et menaces
Aucune action requise.
Gérer les paramètres
Mises à jour de la protection contre les virus et menaces
La veille de sécurité est à jour.
Dernière mise à jour : 11/10/2019 12:58
Rechercher des mises à jour
Protection contre les ransomware
Aucune action requise.
Gérer la Protection contre les ransomware
Vidéos de la Communauté Windows
En savoir plus sur Protection contre les virus et menaces
Vous avez des questions ?
Aide
Qui me protège ?
Gérer les fournisseurs
Contribuer à l'amélioration de Sécurité Windows
Faites-nous part de vos commentaires
Modifier vos paramètres de confidentialité
Affichez et modifiez les paramètres de confidentialité de votre appareil Windows 10.
Paramètres de confidentialité
Tableau de bord de confidentialité
Déclaration de confidentialité
Taper ici pour effectuer une recherche
FRA
14:38
11/10/2019

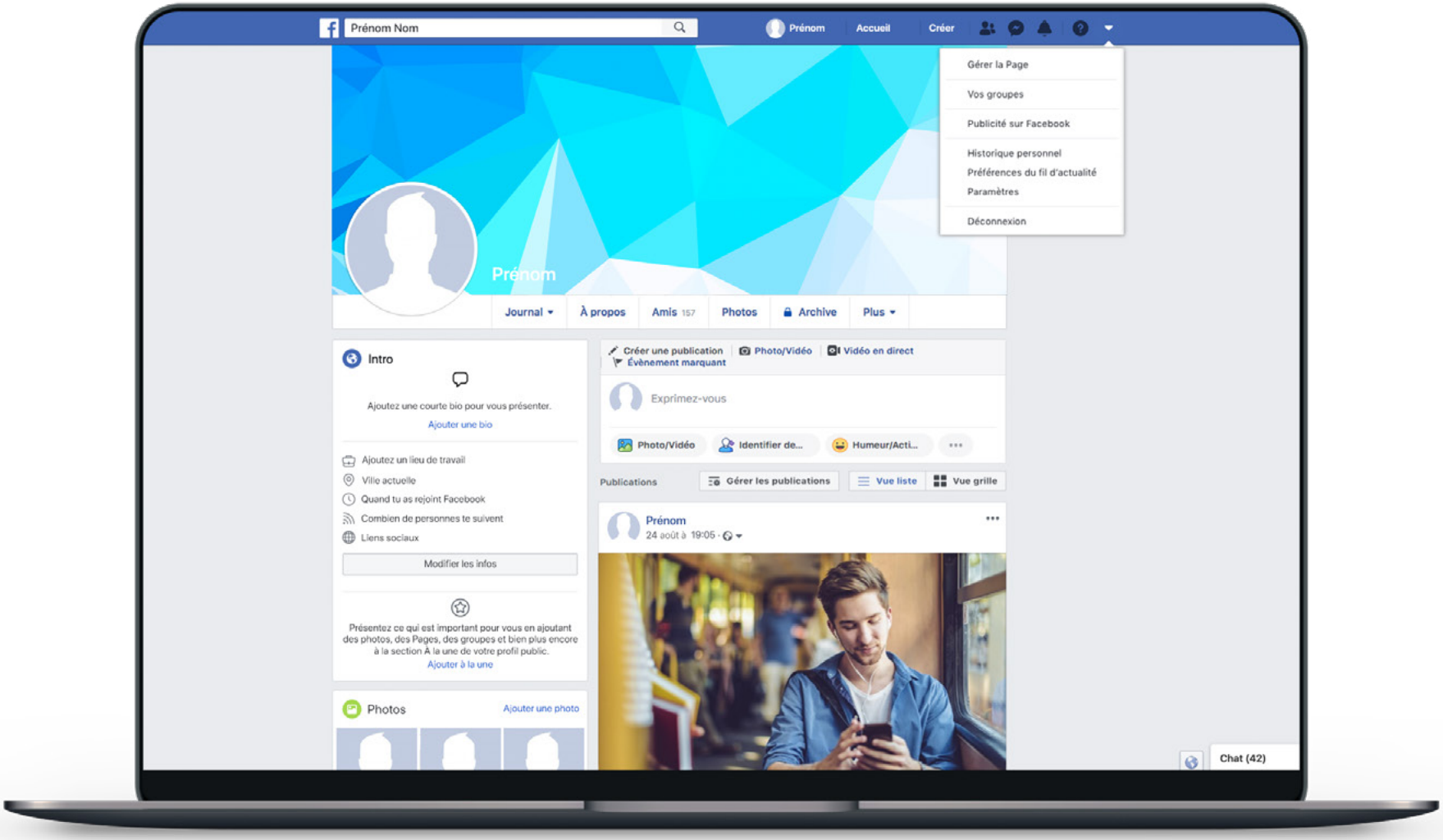
Annexes

2.


