MINISTÈRE
DE L'ÉDUCATION
NATIONALE,
DE L'ENSEIGNEMENT
SUPÉRIEUR
ET DE LA RECHERCHE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention
en cybersécurité

Support pédagogique :

« Le numérique, pas de panique !

Ton petit guide de sécurité sur Internet. »

Préambule à destination des enseignants

Dans un monde de plus en plus tourné vers le tout numérique, les jeunes reçoivent leur 1er smartphone à 11 ans et tablette à 9 ans et sont particulièrement exposés aux risques numériques.

Face à ce constat, le dispositif national d'assistance et de prévention Cybermalveillance.gouv.fr a créé le livret « Le numérique, pas de panique ! » avec le soutien de l'AFNIC et en collaboration avec Bayard Media Développement, afin de sensibiliser les plus jeunes aux bons réflexes à adopter.

Le Ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche a souhaité s'associer à cette démarche pour favoriser la diffusion de ces enseignements essentiels.

Le présent support pédagogique a été construit autour du livret « Le numérique, pas de panique !» spécifiquement pour le corps enseignant afin de l'accompagner dans ce projet de sensibilisation.

Cette présentation peut être découpée en 3 séquences :
1- diapositives 4 à 11 (environ 45mn)
2- diapositives 12 à 16 (environ 45mn)
3- diapositives 17 à 23 (environ 35mn)

Chaque introduction de chapitre propose des questions pour initier l'échange avec les élèves de manière ouverte avant d'approfondir le sujet.

Version numérique du livret

SOMMAIRE

C’est quoi Internet ?

Qui peut me dire ce qu'est Internet ?
Utilisez-vous Internet à la maison ?
Pour quel type d’activité ?

Internet

C'est un réseau informatique à l'échelle mondiale.
Les utilisateurs d'Internet sont appelés les internautes.

A quoi sert Internet ?

- À la consultation d'informations
- À la messagerie instantanée (WhatsApp, Signal, Discord...)
- Aux réseaux sociaux (Snapchat, Instagram, TikTok, Youtube, Twitch...)
- Aux jeux vidéos en ligne
- Aux vidéos et musiques en direct « streaming » (Netflix, Disney+, Spotify, Deezer, Apple Music...)
- À l'envoi ou à la réception de courrier électronique (mail)
- Au transfert de fichiers (photos, vidéos...)

« Où en es-tu avec Internet ? » (cf Livret jeunes Bayard)

Coche les réponses qui te ressemblent le plus,
et compte combien tu as de ★ et de ●
pour découvrir ton profil d'internaute !

1/ Un ami te demande le mot de passe d'un de tes comptes :

★ Tu lui fais jurer de ne le dire à personne.

● Pas question, c'est privé !

2/ Tu es sur ton jeu vidéo préféré lorsqu'un inconnu t'envoie un message :

● Tu l'ignores et tu en parles à un adulte.

★ Tu lui réponds juste une fois par curiosité.

3/ Ton cousin doit choisir un mot de passe pour son compte Amstragram, tu lui conseilles :

★ Un truc facile à retenir comme 1234 ou SOLEIL.

● Un mot de passe compliqué avec des lettres, des chiffres et des signes.

4/ Sur un site, on te demande ton adresse pour recevoir un cadeau :

● Tu demandes l'accord de tes parents.

★ Tu la donnes : pas le choix si tu veux ton cadeau.

5/ On insulte ton grand frère sur TokTok, que doit-il faire ?

● Il doit en parler à ses parents et bloquer la personne qui l'a insulté pour qu'elle ne puisse plus lui envoyer de message ni voir son profil.

★ Pas question qu'il se laisse faire : tu l'aides à trouver les mots pour se défendre.

