LA TECHNOLOGIE AU COLLEGE

Sciences et Techniques Industrielles

Portail national de ressources - éduscol

Région académique HAUTS-DE-FRANCE

CYCLE 4	**Les défis et les risques associés à la transformation numérique**	NIVEAU CINQUIÈME

Présentation de la séquence

Cette séquence a pour objectif de faire découvrir aux élèves les bases de la cybersécurité afin qu'ils soient sensibilisés aux risques liés à l'utilisation des réseaux informatiques. Elle permet d'identifier quelques règles de sécurités à l'environnement numérique, ainsi qu'aux droits de la propriété intellectuelle et de percevoir ainsi la responsabilité dans les dérives liées à la cyberviolence.

Thème abordé :	Les objets et les systèmes techniques : leurs usages et leurs interactions à découvrir et à analyser
Attendu de fin de cycle :	Décrire les liens entre usages et évolutions technologiques des objets et des systèmes techniques

Compétences	**Connaissances**
Identifier des règles permettant de sécuriser un environnement numérique (bases de la cybersécurité) et des règles de respect de la propriété intellectuelle.	Cybersécurité : protection des données personnelles, traces numériques (témoins de connexion, géolocalisation), identification, authentification, respect de la propriété intellectuelle
Appréhender la responsabilité de chacun dans les dérives (cyberviolence, atteinte à la vie privée, aux données personnelles, usurpation d'identité)	Cyberviolence : usurpation d'identité, usage détourné.

PROPOSITION DE DEROULEMENT DE LA SEQUENCE

Séance 1 – Mots de passe dépassés

- Mise en situation (**5 mn**)

Le collège est équipé d'un réseau et pour se connecter à l'espace numérique de travail, les élèves doivent connaitre leur nom d'utilisateur et leur mot de passe.
Les vidéos (1) ou (2) sont montrées à la classe afin de lancer les échanges et d'appréhender la première barrière de protection de sécurité informatique.

- Description de la situation ou questionnement (**5mn**)

A partir des 2 films, chaque élève explique ce qui peut être fait et note aussi ses interrogations.

- Problématique

À la suite des échanges avec la classe, quelques termes de base suivantes doivent apparaitre : *Cybersécurité, cyberattaques, données personnelles, mots de passe...*
La problématique suivante doit émerger : *Que faut-il faire pour bien protéger ses données ?*

- Propositions (ou Mes propositions, ou Hypothèses, ou Mes…) (**5mn**)

Chaque élève écrit ce qu'il connaît sur les règles permettant de sécuriser un environnement numérique, notamment les mots de passes.

➢ Investigations (Recherches) (**25 mn**)

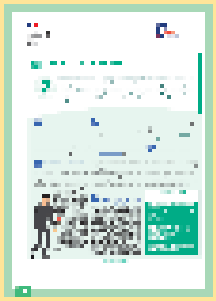
1. Chaque équipe va, à l'aide des ressources fournies ((2) et (3)), définir les attributs d'un « mot de passe solide », Ils doivent analyser leurs caractéristiques : nombres de lettres, chiffres, caractères spéciaux, majuscules…
2. Tester sur des sites (1) et (1bis) dédiés quelques mots de passe et découvrir la rapidité à le casser.
3. Modifier leur propre mot de passe utilisé sur le réseau du collège.
4. Vérifier son bon fonctionnement en se connectant avec le nouveau mot de passe.

Travail à la maison (voir ressources TRAAM) ou en classe : Un élève récupère sur un smartphone égaré.
Quel comportement adopter dans cette situation ? Il convient de retrouver la personne pour lui rendre son smartphone. (Ce travail peut-être réaliser en classe à la place des points 3 et 4)

Quelques équipes présentent leur travail et, suite aux échanges un bilan est réalisé.

➢ **Bilan (15mn)**

*Pour réduire les risques et éviter un piratage de vos différents comptes en ligne, Il est recommandé d'utiliser des mots de passe suffisamment longs, **complexes et différents** pour accéder à chacun des équipements et services.*
*Les **caractéristiques de mot de passe fort**, difficile à craquer sont :*
Au moins 12 caractères, Minuscule, Majuscule, Symboles (?#@…), Chiffres.
*Au moindre doute, ou même par prévention, **changer de mot de passe et activer la double authentification** chaque fois que possible pour renforcer votre sécurité.*
*Enfin, il faut utiliser un **gestionnaire de mots de passe** pour les stocker de manière sécurisée.*

