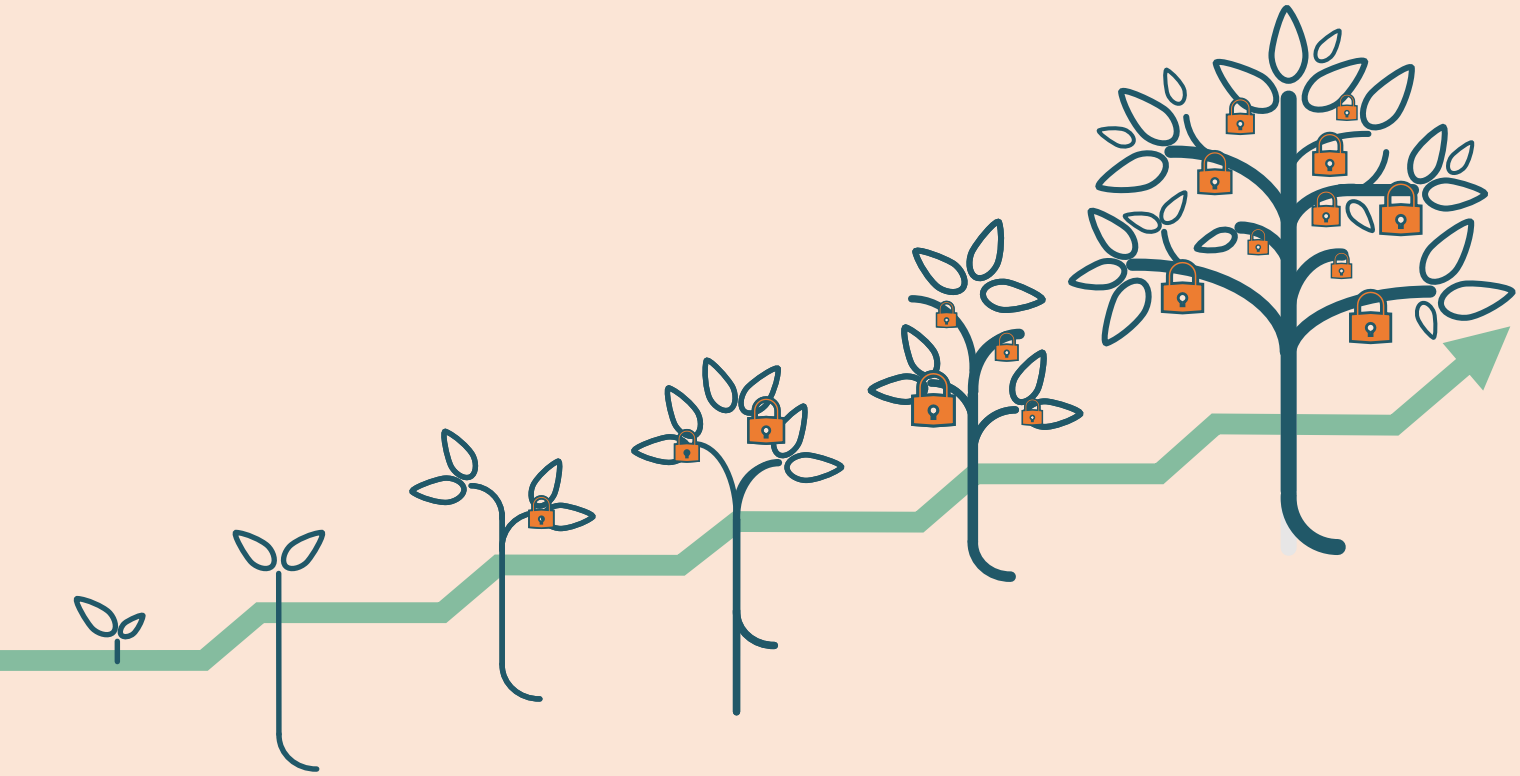
1,2,3 CYBER !