Sécurité Windows
Protection contre les ransomware
Protégez vos fichiers contre des menaces telles que des ransomware et découvrez comment restaurer des fichiers en cas d'attaque.
Accueil
Protection contre les virus et menaces
Protection du compte
Pare-feu et protection du réseau
Contrôle des applications et du navigateur
Sécurité des appareils
Performances et intégrité de l'appareil
Options de contrôle parental
Paramètres
Dispositif d'accès contrôlé aux dossiers
Protégez vos fichiers, dossiers et zones de mémoire sur votre appareil contre toute modification non autorisée par des applications malveillantes.
Activé
Historique des blocs
Dossiers protégés
Autoriser une app via un dispositif d'accès contrôlé aux dossiers
Récupération de données par ransomware
Vous pouvez peut-être récupérer des fichiers dans ces comptes en cas d'attaque de rançongiciels.
Configurer OneDrive pour les options de récupération de fichier dans le cas d'une attaque de ransomware.
Configurer OneDrive
Vous avez des questions ?
Aide
Contribuer à l'amélioration de Sécurité Windows
Faites-nous part de vos commentaires
Modifier vos paramètres de confidentialité
Affichez et modifiez les paramètres de confidentialité de votre appareil Windows 10.
Paramètres de confidentialité
Tableau de bord de confidentialité
Déclaration de confidentialité
Taper ici pour rechercher
FRA
14:39
11/10/2019

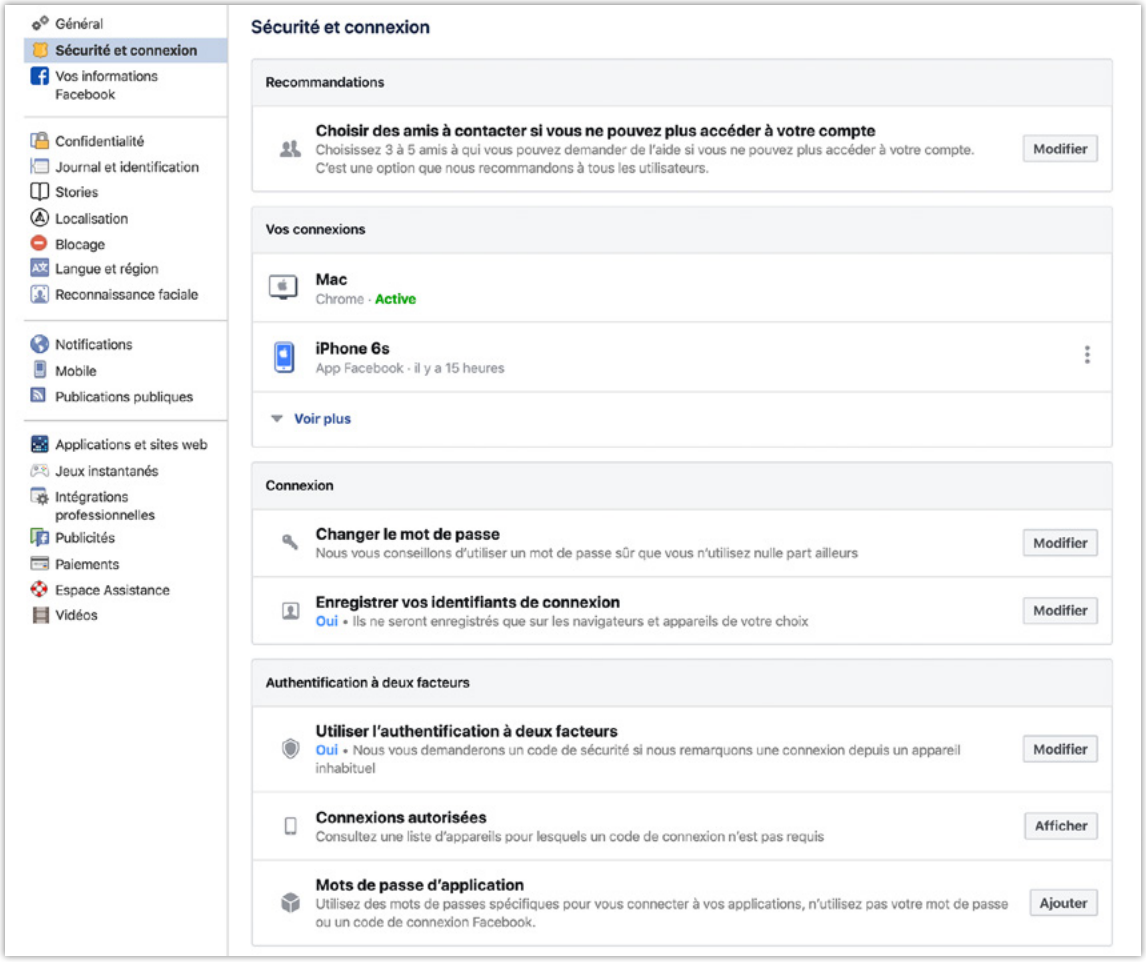
Annexes

3.