Test

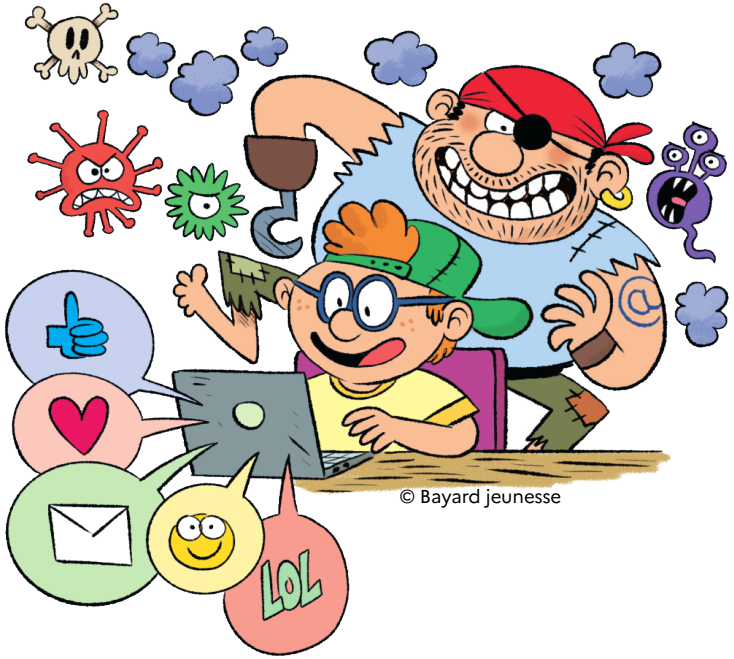
Quel est ton profil d'internaute ?

Tu as une majorité de ★ :

Internet, ça te plaît, mais tu prends souvent des risques.
Alors apprends les bons réflexes.

Tu as une majorité de ● :

Tu connais déjà les règles de prudence, bravo.
Continue comme ça et découvre encore plus d'astuces.



C’est quoi la cybersécurité ?

D’après-vous qu’est-ce-que c’est ?

La cybersécurité

C'est la sécurité sur Internet et celle de tes appareils connectés (téléphone, tablette, ordinateur…). C'est comme une « **armure** » pour Internet qui te protège de tout ce qui pourrait venir gâcher tes activités en ligne.

Sur Internet, il y a des dangers comme les **« pirates informatiques »** qui peuvent voler des informations ou piéger tes appareils avec des virus pour empêcher leur bon fonctionnement.

Tout ceci peut être évité en ayant simplement le **bon comportement et en parlant de ce qui te dérange** avec tes parents, enseignants ou un adulte de confiance comme on le ferait dans une équipe.

Une vidéo sur la « cybersécurité » pour y voir plus clair

Qu'est-ce qu'un virus informatique ?

Un **virus informatique**, c'est un petit programme « malveillant » qui peut **abîmer un appareil** ou **voler des informations**. Il se cache souvent dans des fichiers ou des sites Internet, et il peut **se copier tout seul** pour aller dans d'autres appareils.
*C'est un peu comme un **microbe** !*

Qui sont les pirates informatiques ?

Qui sont-ils?
Pourquoi nous attaquent-ils?
Comment font-ils?

Qui sont les pirates informatiques ?

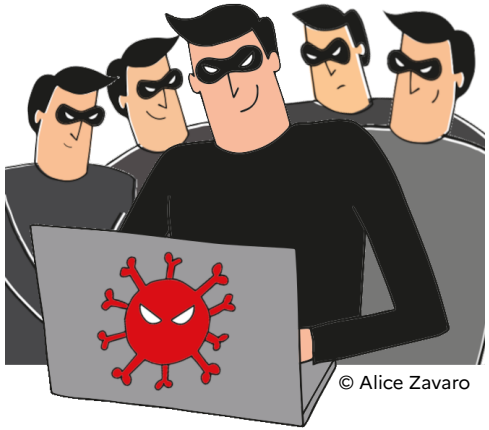
- Des amateurs ou des cybercriminels
- Des pirates « vengeurs » ou malveillants pour des raisons personnelles
- Des « Cyberhacktivistes » qui attaquent au nom d'idées politiques

Pourquoi nous attaquent-ils ?

- L'amusement ou le défi technique à relever
- Le sentiment de puissance, l'influence
- Faire du mal, du tort à quelqu'un (cyberharcèlement)
- L'argent
- L'idéologie

Comment font-ils ?

- En piégeant des personnes avec des mails, messages directs (DM), QR-codes ou SMS d'arnaque (hameçonnage) qui les mènent vers des **faux sites** (ressemblant aux vrais) pour récupérer leurs **informations** et **mots de passe**.
- En utilisant des « **virus** » qu'ils déposent sur des sites Internet ou cachent dans des programmes.



© Alice Zavaro

Une vidéo sur « l'hameçonnage (phishing) » pour y voir plus clair

Comment naviguer en sécurité sur Internet ?

Quels sont les risques ?
Que doit-on faire ou ne pas faire pour être en sécurité sur Internet ?

Quand je navigue sur Internet

Quels sont les risques ?

- **Les arnaques** par des sites Internet, des emails, messages directs (DM) ou SMS frauduleux pour récupérer identifiants et mots de passe (aussi appelé « Hameçonnage »).