Jeu Cyber pour les 11-14 ans



1, 2, 3 Cyber **est un jeu de société sur le thème de la cybersécurité, permettant de sensibiliser les 11-14 ans de manière ludique aux risques d'Internet et aux bons réflexes et bonnes pratiques à adopter.**

CCJ

WAVESTONE

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

1, 2, 3 Cyber **est le fruit d'une collaboration entre l'association CCJ et le cabinet de conseil Wavestone, avec la participation du dispositif Cybermalveillance.**

CCJ

L'association **« Centre de la Cybersécurité pour les Jeunes »** (CCJ) a pour objectif de sensibiliser les jeunes aux enjeux de la cybersécurité, à la dynamique du cyberharcèlement ainsi qu'à l'importance de l'e-réputation. Ses objectifs sont les suivants : **organiser, animer et participer à des programmes d'éducation, de sensibilisation et de formation** ainsi qu'à des conférences traitant des sujets de la cybersécurité, du cyberharcèlement et de l'e-réputation :

- **Sensibiliser les jeunes, le corps enseignant ainsi que les médias des jeunes** aux sujets de la cybersécurité, du cyberharcèlement et de l'e-réputation
- **Sensibiliser les conseillers d'orientation** aux métiers de la cybersécurité
- Proposer **un programme de mentorat des jeunes** par des professionnels en cybersécurité
- **Nouer des partenariats** avec des organismes qui permettront au CCJ de sensibiliser les jeunes aux enjeux de la cybersécurité, à la dynamique du cyberharcèlement ainsi qu'à l'importance de l'e-réputation
- **Publier des articles et des vidéos** de sensibilisation

WAVESTONE

Au **croisement du conseil en management et du conseil en digital**, Wavestone accompagne les grandes entreprises et organisations dans leurs transformations les plus critiques avec la conviction qu'il ne peut y avoir de transformation réussie sans une culture partagée de l'enthousiasme. Wavestone constitue le 1er cabinet de conseil indépendant en France. Il rassemble plus de 3100 collaborateurs à travers le monde, dont 500 spécialisés sur les sujets de cybersécurité et confiance numérique.

Au-delà de ses opérations dans ce domaine, Wavestone **s'implique dans la sensibilisation du grand public aux risques liés au numérique** et **s'engage pour le développement d'une meilleure hygiène numérique** globale. Cet engagement se matérialise par exemple par l'implication dans l'élaboration d'un *cahier de vacances de sensibilisation des 7-11 ans* porté par l'association ISSA France (« les As du Web »), la *publication régulière de vidéos de sensibilisation* tournées par et avec des collaborateurs de Wavestone, etc.

Ce jeu de société constitue un autre exemple de l'engagement de Wavestone auprès du grand public.

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Avec la participation de Cybermalveillance.gouv.fr, le dispositif national d'assistance aux victimes de cybermalveillance et de sensibilisation aux risques numériques des publics, quels que soient leur âge et leur niveau de connaissance en matière de sécurité du numérique.

La plateforme en ligne Cybermalveillance.gouv.fr assure un accompagnement à deux niveaux :

- **Vous êtes victimes d'actes de cybermalveillance (escroqueries, piratage de comptes...) ?** Cybermalveillance.gouv.fr fait un **diagnostic précis de votre situation et vous met en relation**, le cas échéant, avec les spécialistes et organismes compétents proches de chez vous
- **Vous souhaitez comprendre les risques numériques et savoir comment réagir ou adopter les bonnes pratiques ?** Cybermalveillance.gouv.fr met à disposition **des outils de sensibilisation et de nombreux conseils** sur des thématiques du quotidien, et sous différents formats (vidéos, fiches réflexes, mémos, bandes-dessinées...).

Pour en savoir plus, rendez-vous sur **www.cybermalveillance.gouv.fr**.

INFORMATIONS PRATIQUES

Net Ecoute :
Site de sensibilisation aux dangers du net : https://www.netecoute.fr/ (possibilité de discuter via un chatbot)
Numéro de téléphone : 0800 200 000

PHAROS (plateforme de signalement de contenu) :
https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action

Plateforme de sensibilisation et d'aide aux victimes (cybermalveillance) :
https://www.cybermalveillance.gouv.fr/

Icônes utilisées dans ce livret :

Les icônes utilisées dans ce livret sont issues du pack Microsoft ou crées par la société Freepik, plus précisément par Eleonor Wang (https://www.flaticon.com/authors/eleonor-wang) et sont accessibles à ce lien : https://www.flaticon.com/.

Deux façons de jouer

Avec un animateur : la partie est ponctuée d'interventions et de moments d'échanges visant à réfléchir de manière ludique aux usages et aux dangers d'Internet ainsi qu'aux bons réflexes à adopter en conséquence.