Ressources pour le professeur	**Ressources pour les élèves**
Vidéos : (1) https://www.dailymotion.com/video/x6lxrwt (2) https://www.dailymotion.com/video/x7txg0c Livret pédagogique.pdf  https://www.cybermalveillance.gouv.fr/tous-nos-contenus/kit-de-sensibilisation Kit_sensibilisation.pdf Activités complémentaires (TRAAM) : https://ppc-formation.fr/divers/smartphone/smartphone.html https://ppc-formation.fr/divers/smartphone/2/smartphone.html	(1) https://www.cnil.fr/fr/generer-un-mot-de-passe-solide (1bis) https://ppc-formation.fr/divers/mdp/mdp.html (2) Connaître les recommandations pour le choix d'un mot de passe robuste. (3)https://www.cybermalveillance.gouv.fr/tous-nos-contenus/kit-de-sensibilisation (*page 3 et 4*)

Séance 2 Phishing et hameçonnage, comment passer à travers les filets ?

- Mise en situation

Il s'agit d'expliquer aux élèves les principales menaces en ligne : virus, logiciels malveillants, phishing…etc. L'enseignant montre aux élèves les vidéos : reception colis.mp4 et L'hameçonnage (ou phishing en anglais) « Comment pêcher un n.mp4

- Description de la situation ou questionnement (**5mn**)

Chaque élève explique ce qu'il comprend et note aussi ses interrogations.

- Problématique (**10mn**)

Phishing et hameçonnage, comment passer à travers les filets ?

- Propositions (ou Mes propositions, ou Hypothèses, ou Mes…) (**5mn**)

Chaque élève écrit ce qu'il connait sur le phishing, notamment les courriers ou SMS reçus et explique comment s'en protéger.

- 1 - Investigations (**20 mn**)

Mise en situation et questionnement

Les élèves se mettent en situation de recevoir un mail malveillant.

Consigne(s) :

Les élèves doivent identifier les indices indiquant qu'il s'agit d'une tentative de fraude. Pour cela l'enseignant fournit un exemple de courriel de phishing et de situation de réception de colis (vidéo).

Objet : Mise à jour importante de sécurité de votre compte

Cher utilisateur,
Nous vous informons qu'il y a eu une activité inhabituelle détectée sur votre compte. Pour protéger vos informations et garantir la sécurité de votre compte, nous vous demandons de bien vouloir effectuer une mise à jour de sécurité dès que possible. Pour ce faire, veuillez cliquer sur le lien ci-dessous et suivre les instructions fournies :
[http://www.securiconte.biz]
Nous vous prions de prendre cette mesure de sécurité au sérieux afin d'éviter toute violation de vos données personnelles.
Si vous avez des questions ou des préoccupations, n'hésitez pas à contacter(securicomte@info.gs)

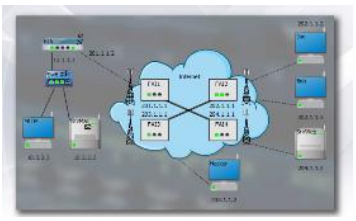
notre service d'assistance à la clientèle.

https://www.dailymotion.com/video/x8rvpgc

Quelques équipes présentent leur travail et à la suite des échanges un bilan est réalisé.
(Montrer la vidéo : Identifier des situations d'arnaque par manipulation psychologique (hameçonnage, usurpation d'identité, faux support informatique).

- 2 – Activité complémentaire

  Simulation d'une cyberattaque avec le logiciel NETSIM



Bilan (15 mn) :

Des signes révélateurs à surveiller :

1. L'adresse e-mail de l'expéditeur.
2. Demandes de renseignements personnels
3. Liens suspects
4. Demandes urgentes ou menaçantes
5. Contenu et orthographe douteux
6. Pièces jointes suspectes
7. Incohérences dans l'identité de l'expéditeur ou de l'entreprise

Ressources pour le professeur	**Ressources pour les élèves**
Identifier des situations d'arnaque par manipulation psychologique (hameçonnage, usurpation d'identité, faux support informatique). **https://www.dailymotion.com/video/x7umc11** **Fiche d'activité** « Vol d'identifiants » **avec le logiciel Netsim**	Fichier : mail sécurité compte.docx Vidéos : - reception colis.mp4 - L'hameçonnage (ou phishing en anglais) « Comment pêcher un n.mp4

Séance 3 Le plagiat, ce n'est pas l'original, c'est du pénal.