- **Les virus** peuvent infecter un ordinateur suite à l'installation d'un programme malveillant, un clic sur un lien douteux ou l'insertion d'une clef USB non fiable. Ils peuvent alors voler des données sur l'ordinateur.

- **Les contenus choquants** : voir des images choquantes, interdites aux mineurs, peut te perturber.

Quelles sont les bonnes pratiques ?

- Cliquer uniquement sur les liens que tu connais
- Utiliser des mots de passe forts et uniques pour chaque compte
- Ne pas communiquer d'informations personnelles (nom, prénom, adresse, email, numéro de téléphone)

- Aller uniquement sur des sites officiels
- Ne pas enregistrer tes mots de passe dans le navigateur qui n'a pas de sécurité pour les protéger

- Respecter l'âge recommandé
- Ne pas tricher sur ton âge quand un site le demande
- Demander à tes parents au moindre doute sur le contenu d'un site

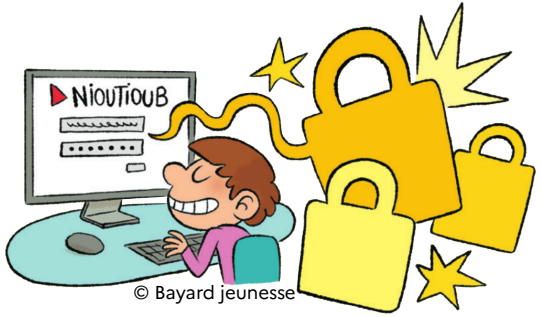
Comment créer mes mots de passe ?

- Qu'est ce qu'un mot de passe « fort » ?
C'est un mot de passe impossible à deviner pour les pirates informatiques.
Idéalement : 12 caractères minimum, mélangeant les lettres majuscules, minuscules, chiffres et caractères spéciaux.
(Ne jamais mettre de données personnelles : date naissance, prénom, nom etc.)

- Pourquoi en avoir des différents pour chaque site ?
Si un pirate récupérait ton mot de passe il l'essaierait sur d'autres sites Internet en se connectant à ta place.
Il est donc important de ne pas utiliser le même partout !

- Astuce pour les créer avec la « Méthode phonétique »
Prendre une phrase de ton choix (titre de chanson, de BD, livre …) que tu transformes en ajoutant des majuscules, des symboles et chiffres.

Exemple : Tintin au Tibet → « #T1t1oTibet! »



- Activité individuelle à faire en classe :
Chaque élève doit se créer un mot de passe en utilisant la méthode.
Attention, les mots de passe créés aujourd'hui ne devront pas être utilisés par la suite.

Les réseaux sociaux

Ai-je le droit d'utiliser les réseaux sociaux ?
Quels sont les risques ?
Quelles sont les bonnes pratiques ?

Ai-je le droit d'utiliser les réseaux sociaux ?

- L'âge légal pour s'inscrire seul sur les réseaux sociaux est de 15 ans.
- Les réseaux sociaux sont interdits au moins de 13 ans.
- Une autorisation parentale est nécessaire entre 13 et 15 ans.

Quels sont les risques ?	Quelles sont les bonnes pratiques ?
- Utilisation, modification ou diffusion de tes photos à ton insu.	- Toujours demander l'autorisation de la personne dont on veut publier la photo. - Éviter de poster des photos de toi. Si quelqu'un publie une photo gênante ou humiliante de toi, parles-en à un adulte.
- Messages répétés de menaces ou d'injures « cyberharcèlement ».	- Paramétrer tes comptes en « privé » pour limiter l'accès aux personnes que tu souhaites. - Si tu es victime ou témoin de harcèlement ou de violences en ligne, contacte le **3018** (E-enfance).
- Être contacté par un adulte malintentionné se faisant passer pour un enfant.	- Ne pas accepter comme ami les gens que tu ne connais pas ou pas bien. - En parler à tes parents ou un adulte de confiance.

Une vidéo sur les « réseaux sociaux » pour y voir plus clair

Insulter ou menacer une personne en ligne est interdit par la loi.

Comment jouer en ligne en toute sécurité ?

Quels sont les risques ?
Quelles sont les bonnes pratiques ?

Quand je joue en ligne

Quels sont les risques ?

- En téléchargeant des jeux vidéos piratés, des **virus** peuvent infecter ton téléphone ou ordinateur et voler tes mots de passe, photos...