En autonomie : les joueurs souhaitent tout simplement passer un bon moment à deviner et faire deviner des mots en lien avec la cybersécurité

Rôle de l'animateur

L'animateur joue un **rôle clé** dans la première variante de ce jeu. En effet, il devra **faciliter les échanges** avec et entre les joueurs, **orienter les discussions pour en déduire les bonnes pratiques à adopter sur Internet.**

Pour ce faire, **ce livret est mis à sa disposition.** Il contient **les règles du jeu** détaillées ainsi qu'un **guide** leur permettant de rebondir sur certains termes clés et les bonnes pratiques qui devront être partagées.

Dispositif conseillé :

Entre 6 et 12 joueurs de 11 à 14 ans

Durée :

Introduction + Jeu + Bilan: 75 minutes

Contenu du jeu

- **Un livret animateur**
- **35 cartes de jeu**
- **Un buzzer et un sablier**
- **Un poster géant et un stylo**
- **Plusieurs feuilles et feutres**

Déroulé

10 min

1 Introduction

L'objectif de cette introduction est de **faire prendre conscience aux joueurs de la multitude de leurs usages d'Internet**. En effet, Internet couvre un périmètre très large : réseaux sociaux, jeux en ligne, moteurs de recherche, etc.

Lors de cette première session d'échange, **les enfants réfléchissent et échangent sur leurs pratiques et activités sur Internet**. L'animateur lance les sujets en posant des questions et en relance pour avoir un maximum de réponses.

Quelques idées pour animer les discussions

Aujourd'hui nous allons jouer au « 1, 2, 3, Cyber ! ». Le but est simple : faire deviner à son équipe un maximum de mots en lien avec Internet. Mais avant de commencer, parlons justement d'Internet !

- *Que faites-vous sur Internet ?*
- *Quels appareils électroniques avez-vous ? Que faites-vous sur ceux-ci ?*
- *Quelles applications utilisez-vous ?*
- *Avec qui communiquez-vous en ligne ?*
- *Quelles données partagez-vous en ligne ? Avec qui ? Pourquoi ?*

L'animateur écrit sur le paperboard les pratiques et activités partagées par les joueurs, en les répétant à voix haute pour avoir confirmation par les joueurs.

En principe, les pratiques et activités suivantes seront probablement mentionnées :

- **Réseaux sociaux :** Instagram, TikTok, Youtube, blogs
- **Canaux de communication** : WhatsApp, Messenger, Snapchat, Skype, etc.
- **Jeux en ligne** : Fortnite, Overwatch, League of Legend (LoL), Call of Duty (CoD), Fifa, etc.
- **Forums en ligne**
- **Téléchargement en ligne et streaming**

Avant de lancer le jeu, il est important de relire ce qui a été partagé, demander aux joueurs s'ils pensent à d'autres pratiques et activités, puis compléter si besoin.

Mettre cette liste de côté et commencer le jeu.

45 min

Préparation du jeu

Il faut en premier lieu **diviser le groupe en équipes**. Le nombre d'équipes sera à adapter en fonction du nombre de joueurs : de 2 à 3 équipes de 3 à 5 joueurs chacune.

L'animateur commence par demander aux joueurs de se choisir un nom d'équipe, de préférence en lien avec Internet. Ils les inscrit sur le panneau des scores.

Parmi les 35 cartes à disposition, **constituez un jeu de 15 cartes**.

Ces mêmes 15 cartes serviront durant les 3 manches, le but étant que les joueurs se les approprient au maximum.

Pour constituer le jeu de 15 cartes, sélectionnez :

- **Les 10 mots suivants** : *cyberharcèlement, fake news, hameçonnage, ami virtuel, vie privée, mot de passe, signalement, chantage, challenge, cellule d'écoute.* Des messages importants sont associés à ces mots et devront donc faire l'objet d'interventions de la part de l'animateur au fil du jeu.
- **Et 5 autres cartes au hasard**.

Astuce sur la disposition des joueurs

Ne regroupez pas les joueurs de la même équipe : alternez dans la répartition, afin qu'ils se sentent concernés même quand ce n'est pas leur tour.

2 Jeu

La partie se déroule en **3 manches**, constituées de **plusieurs tours de 45 secondes**.

Objectif : à chaque tour, un joueur différent fait deviner à ses coéquipiers un maximum de cartes (un mot à faire deviner par carte).

Une manche se termine lorsque tous les mots en jeu ont été devinés.

La façon de faire deviner les mots varie d'une manche à l'autre : les détails sont donnés en p. 8 et 9.