Prénom Nom
Prénom
Accueil
Créer
Gérer la Page
Vos groupes
Publicité sur Facebook
Historique personnel
Préférences du fil d'actualité
Paramètres
Déconnexion
Prénom
Journal
À propos
Amis 157
Photos
Archive
Plus
Intro
Ajoutez une courte bio pour vous présenter.
Ajouter une bio
Ajoutez un lieu de travail
Ville actuelle
Quand tu as rejoint Facebook
Combien de personnes te suivent
Liens sociaux
Modifier les infos
Présentez ce qui est important pour vous en ajoutant des photos, des Pages, des groupes et bien plus encore à la section À la une de votre profil public.
Ajouter à la une
Photos
Ajouter une photo
Créer une publication
Photo/Vidéo
Vidéo en direct
Événement marquant
Exprimez-vous
Photo/Vidéo
Identifier de...
Humeur/Acti...
Publications
Gérer les publications
Vue liste
Vue grille
Prénom
24 août à 19:05
Chat (42)

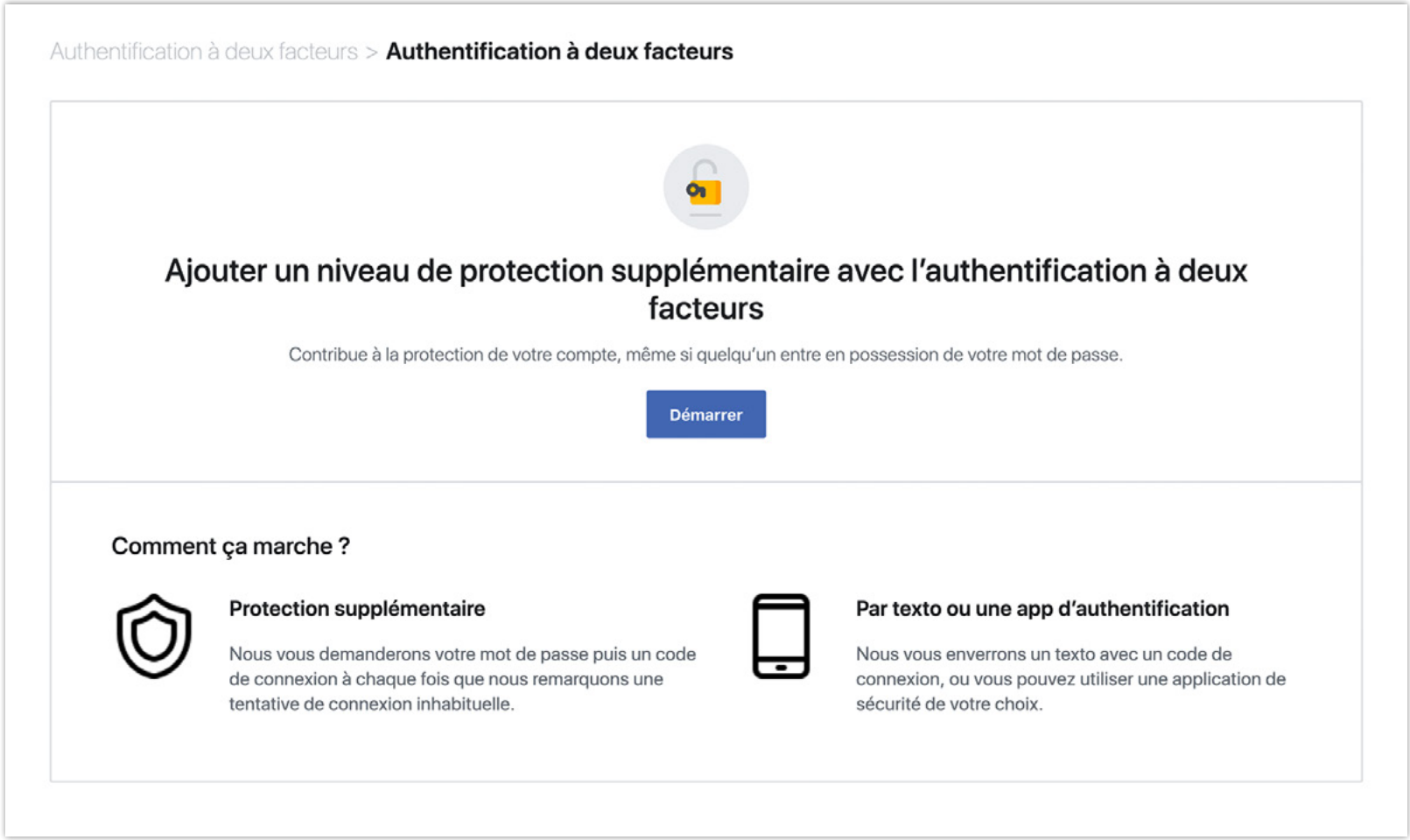
Annexes

4.


Général
Sécurité et connexion
Vos informations Facebook
Confidentialité
Journal et identification
Stories
Localisation
Blocage
Langue et région
Reconnaissance faciale
Notifications
Mobile
Publications publiques
Applications et sites web
Jeux instantanés
Intégrations professionnelles
Publicités
Paiements
Espace Assistance
Vidéos
Sécurité et connexion
Recommandations
Choisir des amis à contacter si vous ne pouvez plus accéder à votre compte
Choisissez 3 à 5 amis à qui vous pouvez demander de l'aide si vous ne pouvez plus accéder à votre compte. C'est une option que nous recommandons à tous les utilisateurs.
Modifier
Vos connexions
Mac
Chrome · Active
iPhone 6s
App Facebook · il y a 15 heures
Voir plus
Connexion
Changer le mot de passe
Nous vous conseillons d'utiliser un mot de passe sûr que vous n'utilisez nulle part ailleurs
Modifier
Enregistrer vos identifiants de connexion
Oui • Ils ne seront enregistrés que sur les navigateurs et appareils de votre choix
Modifier
Authentification à deux facteurs
Utiliser l'authentification à deux facteurs
Oui • Nous vous demanderons un code de sécurité si nous remarquons une connexion depuis un appareil inhabituel
Modifier
Connexions autorisées
Consultez une liste d'appareils pour lesquels un code de connexion n'est pas requis
Afficher
Mots de passe d'application
Utilisez des mots de passes spécifiques pour vous connecter à vos applications, n'utilisez pas votre mot de passe ou un code de connexion Facebook.
Ajouter