- **Des adultes malintentionnés** peuvent se faire passer pour des amis et vouloir discuter avec toi
- Communiquer ton prénom, nom ou visage peut permettre à des personnes malveillantes de te retrouver dans la vraie vie

- **Les contenus choquants** : voir des images choquantes qui ne correspondent pas à ton âge peut te perturber.

Quelles sont les bonnes pratiques ?

- Télécharger uniquement des jeux sur des sites de confiance
- Vérifier avec un adulte que c'est un site de confiance

- Faire attention avec qui tu discutes, ne raconte rien de personnel
- Utiliser systématiquement un pseudonyme (nom que tu inventes pour masquer ta vraie identité)
- Ne pas hésiter à signaler et bloquer un joueur au comportement malveillant
- Créer un « avatar » (image pour remplacer ta photo)

- Respecter et suivre le conseil du logo **PEGI** pour l'âge recommandé, cela évite d'avoir des surprises
- Parler à tes parents des contenus ayant pu te choquer

PEGI pour « Pan European Game Information » est un système composé de cinq catégories d'âge et de huit descriptions qui fournit des informations sur l'âge approprié et le type de contenu, afin de s'assurer que les jeux ne sont pas susceptibles d'heurter la sensibilité des joueurs.

Attention aux fausses informations sur Internet !

Comment appelle-t-on une fausse information diffusée volontairement sur les réseaux sociaux?

Face aux fausses informations ou « fake news »

Quelle est la bonne attitude ?

- Se méfier des titres trop accrocheurs
- Vérifier le contenu de la source et analyser son authenticité
- Vérifier les images
- Réfléchir avant de repartager
- Signaler les contenus interdits

Quelles sont les bonnes pratiques ?

- Plus un contenu fait un effet « whaou » plus il faut s'en méfier
- Croiser les informations sur différents sites (faits, chiffres, dates et contexte de la publication…)
- Faire une recherche inversée à partir d'une image ou d'une vidéo peut aider à vérifier si le contenu a déjà été utilisé dans un contexte différent
- Ne pas repartager des contenus douteux pour éviter que d'autres se fassent piéger à leur tour
- En cas de doute, il faut en parler à tes parents ou un adulte de confiance qui peuvent signaler les contenus interdits sur la plateforme « Pharos » (internet-signalement.gouv.fr)

Recommandations fournies par :

VIGINUM

En cas de problème, vers qui je me tourne ?

À qui pensez-vous en premier ?
Connaissez-vous certains organismes spécialisés ?

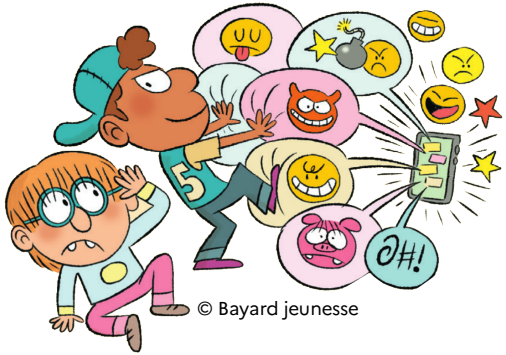
Si j'ai une question ou un problème

Je ne dois pas rester seul et en parler à un adulte, parent, grand-parent ou enseignant.

Voici des sites utiles en cas de problème :

Cybermalveillance.gouv.fr

Sur ce site, toi et tes parents pouvez apprendre **plein de bonnes pratiques pour aller sur Internet en toute (cyber) sécurité !**
Par exemple, gérer tes mots de passe, protéger tes appareils et tes comptes, apprendre à reconnaître les arnaques...



17cyber.gouv.fr

Sur ce site, **tu réponds à un questionnaire sur ta situation** (tu as reçu un mail suspect ou un appel malveillant, tu penses que tu as été piraté...), un diagnostic est établi et on donne des conseils pour agir et des contacts pour t'aider.

e-enfance.org

Victime ou témoin de harcèlement ou de violences en ligne ? Appelle le **3018** ou utilise l'**appli 3018**. C'est gratuit, anonyme et confidentiel.
Des psychologues et des juristes sont là pour t'aider de façon claire et adaptée

En synthèse :

Voici 6 conseils essentiels pour utiliser Internet en tout sécurité :

- Utilise un pseudonyme et ne révèle rien sur ta vie personnelle
- Méfie-toi des messages inattendus et alarmants
- Respecte l'âge légal pour les réseaux sociaux
- Crée des mots de passe solides et différents pour chaque compte
- Ne télécharge pas de contenus piratés ou non officiels
- Ne crois pas tout ce que tu vois sur Internet