Important !

Pour la première variante, l'objectif sera, au-delà du jeu, **de faire discuter les joueurs** sur leurs expériences sur Internet, les challenger sur leurs connaissances d'Internet, **identifier avec eux les dangers d'Internet et en tirer les bonnes pratiques** et les bons comportements **à adopter sur Internet**.

Chacune des manches donnera ainsi lieu à une **session d'échange**. Cette session aura lieu à la fin de chaque manche, une fois que toutes les cartes auront été devinées.

L'animateur a **trois manches pour aborder l'ensemble des sujets**, il ne faut pas chercher à tous les traiter dès la première manche. Vous trouverez sur les pages suivantes une explication sur le déroulé de chaque manche ainsi qu'une proposition de répartition des échanges entre les différentes manches.

Pour chaque mot, une liste de questions à poser afin d'en déduire ensemble les bonnes pratiques à adopter sur Internet est proposée en fin de livret.

Attention à ne pas casser la dynamique du jeu avec un échange trop long !

A la fin de chaque manche

A la fin de chaque manche, l'animateur doit créer un moment d'échange sur plusieurs mots (entre un et quatre selon le rythme de la partie). Pour cela, il prend la carte à évoquer et **questionne les joueurs** en commençant par une question simple : *comment avez-vous deviné ce mot ?*

Ensuite, un ensemble de questions peut être posé pour amener les joueurs à énoncer d'eux-mêmes les bonnes pratiques attendues.

A la fin de l'échange, **l'animateur résume les bonnes pratiques**, en faisant écho aux propos tenus.

A la fin du livret, pour chaque mot, se trouvent un ensemble de **questions et de bonnes pratiques à adopter**, qui peuvent servir de support à l'animateur. **Il convient donc de le consulter à la fin de chaque manche afin de pouvoir animer l'échange.**

Manche 1

Sur chaque carte apparaît un mot au centre, que le joueur doit faire deviner.
Pour faire deviner ce mot, **le joueur a uniquement le droit de parler**, mais autant qu'il le souhaite.

Les dérivés du mot à faire deviner ou les traductions directes dans une autre langue sont interdits, sous peine de pénalité d'un point.
En bas de chaque carte sont également écrits **trois mots.** Ces mots peuvent être lus à voix haute par le joueur pour l'aider à faire deviner le mot central. Après que chaque équipe a joué une fois, l'animateur peut décider de complexifier le jeu s'il le juge nécessaire : les trois mots deviennent alors des mots interdits : chaque mot interdit prononcé coûtera un point à l'équipe concernée.
Quand les 45 secondes du tour sont révolues, il faut placer la dernière carte utilisée au milieu de la pile de cartes restantes.
Il est interdit de passer des mots, même en cas de difficulté. Cela permet aux joueurs de s'approprier les termes. Si le mot n'est pas connu des joueurs, il est par exemple autorisé de procéder par rébus.

Une fois que toutes les cartes ont été devinées, la manche est terminée. L'animateur comptabilise les points **: un point par carte devinée**. Il ne faut pas oublier de déduire les potentiels points de pénalité. Les points sont inscrits sur le tableau des scores.

Sur quels mots rebondir à la fin de cette manche ?
Nos recommandations

Cyberharcèlement

Hameçonnage

Challenge

Ami virtuel

Manche 2

Pour cette manche, le joueur doit **faire deviner les mots en les dessinant**. **Les mêmes cartes que celles de la première manche sont utilisées**.

Il est strictement interdit d'utiliser des lettres dans le dessin et de parler en dessinant (sous peine de pénalité d'un point). Tout comme pour la première manche, les rébus sont autorisés.
De même que pour la première manche, il **est interdit de passer des mots**, même en cas de difficulté.

Une fois que toutes les cartes ont été devinées, on comptabilise les points : **un point par carte devinée**. Il ne faut pas oublier de déduire les potentiels points de pénalité. On additionne ces points avec ceux de la manche précédente.

Sur quels mots rebondir à la fin de cette manche ?
Nos recommandations

Chantage

Fake news

Vie privée

Manche 3

Pour cette troisième et dernière manche, le joueur doit faire deviner le mot inscrit sur sa **carte en ne prononçant qu'un seul mot**.

Il est interdit d'utiliser l'un des mots inscrits en bas de la carte. Compte tenu de la difficulté de la manche, le joueur qui fait deviner **a le droit de passer deux mots maximum** sur son passage.