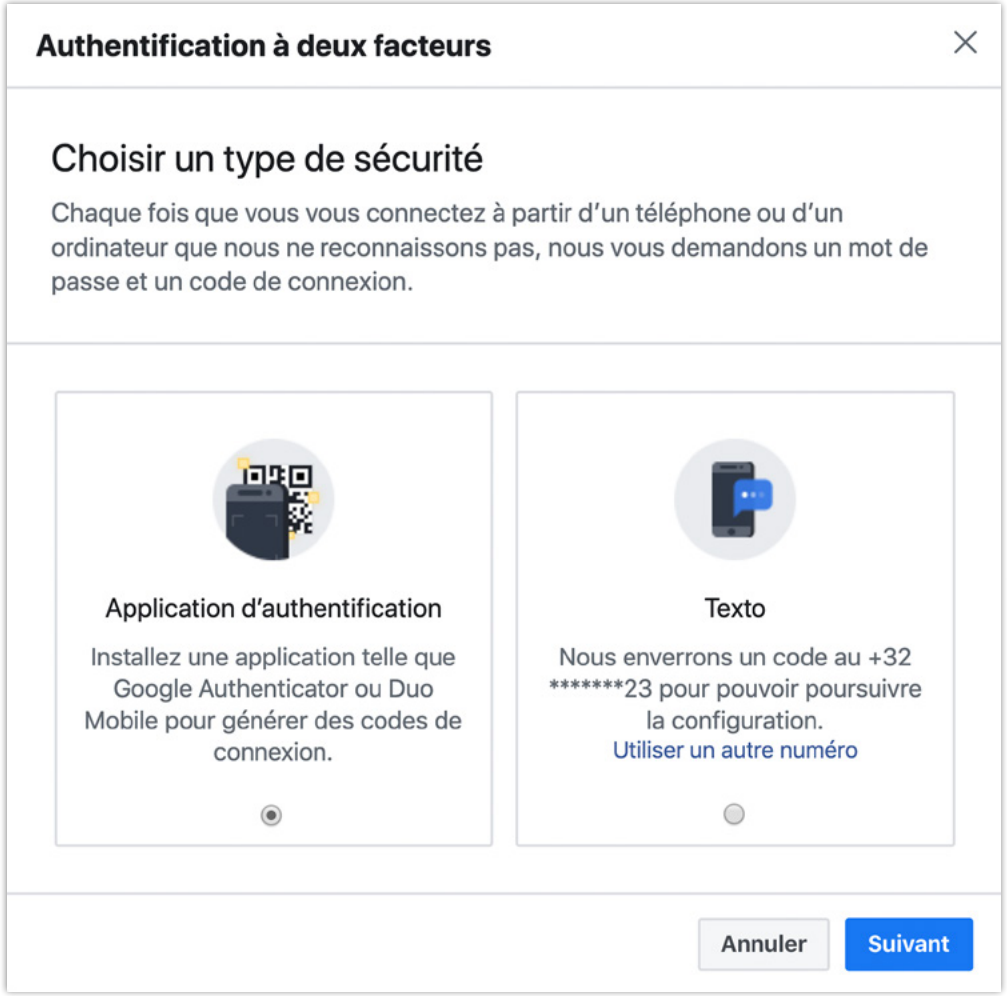
Annexes

5.


Authentification à deux facteurs > Authentification à deux facteurs
Ajouter un niveau de protection supplémentaire avec l'authentification à deux facteurs
Contribue à la protection de votre compte, même si quelqu'un entre en possession de votre mot de passe.
Démarrer
Comment ça marche ?
Protection supplémentaire
Nous vous demanderons votre mot de passe puis un code de connexion à chaque fois que nous remarquons une tentative de connexion inhabituelle.
Par texto ou une app d'authentification
Nous vous enverrons un texto avec un code de connexion, ou vous pouvez utiliser une application de sécurité de votre choix.