Sensibiliser aux droits de propriété intellectuelle, droits d'auteur, les marques déposées et les brevets.

- Mise en situation ((**5mn**)

Situation 1

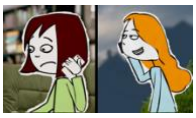
Étude de cas

Dans un collège, une étudiante en classe de 3e, a été accusée de plagiat après avoir remis un devoir en histoire. Le devoir portait sur la Révolution française et représentait une part importante de son évaluation finale pour le trimestre.

Découverte du Plagiat :

Le professeur, monsieur Caradec, a remarqué que certaines parties du travail, semblaient écrites dans un style très différent du reste de son texte. En utilisant un logiciel de détection de plagiat, il a découvert que de larges parties du devoir étaient directement copiées à partir d'un article en ligne sans aucune citation appropriée.

Situation 2 : vidéo - Hadopi-02



- Description de la situation ou questionnement (**5mn**)

Chaque élève écrit ce qu'il pense de ces situations. Après des échanges avec la classe, l'enseignant pose la problématique suivante.

- Problématique (**5 mn**)

Avons-nous le droit de faire ce qui est présenté dans les 2 situations ?

- Investigations (**30 mn**)

Chaque équipe à l'aide des ressources doit répondre à cette question et expliquer ses réponses.

Bilan classe entière

- Bilan (**10mn**):

Il est important de respecter des règles pour protéger le travail des autres et ses propres droits.

Le **droit d'auteur** est une protection légale qui donne au créateurs (comme les écrivains, les artistes, les musiciens, etc.) des droits sur leurs œuvres. C'est un délit passible de sanctions civiles et pénales.

Par exemple, le **plagiat** concerne l'appropriation des idées et des créations d'autrui. C'est considéré comme une forme de vol intellectuel. Cela peut entrainer des sanctions sévères allant de la réprimande à l'exclusion. Pour éviter le plagiat, il est important de citer ses sources et de reformuler les idées.

Le **droit à l'image** protège l'utilisation de l'image d'une personne sans leur accord. Les sanctions pour la violation du droit à l'image peuvent inclure des amendes, des dommages et intérêts pour préjudice moral

Ressources pour le professeur	**Ressources pour les élèves**
- **https://www.hadopi.fr/** - **https://eduscol.education.fr/document/12886/download** - **https://sensib.arcom.fr/enseignant/choix-activite/2/bdtool**	Vidéo **: -** Hadopi-02 - UA Webcam Plagiat - YouTube Site https://sha.univ-poitiers.fr/dpt-psycho/wp-content/uploads/sites/71/2020/01/GUIDE-ETUDIANT_EVITER-LE-PLAGIAT-revu.pdf plagiat fraude courante....url Fichiers : Fiche1_Hadopi_notion_oeuvre_protegee_synthese.pdf Fiche6_Hadopi_trouver_ressources_internet_synthese.pdf Fiche7_Hadopi_telechargement_illegal_synthese.pdf

Séance 4 – Evaluation

Evaluation de la séquence « cybersécurité », l'élève à travers un questionnement et des études de cas doit montrer l'acquisition des compétences développées lors des séances précédentes.

1 - **Cybersécurité :**
Quelles sont les éléments qui permettent d'identifier un mail frauduleux ?

Quelles sont les actions à mettre en place rapidement ?

Quelles sont les caractéristiques d'un mot de passe fort ?

Quels sont les risques si votre espace numérique est piraté ?

2 - Phishing :

Rechercher des infos suspectes, justifier vos réponses.

Quelles conséquences si on clique sur le lien ?

Pourquoi les cookies peuvent être problématiques ?

Energie la France

Cher client,

Section de contrôle des contes clients

La mise à jour de votre compte à ce jour, nous donne un solde débiteur de 6,40 EUROS, vous êtes prié de régulariser votre débit avant la fin de cette semaine pour éviter des frais supplémentaires à votre charges.

Joindre un chèque de votre facture à l'ordre d'Energie de France

Cliquez ici pour régler directement votre facture

Cordialement

Anne Sophie Larrivière
Directrice adjointe du service de recouvrement

3 - Confidentialité :

Comment aider Louis, témoin de cyberharcèlement envers Charlie, recevant régulièrement des messages d'insultes sur un réseau social ?

Répondre à cette question en concevant une petite bande dessinée d'une planche avec la fabrique à BD :

https://bdnf.bnf.fr/fr