Une fois que toutes les cartes ont été devinées, on comptabilise les points **: un point par carte devinée**. Il ne faut pas oublier de déduire les potentiels points de pénalité. On additionne ces points avec ceux de la manche précédente pour ainsi obtenir des totaux.
L'équipe gagnante est celle qui récolte le plus de points ! **Félicitations** à elle !

Sur quels mots rebondir à la fin de cette manche ?
Nos recommandations

Signalement

Cellule d'écoute

Mot de passe

20 min

3 Bilan

L'animateur peut commencer par une question simple : **est-ce que vous avez passé un bon moment ? Qu'en retenez-vous ?**

Ensuite, **il revient sur les éléments suivants**, sous forme de **résumé** :

Internet est un outil vraiment pratique et offre plein de possibilités pour communiquer, s'amuser, s'informer, etc.

Malheureusement, il peut aussi être utilisé par des personnes malintentionnées, capables d'utiliser tous les moyens à disposition pour arriver à leurs fins : cyberharcèlement, piratage de comptes, vols de mots de passe, usurpation d'identité, hameçonnage / phishing, récupération et utilisation de données personnelles, diffusion de fake news, etc.

Heureusement, quelques **bonnes pratiques et réflexes clés** vous permettront d'identifier et de déjouer la plupart des pièges.

Comment conclure le jeu ?

Il est important de conclure le jeu par **une synthèse des principales notions abordées pendant la session**, pour confirmer que les messages clés ont bien été compris.

Bien rappeler les bonnes pratiques

La synthèse de ces bonnes pratiques est rappelée en page suivante.

Quels sont les bons comportements à adopter?

- **En cas de doute sur les intentions d'un message reçu, le plus simple est de ne pas donner suite**. Si ce doute arrive dans un second temps, **il n'est jamais trop tard : parlez-en autour de vous** à des personnes de confiance. Selon les cas, un signalement sur le site www.internet-signalement.gouv.fr peut être fait et de l'aide peut être apportée via le site www.cybermalveillance.gouv.fr.
- De manière plus générale : **vous n'êtes pas seuls !** Victime ou témoin de comportements anormaux, il est nécessaire et important d'en parler pour trouver des solutions : vos parents, le signalement, les cellules d'écoute
- **Restreindre aux seules personnes de confiance les informations personnelles ou sensibles que vous ne voudriez pas voir diffusées sur Internet** : ne pas communiquer ces informations à des inconnus, configurer ses paramètres de sécurité et confidentialité sur les réseaux sociaux, désactiver la géolocalisation des photos partagées publiquement, etc.
- **Protéger l'accès à vos comptes** : vos **mots de passe** doivent rester secrets en toute circonstance, **compliqués à deviner pour les autres et faciles à retenir par vous**. Ils ne doivent pas être partagés et doivent régulièrement être changés, par précaution. Pour qu'ils soient plus sécurisés, préférez les mots de passe longs aux courts et faîtes une combinaison de lettres minuscules, majuscules, chiffres et caractères spéciaux.

Il est désormais temps de se dire au revoir, tout en demandant une dernière fois s'il reste aux joueurs des questions ou des remarques sur cette séance et sur la cybersécurité plus largement.

Mots à débriefer

Questions

Ici se trouvent les questions qui vous permettront d'initier les échanges avec les enfants, voir les relancer lorsque ceux-ci s'épuisent.

Bonnes pratiques

Ici se trouvent les messages clés à faire passer aux participants durant la session de jeu. L'idéal est, grâce aux questions, de les faire atterrir naturellement sur celles-ci.

Ami virtuel

Questions

- Est-ce que via vos réseaux sociaux, des jeux en ligne, des forums, vous êtes amenés à discuter en ligne ? Avec qui ?
- Est-ce que vous discutez parfois avec des gens que vous n'avez jamais rencontré dans la vraie vie, des amis virtuels ?
- Qu'est-ce que vous partagez avec eux ? Quelles données ?
- Est-ce qu'un inconnu vous a déjà demandé des informations qui vous ont paru louches ?
- Est-ce qu'un inconnu vous a déjà proposé de vous rencontrer dans la vraie vie ?
- Comment réagissez-vous dans ces cas-là ? Comment réagir ?