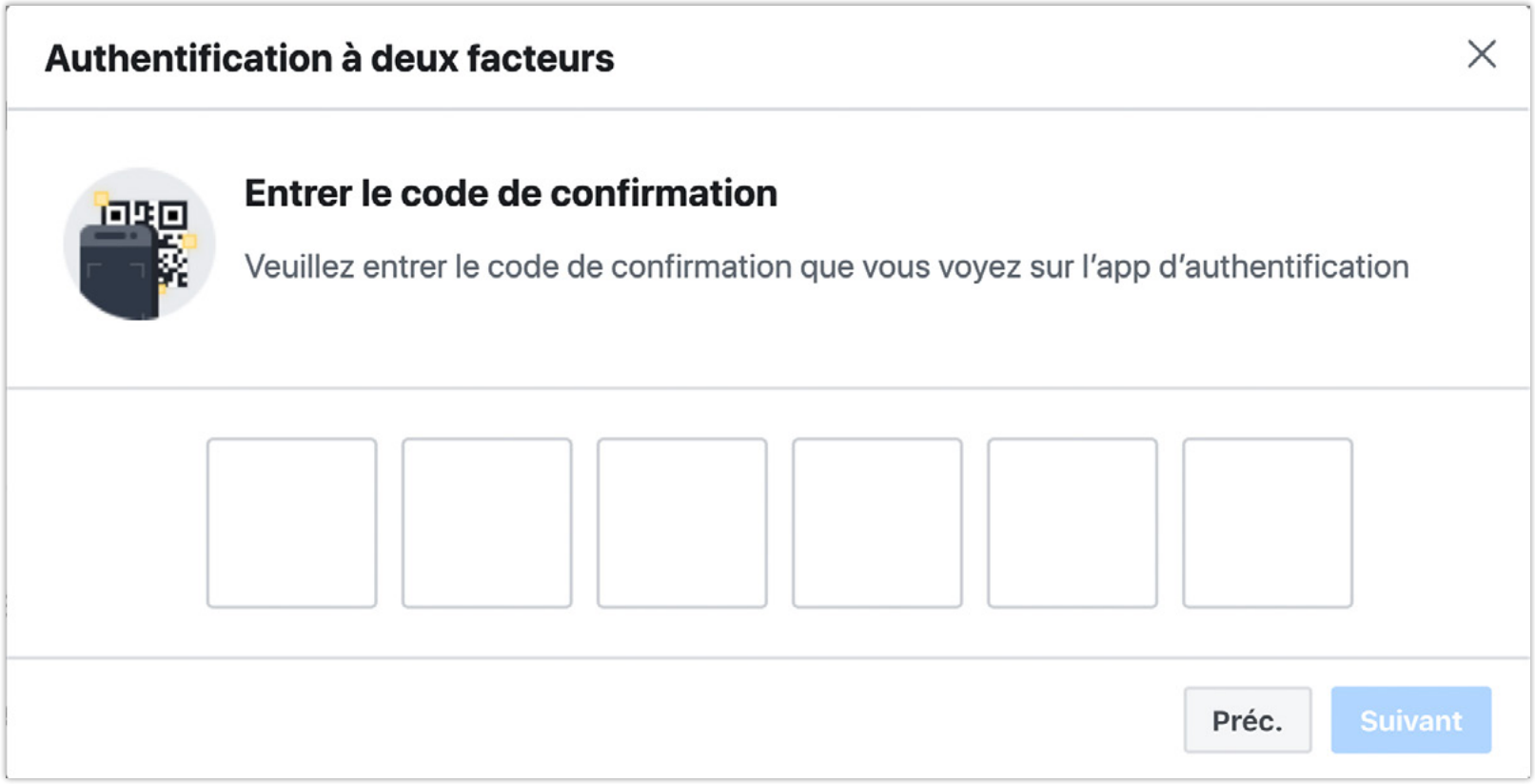
Annexes

6.


Authentification à deux facteurs
Choisir un type de sécurité
Chaque fois que vous vous connectez à partir d'un téléphone ou d'un ordinateur que nous ne reconnaissons pas, nous vous demandons un mot de passe et un code de connexion.
Application d'authentification
Installez une application telle que Google Authenticator ou Duo Mobile pour générer des codes de connexion.
Texto
Nous enverrons un code au +32 *******23 pour pouvoir poursuivre la configuration.
Utiliser un autre numéro
Annuler
Suivant

Annexes

7.


Authentification à deux facteurs
Entrer le code de confirmation
Veuillez entrer le code de confirmation que vous voyez sur l'app d'authentification
Préc.
Suivant