À vous de jouer

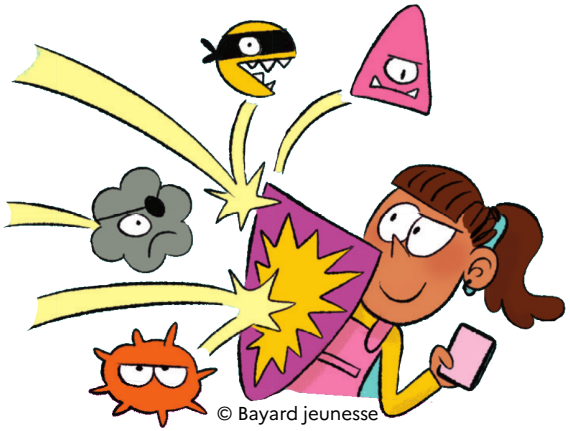
Pour partager les cyber-réflexes en classe

À vous de jouer pour partager les cyber-réflexes !

La sensibilisation à la cybersécurité n'est pas un temps fort ponctuel : c'est une démarche continue qui vise à ancrer, dès le plus jeune âge, les bons réflexes numériques.

En tant qu'enseignants, vous avez un rôle clé : prolonger cette dynamique tout au long de l'année grâce à des initiatives variées et créatives avec vos élèves – jeux, fresque, exposé, dessin, vidéo, BD, théâtre…laissez parler l'imagination !

Toutes les productions seront valorisées dès le mois d'octobre et pourront être déposées tout au long de l'année scolaire sur la page **« Éduscol – Éducation et cybersécurité »**



👉 https://eduscol.education.fr/3679/education-et-cybersecurite

Sur cette page vous trouverez également des informations et des ressources pratiques.

En partenariat avec :

MINISTÈRE
DE L'ÉDUCATION
NATIONALE,
DE L'ENSEIGNEMENT
SUPÉRIEUR
ET DE LA RECHERCHE

Liberté
Égalité
Fraternité

Réalisé par :

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention
en cybersécurité

Avec le soutien de :

afnic

Internet
made in France

Ressources

Pour trouver des ressources complémentaires :
Guides, fiches, quiz, affiches...

Risques

- L'hameconnage
    - Hameçonnage [fiche] (Cybermalveillance.gouv.fr)
    - Les arnaques du Web [vidéo] (Lumni)

- Le piratage de compte [fiche] (Cybermalveillance.gouv.fr)

- Le cyberharcèlement
    - Cyberharcèlement [fiche] (E-enfance.org - 3018)
    - Les Cliquadonffe – Episode 2, le cyberharcèlement [BD] (E-enfance.org)
    - Le site de l'Education Nationale dédié à la lutte contre le harcèlement [ressources] (education.gouv.fr)

- Les fausses informations
    - Comprendre et déjouer les mécanismes de manipulation de l’information [dossier pédagogique] (VIGINUM | Educ'ARTE)
    - Comment débusquer les manipulations de l'information : « Le débrief de Clara et Raphaël » [podcast] (VIGINUM | CLEMI)

- L'usurpation d’identité [fiche] (Cybermalveillance.gouv.fr)

Bonnes pratiques

- Les mots de passe [fiche] (Cybermalveillance.gouv.fr)
- La sécurité sur les réseaux sociaux [fiche] (Cybermalveillance.gouv.fr)
- Le « Cyber Guide Famille » [livret] (Cybermalveillance.gouv.fr)
- Tous ensemble, prudence sur Internet ! Les ressources pour les 8-10 ans et les 11-15 ans [ressources] (CNIL)
- Téléphonie mobile / Smartphones
  - La sécurité des appareils mobiles [fiche] (Cybermalveillance.gouv.fr)
  - Premier smartphone [guide famille] (Internet sans crainte)
  - « Pourquoi on est accro au téléphone ? » [atelier] (Internet sans crainte)
- Éducation et cybersécurité [ressources] (ÉDUSCOL)
- Sensibilisation des 8-12 ans « Bienvenue dans la vie numérique » : 5 séances clés en main [ateliers] (Internet sans crainte)
- Cyber reflexes [affiche] (CNIL / Cybermalveillance.gouv.fr)

Quiz

- Édition spéciale des Incollables « Deviens un super-héros du Net » [quiz] (E-enfance.org - 3018/Cybermalveillance.gouv.fr)
- Testez vos connaissances (mots de passe/hameçonnage/appareils mobiles/usages pro-perso) [quiz] (Cybermalveillance.gouv.fr)
- Les As du web [cahier activités] (Lumérique)