Bonnes pratiques

- Sur Internet, il est difficile de concrètement savoir qui se cache derrière vos amis virtuels (derrière des pseudonymes, des avatars, etc.).
- **Ne partagez aucune donnée privée sur vous ou sur votre famille avec un inconnu. N'acceptez pas de rendez-vous dans la vraie vie d'inconnus rencontrés sur Internet.**
- En cas de doute sur l'identité de vos amis virtuels et/ou sur le type de discussion(s) que vous entretenez, n'hésitez pas à **en discuter avec vos parents ou un tiers de confiance** (professeurs, CPE, oncles et tantes, grands-parents, fratrie, etc.).

Cyber-harcèlement

Questions

- Qu'est-ce que le cyberharcèlement ? Quelles en sont les conséquences et les dérives selon vous ?
- Est-ce que vous avez déjà été impliqué(e) ou témoin d'une situation de cyberharcèlement (auteur, victime) ? Si oui, comment avez-vous réagi ?
- Quelle attitude devrait-on adopter lorsque l'on est témoin de cyberharcèlement ?
- Quelle attitude devrait-on adopter lorsque l'on est victime de cyberharcèlement ? Pensez-vous modifier certains de vos comportements en ligne suite à notre discussion ? Si oui, lesquels ?

Bonnes pratiques

- Le cyberharcèlement est un effet de groupe visant à nuire (insultes, moqueries, agression, etc.), et ce à l'encontre d'une personne souvent isolée, via les canaux numériques et dans la durée.
- **Ne participez en aucun cas au mouvement de cyberharcèlement** car cela peut s'avérer très dangereux ! Il peut provoquer suicide, anxiété, déscolarisation, replis sur soi, exclusion, dépression, etc.
- Aussi, si vous êtes victime, ou témoin d'une situation de cyberharcèlement, **n'hésitez pas à le signaler, et/ou à en discuter avec quelqu'un de confiance** (parents, professeurs, CPE, oncles et tantes, grands-parents, fratrie, etc.). La plateforme NetEcoute permet aussi de se confier et de signaler ses problèmes

Questions

- Qu'est-ce que le cyberharcèlement ? Quelles en sont les conséquences et les dérives selon vous ?
- Est-ce que vous avez déjà été impliqué(e) ou témoin d'une situation de cyberharcèlement (auteur, victime) ? Si oui, comment avez-vous réagi ?
- Quelle attitude devrait-on adopter lorsque l'on est témoin de cyberharcèlement ?
- Quelle attitude devrait-on adopter lorsque l'on est victime de cyberharcèlement ? Pensez-vous modifier certains de vos comportements en ligne suite à notre discussion ? Si oui, lesquels ?

Bonnes pratiques

- Des attaquants peuvent utiliser la toile afin de vous tendre des pièges . Que ce soit par mail, SMS ou tchat, il faut rester vigilant lorsque l'on reçoit un message invitant à cliquer sur un lien ou un document. Celui-ci peut être piégé !
- Pour déceler les pièges, prêtez attention entre autres aux points suivants : l'adresse de l'émetteur, le contenu, la structure du lien si lieu est (en cas de doute, cherchez l'organisme sur un moteur de recherche, utilisez l'adresse obtenue et vérifiez si sa structure correspond à celle reçue).
- Quoi qu'il en soit, **n'ouvrez pas de pièces jointes et ne cliquez pas sur des liens contenus dans des mails provenant d'un inconnu et/ou qui vous paraissent douteux** (fautes d'orthographe, cadeaux exceptionnels, etc.). Cela peut mener à des arnaques, à des fraudes et à des virus qui viendront bloquer votre appareil électronique.
- **Si vous vous êtes fait piéger, ne cherchez pas à le cacher** : parlez-en avec vos parents ou un tiers de confiance (professeurs, CPE, oncles et tantes, grands-parents, fratrie, etc).

Questions

- Est-ce que vous avez déjà entendu parler d'un challenge circulant sur la toile ? Est-ce que vous avez déjà entendu parler du «Blue whale challenge » ou du défi de la cannelle ? Qu'est-ce que c'est ?
- Vous a-t-on déjà poussé à participer à ce type de challenge ? Comment avez-vous réagi ?

Bonnes pratiques

- Les challenges, ou défis en ligne, sont une pratique très répandue. Récemment deux cas concrets de challenge sévissent en ligne (cf. encadré).
- Si jamais un inconnu vous aborde en ligne, ou même une connaissance voire un ami et vous demande de relever des défis de ce type, **le premier réflexe à avoir est d'en discuter avec quelqu'un de confiance** (parents, professeurs, CPE, oncles et tantes, grands-parents, fratrie, etc).