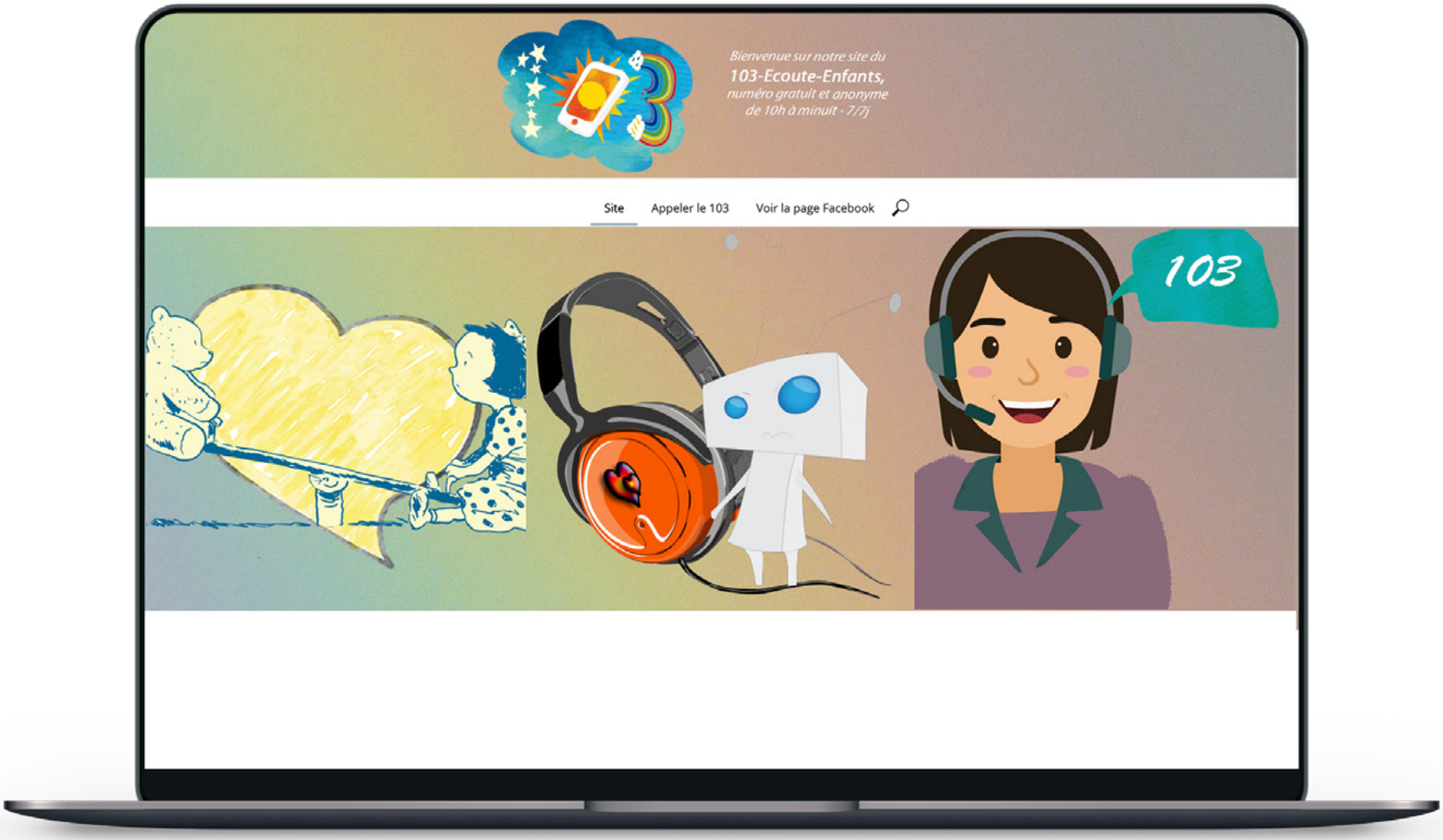
Annexes

8.


NL | FR
A propos de nous | FAQs | News | Media Center | Contact | Garanties de qualité | Jobs | Partenariat | Volontariat
Child Focus
116000
Fondation pour Enfants Disparus et Sexuellement Exploités
Cherchez sur le site
Disparitions
Exploitation sexuelle
Prévention
Volontariat
Formations
Besoin d'aide?
Je donne
Child Focus est là pour vous aider !
Appelez le 116000 (7/7 24/24)
Nous contacter par Facebook
Envoyez un mail à un collaborateur
Prevention » Securité en ligne » Adolescents » Un problème sur Internet ?
Mes parents me tappent sur les nerfs !!
Mes potes en ligne
Sexe & Internet
Ta responsabilité
Ta réputation
Trop beau pour être vrai ?
Un problème !?
Notre ligne d'aide
Quelqu'un te pose un problème ?
Retirer du contentu d'Internet?
Ton compte hacké…
Un problème sur Internet ?
Si quelque chose te dérange ou te met mal à l'aise en ligne et que t'as déjà essayé de résoudre la situation par toi-même mais que cela continue : parles-en sincèrement à quelqu'un.
Que ce soit un internaute qui te harcèle, que ce soit ton compte qui ait été hacké ou quelqu'un qui te manque de respect en postant des photos ridicules sur les réseaux sociaux… ne reste pas avec ce poids surtout si tu sens que