PARTIE 3 Que faire en cas... ?

Que faire pour assurer ta cybersécurité ?

INFORMATION PRÉALABLE

L'essor d'internet a profondément changé notre société. Une vie sans internet est devenue quasiment inimaginable. Une grande partie de la population est connectée en permanence, que ce soit à la maison, à l'école ou au travail. Nous sommes actifs sur les réseaux sociaux, nous payons nos factures en ligne et nous utilisons internet pour apprendre et nous divertir. Si internet et les e-mails présentent beaucoup d'avantages, ils ont aussi un revers : la cybercriminalité, que l'on rencontre sous forme de phishing, logiciels malveillants, hacking, attaques par déni de service (AttaquesDDos) et fraudes à la carte bancaire. Chacun risque d'être un jour confronté à une escroquerie sur internet.
Il est donc important de se prémunir contre cette forme de criminalité et de rester vigilant lorsque l'on se connecte. Les conseils les plus importants pour les parents se trouvent dans la brochure informative.
N'hésitez pas à discuter de ces conseils en classe.
Pour plus d'informations sur la cybersécurité : safeonweb.be.
Dans cette leçon, nous nous limiterons à la cybersécurité, c'est-à-dire la protection des données en ligne et sur certains appareils. Pour plus d'informations sur la sécurité sur internet, les médias sociaux et le harcèlement en ligne, visitez le site web de Child Focus.

OBJECTIFS

- Les élèves sauront qu'ils doivent être prudents lorsqu'ils se connectent.
- Les élèves sauront qu'ils ne peuvent pas partager leurs mots de passe et informations sensibles.
- Les élèves seront capables de donner des exemples de dangers liés à internet.
- Les élèves sauront comment faire face à ces dangers.
- Les élèves oseront parler des dangers liés à internet.

MATÉRIEL

Annexe 1

- Check-list (annexe 1)
- Internet
- Du papier

DÉROULEMENT DE LA LEÇON

1) Introduction

Si vous utilisez un mot de passe sur l'ordinateur de votre école ou pour accéder à internet, vous pouvez l'afficher sur l'écran d'accueil. Invitez quelques élèves à déchiffrer votre mot de passe. Demandez aux élèves s'ils trouvent astucieux que vous utilisiez un mot de passe, s'ils en utilisent eux-mêmes et dans quel contexte (comptes de jeu, médias sociaux, accès à un ordinateur (portable ou non), téléphone portable, compte bancaire). *Quelqu'un a-t-il déjà communiqué son mot de passe à quelqu'un d'autre ? À qui ? Était-ce (im)prudent ?* Demandez aux élèves d'expliquer pourquoi les mots de passe sont importants.

2) Activité principale

Divisez la classe en cinq groupes, et proposez à chaque groupe de chercher de l'information sur un des points à étudier. Demandez aux groupes de prévoir une présentation par ordinateur (PowerPoint) à montrer à l'ensemble de la classe. Précisez qu'ils devront expliquer quel est leur sujet, comment on peut assurer sa cybersécurité sur ce point et ce qu'il faut faire si un problème survient malgré tout. Les points à examiner sont :

- les sauvegardes,
- les virus informatiques et les logiciels antivirus,
- le phishing et les spams,
- les mots de passe,
- le piratage et les mises à jour.

Une fois que les élèves savent ce qu'est le phishing, ce que sont les bons et mauvais mots de passe et quelles informations ils doivent ou ne doivent pas partager, ils peuvent également jouer au niveau « Surf safe » du jeu en ligne BE-Ready.

3) Pour aller plus loin

Les élèves établissent, chacun pour soi, une check-list de ce qu'il faut faire avant, pendant et après un épisode de cybercriminalité. Si nécessaire, rappelez d'abord ce qu'est une check-list et comment elle se présente. Discutez des check-lists en classe ou donnez-les comme devoir à faire à la maison. À partir des listes établies individuellement par les enfants, vous pouvez constituer (vous-même ou avec la classe) une check-list définitive que les élèves ramèneront à la maison. En annexe, vous trouverez un modèle de check-list (annexe 1).

Annexe 1

Nom : .....

JE VEILLE À MA CYBERSÉCURITÉ !

Sur internet, il faut rester vigilant. Tu peux faire un tas de choses pour te protéger.

AVANT

- ◯ Je ne communique jamais mes **mots de passe** et je les change régulièrement.
  Ton mot de passe, c'est comme ta brosse à dents : tu ne la donnes pas à quelqu'un d'autre et tu la changes régulièrement ! Cherche à avoir un mot de passe solide.
- ◯ J'effectue régulièrement des **sauvegardes** et des **mises à jour** avec l'aide de mes parents.
- ◯ Je sais que tout ce que je lis sur internet n'est pas nécessairement vrai. Je peux reconnaitre un **message non fiable** : je n'y réponds jamais, je le supprime immédiatement.
- ◯ Je partage des informations avec **prudence**. Je ne sais jamais qui pourrait me lire !
- ◯ Je **couvre** ma **caméra** à l'aide d'un autocollant ou d'un cache webcam.
  Tu fermes aussi tes rideaux quand tu ne veux pas que les autres regardent à l'intérieur, pas vrai ?

PENDANT

En cas de virus informatique :

- ◯ Je demande à mes parents d'activer le **logiciel antivirus**.
  S'il y a un virus dans ton ordinateur, le logiciel antivirus va l'éliminer.
- ◯ Si je n'en ai pas encore installé sur mon ordinateur, je choisis un logiciel antivirus fiable avec mes parents (safeonweb.be/fr/infecte-par-un-virus) et je le fais fonctionner.

Si mon compte est piraté :

- ◯ J'active mon **logiciel antivirus**.
  Je **change** immédiatement tous mes **mots de passe**. Je fais cela sur un ordinateur fiable, donc pas sur l'appareil à partir duquel mon compte a été piraté.

Si je rencontre d'autres problèmes informatiques :

- ◯ Je demande **conseil** à un adulte, par exemple à l'un de mes parents ou à un professeur.
  Plus vite tu informes quelqu'un de ton problème, plus vite il sera résolu.

APRÈS

Si je suis victime de cybercriminalité :

- ◯ **J'informe** mes parents et je les accompagne à la police.