Exemples de challenges

- **Le « Blue Whale Challenge »:** Un « tuteur » rentre en communication avec un internaute et lui lance une série de défis que celui-ci doit relever. Il a ainsi un défi à réaliser par jour (du plus simple, de type dessiner une baleine bleue sur une feuille, jusqu'à des défis pouvant mettre en péril sa santé). Le joueur doit ensuite poster la preuve de la réalisation du défi sur les réseaux sociaux.
- **Le défi de la cannelle :** Il est demandé au participant d'ingurgiter une cuillère à soupe, voire plus, de cannelle en poudre, se filmer et poster la vidéo sur les réseaux sociaux. Ce type de défi se propage rapidement car, une fois la vidéo publiée, le joueur peut nommer 3 personnes qui devront relever le défi et ainsi de suite. Ce défi est dangereux car il peut mener à des étouffements.

Chantage

Questions

- Est-ce que vous avez déjà été victime de chantage en ligne ? Qu'est-ce que peut être le chantage en ligne ?
- Est-ce que vous avez déjà entendu parler du Momo Challenge ? Du chantage à la webcam ?
- Comment est-ce que vous réagiriez si vous étiez victime de chantage en ligne ?

Bonnes pratiques

- Un internaute malintentionné, peut rentrer en contact avec vous et vous demander certaines données (type données bancaires pour faire des achats), voire vous demander de relever des défis (du plus simple au plus tordu). Si vous ne répondez pas positivement à ses demandes, celui-ci vous menace de dévoiler des informations privées à votre propos, vos secrets par exemple (les communiquer à vos contacts Instagram, par mail ou à vos parents).
- Si **jamais vous êtes victime de ce genre de pratiques, ne répondez pas, ne payez rien, conservez les preuves** (captures d'écran, mails, etc.), **et trouvez de l'assistance sur le site www.cybermalveillance.gouv.fr**.
- Surtout, parlez-en avec vos parents ou un tiers de confiance (professeurs, CPE, oncles et tantes, grands-parents, fratrie, etc.

Cas de chantage

- **Le chantage à la webcam** : Un internaute malintentionné menace sa victime de dévoiler des images compromettantes de lui, prises à son insu via sa webcam si celui-ci ne communique pas des données bancaires ou ne paye pas une rançon en ligne. Au-delà des bonnes pratiques générales, il est important de toujours garder un cache sur la webcam lorsque celle-ci est inutilisée.
- **Le Momo challenge** : Celui-ci consiste à rentrer en contact avec un interlocuteur anonyme : « momo » sur les réseaux sociaux. Cet interlocuteur menace ensuite ses victimes de dévoiler des informations personnelles si ceux-ci refusent de se soumettre à une série de défis, souvent violents.

Questions

- Qu'est-ce que la vie privée pour vous ? Est-ce que vous vous êtes déjà retrouvé(e) dans des situations que vous avez jugé « intrusives » ? Si oui, lesquelles ?
- Que faites-vous sur la toile pour protéger votre vie privée ?
- Quelles données évitez-vous de partager sur la toile ? Qu'est-ce qu'une donnée personnelle ?
- Est-ce que dans la vraie vie, vous les dévoilez facilement et pourquoi ? Est-ce que vous en partagez certaines en ligne ? Via quels canaux ?
- Savez-vous ce qu'est la géolocalisation ? Est-ce une donnée sensible selon vous ? Pourquoi ? Avez-vous des exemples d'applications qui utilisent votre géolocalisation ?

Bonnes pratiques

- Afin de conserver votre vie privée sur Internet, quelques bonnes pratiques à adopter :
- Par défaut, ce que vous publiez sur les réseaux sociaux est accessible à tout le monde : vérifiez bien les paramètres de « confidentialité » ou « sécurité » et réglez-les pour être sûr que seuls vos amis ont accès à vos données.
- **Réfléchissez méticuleusement aux données que vous partagez sur Internet** : âge, données bancaires (les vôtre ou celles de vos parents), adresse postale, opinions politiques, religieuses, etc.
- **Désactivez la géolocalisation lorsque vous prenez des photos**. Lorsque vous postez une photo en ligne, celle-ci comporte ce que nous appelons des « métadonnées » dont votre géolocalisation ! Cela signifie que toute personne ayant accès aux photos publiées peut savoir où la photo a été prise et donc où vous vous trouvez à un instant T. Très pratique pour un cambrioleur qui veut savoir si vous êtes chez vous par exemple.
- Aussi, il est important de **garder en tête qu'Internet a la mémoire longue !** Tout ce que vous postez aujourd'hui alimente ce que l'on appelle votre e-réputation et pourra impacter votre futur. Ainsi, réfléchissez bien à deux fois avant de publier du contenu.