ça devient vraiment pénible. Tourne-toi vers un pote, une copine, tes frères et sœurs ou un cousin. Bref, regarde ce que vous pouvez faire ensemble pour remédier au problème. Le mieux c'est d'en parler aussi à un adulte en qui tu as confiance : tes parents, un oncle, ta grand-mère (hé qui sait ;-), un prof ou un éducateur… Exprime-lui ce que tu ressens et insiste bien sur le fait que si tu lui en parles c'est parce que tu lui fais confiance. Tu penses peut-être qu'ils ne trouveront pas une solution miracle mais tu serais bien étonné. Ils pourront sûrement t'aider et te conseiller.
En parler...
L'essentiel est que tu ne restes pas seul avec ton problème. Parles-en à quelqu'un en qui tu as confiance.
Tu peux aussi trouver une écoute attentive et de confiance via la ligne d'aide de Child Focus (lien vers bouton aide) . Tu recevras des conseils et tu auras l'occasion de discuter avec un collaborateur de Child Focus de manière anonyme afin de voir ce que qui est possible de faire pour te sortir de ton problème.
Enfin, il existe d'autres organisations qui pourront t'aider, t'informer et t'accompagner comme :
SOS Jeunes (www.sosjeunes.be) qui accueille des jeunes en difficulté, les écoute en toute confiance, les informe et les aide grâce à un

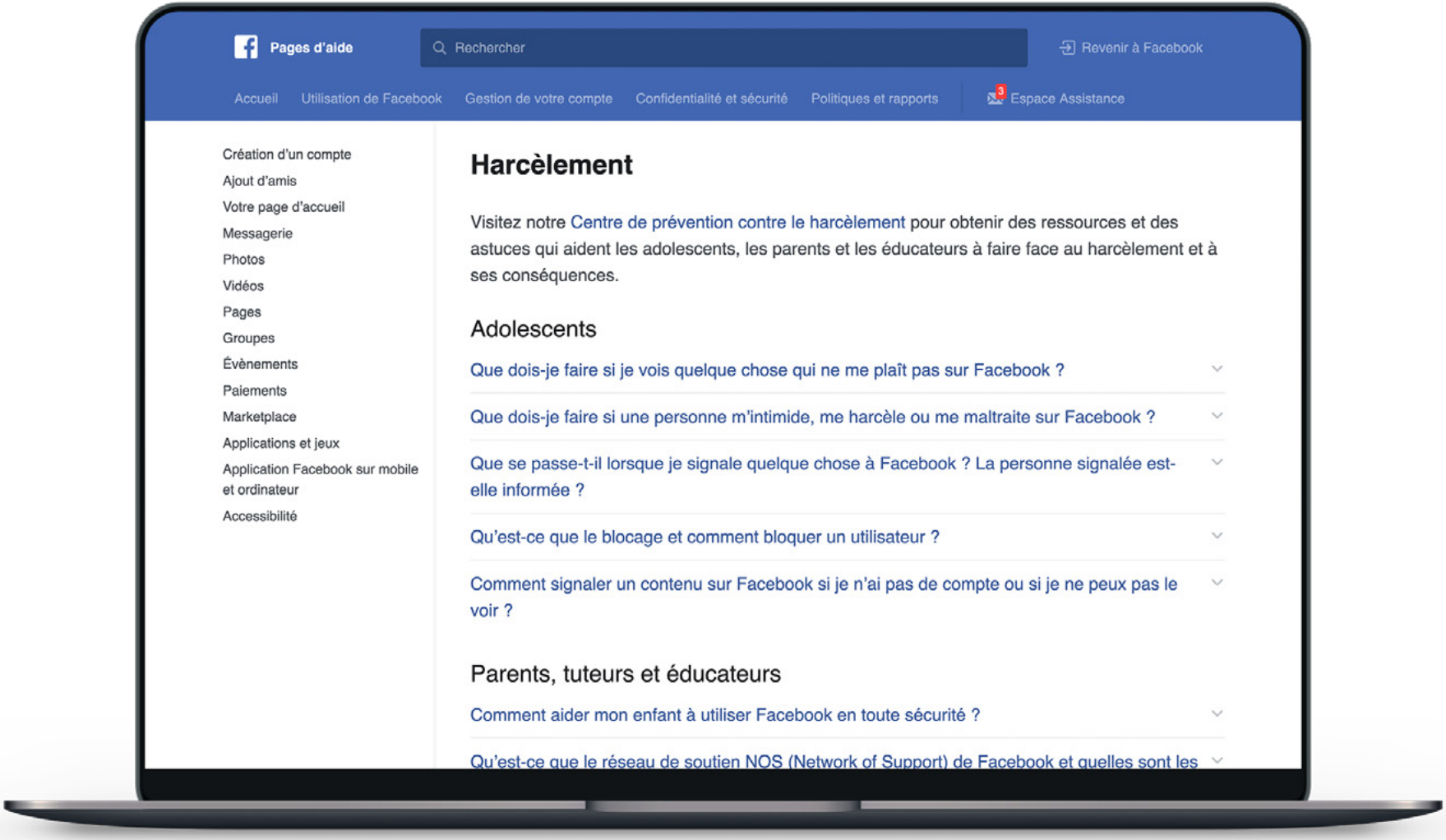
Annexes

9.


Bienvenue sur notre site du
103-Ecoute-Enfants,
numéro gratuit et anonyme
de 10h à minuit - 7/7j
Site
Appeler le 103
Voir la page Facebook
103

Annexes

10.


Pages d'aide
Rechercher
Revenir à Facebook
Accueil
Utilisation de Facebook
Gestion de votre compte
Confidentialité et sécurité
Politiques et rapports
Espace Assistance
Création d'un compte
Ajout d'amis
Votre page d'accueil
Messagerie
Photos
Vidéos
Pages
Groupes
Évènements
Paiements
Marketplace
Applications et jeux
Application Facebook sur mobile et ordinateur
Accessibilité
Harcèlement
Visitez notre Centre de prévention contre le harcèlement pour obtenir des ressources et des astuces qui aident les adolescents, les parents et les éducateurs à faire face au harcèlement et à ses conséquences.
Adolescents
Que dois-je faire si je vois quelque chose qui ne me plaît pas sur Facebook ?
Que dois-je faire si une personne m'intimide, me harcèle ou me maltraite sur Facebook ?
Que se passe-t-il lorsque je signale quelque chose à Facebook ? La personne signalée est-elle informée ?
Qu'est-ce que le blocage et comment bloquer un utilisateur ?
Comment signaler un contenu sur Facebook si je n'ai pas de compte ou si je ne peux pas le voir ?
Parents, tuteurs et éducateurs
Comment aider mon enfant à utiliser Facebook en toute sécurité ?
Qu'est-ce que le réseau de soutien NOS (Network of Support) de Facebook et quelles sont les