Questions

- Est-ce qu'il est possible de trouver des fausses informations sur Internet ?
- Cela vous est-il déjà arrivé ? Comment vous en êtes-vous rendu compte ?
- Pour vos exposés comment vérifiez-vous les informations que vous trouvez sur Internet ?
- Plus largement, comment peut-on vérifier si une information est correcte ou non ?

Bonnes pratiques

- De fausses informations circulent sur Internet… Bien sûr puisque n'importe qui peut y poster ce qu'il souhaite !
- Ainsi, avant de relayer des informations, ou avant d'utiliser du contenu (pour des exposés par exemple), **il est important de vérifier et croiser les informations que vous trouvez sur Internet**. En cas de doute, n'hésitez pas à en parler avec vos parents ou un tiers de confiance (professeurs, CPE, oncles et tantes, grands-parents, fratrie, etc.).

Mot de passe

Questions

- Sur quels réseaux sociaux avez-vous un compte ?
- Comment choisissez-vous votre mot de passe ?
- Est-ce que vous utilisez le même mot de passe pour chacun de vos comptes ?
- Est-ce que vous avez déjà donné votre mot de passe à un ami ?

Bonnes pratiques

- Les mots de passe protègent l'accès à vos comptes et donc à vos données : ils doivent rester secrets si vous ne souhaitez pas que des personnes mal intentionnées usurpent votre identité ou volent vos informations.
- Il faut choisir des mots de passe à la fois compliqués à deviner pour les autres et faciles à retenir pour vous.
- **Avoir un mot de passe différent par site ou application réduit aussi les risques de se faire voler ses mots de passe.**
- Ne les partagez pas et ne les écrivez pas sur un papier. Enfin, changez de mot de passe régulièrement, par précaution.
- Restez particulièrement vigilant pour le mot de passe de votre adresse mail. Si celui-ci est compromis, cela permettrait aux hackers de réinitialiser vos mots de passe sur vos différents comptes et d'accéder aux sites sur lesquels vous êtes inscrits

Signalement

Questions

- Avez-vous déjà été confronté sur Internet à une photo / une vidéo qui vous a mis mal à l'aise ?
- Si oui, lesquels et pourquoi ?
- Comment avez-vous réagi ?
- Est-ce qu'une photo de vous qui ne vous plaisait pas a déjà circulé sur la toile ?
- Que pourrait-on faire dans ces cas-là ?

Bonnes pratiques

- Sur Internet, vous pouvez être confronté(e), sans le vouloir, à du contenu choquant. Si cela vous arrive, vous pouvez signaler le contenu : directement sur le site si possible (Facebook, Instagram, etc.) ou via la plateforme de signalement PHAROS (www.internet-signalement.gouv.fr).
- **Si un contenu vous a choqué, il est important de ne pas se sentir gêné d'en discuter avec un tiers de confiance** (professeurs, CPE, oncles et tantes, parents, grands-parents, fratrie, etc).
- De même, sur Internet, vous disposez d'un droit sur les photos où vous êtes identifiable ! Ainsi, si **une photo de vous circule et vous dérange, n'hésitez pas à signaler le contenu** et / ou à en discuter avec vos parents ou tout autre personne de confiance.

Cellule d'écoute

Questions

- Si l'une des situations précédemment évoquées vous arrivait, à qui est-ce que vous en parleriez ?

Bonnes pratiques

- Il est important d'échanger sur nos expériences d'Internet !
- **Si jamais vous êtes victime, témoin ou acteur de l'une des situations précédemment évoquées, il faut en discuter !**
- Si vous ne souhaitez pas en discuter avec vos proches, il est possible d'appeler le numéro qui est inscrit sur votre livret. Vous pourrez en parler en tout anonymat et recevoir des conseils.

MES NOTES

1,2,3 CYBER !

Jeu Cyber pour les
11-14 ans

CCJ

WAVESTONE

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique