Séquence 5	La protection des données E1
Thème	Les objets et les systèmes techniques : leurs usages et leurs interactions à découvrir et à analyser
Compétences	OST 1.2.1a Identifier et appliquer les règles pour un usage raisonné des objets communicants et des environnements numériques (propriété intellectuelle, identité numériques (propriété intellectuelle, identité numérique, témoins de connexion, géolocalisation).

1. Sécuriser nos données, se protéger des arnaques

Situation déclenchante :

La cybersécurité apparaît comme étant de nos jours une priorité pour les entreprises : la protection de leurs systèmes d'informations et de leurs données contre les cyber-attaques est devenue un véritable enjeu. Les menaces informatiques telles que les virus, les piratages, les fuites de données sont de plus en plus répandues et sophistiquées. La cybersécurité englobe un ensemble de pratiques visant à sécuriser au maximum les réseaux, les applications , les données et les objets connectés.
Elle s'appuie sur des protocoles de sécurité, la formation des utilisateurs avec l'adoption de moyens de protection comme les anti-virus, les mots de passe et les systèmes de cryptage.
Les attaques deviennent de plus en plus complexes, la cybersécurité est devenue un enjeu crucial pour les entreprises à un point tel que de nouveaux métiers sont apparus …

Problématique : Quels moyens avons-nous pour sécuriser nos données, se protéger des arnaques. Que mettent en place les entreprises pour se protéger ?

Investigations : Regarder les vidéos suivantes et répondre aux questions ci-dessous

https://www.youtube.com/shorts/kSg9YLP_2_E
https://www.youtube.com/shorts/SziCWSTS5BM
https://www.youtube.com/watch?v=YI-6nZFxwNg
https://www.youtube.com/shorts/omHN1gwkVkM

1 – Combien de caractères doit contenir au minimum un mot de passe ?

2 – Comment s'appelle la technique d'attaque la plus utilisée par les hackers pour trouver un mot de passe ?

3 – En quoi consiste-t-elle ?

4 – Comment s'appellent les 4 techniques d'attaque utilisées par les hackers ?

-
-
-
-

5 – Combien de combinaisons, un ordinateur standard peut-il tester ?

Travail à faire : comment choisir un bon mot de passe ?
Il existe pour cela des sites qui te permettent de connaître la catégorie (A, B, C, D, E) de ton mot de passe.

Utiliser le site suivant http://ssi.economie.gouv.fr/motdepasse pour tester cette liste de mots de passe et indiquer le résultat obtenu :

Mot de passe	Fiabilité
12345678	
12345678/	
motdepasse	
password	
leverdesoleil	
chat	
chatnoir	
222222	
Football	

Mot de passe	Fiabilité
Football1998	
2025motdepass	
Password2025	
Ch@tnoir2025	
Ch@tnoir2025!	
T0n!d4caCh@b31	
ChatNoir/560du71*	
L5verDeSoleil2025!	
A1ph@B3tS3cur3?	

À partir de ces tests, d'après ce site, qu'est-ce qu'un bon mot de passe et que doit-il contenir ?

2. Comment se protéger d'une technique de piratage très utilisée, la technique du hameçonnage ou phishing ? :

Se connecter au site https://phishingquiz.withgoogle.com/?hl=fr et répondre aux différentes questions.

- A quoi faut-il faire attention pour éviter de se faire avoir par une tentative d'hameçonnage / phishing ?

-
-
-
-

- Donner une définition de l'hameçonnage :

3. Une autre méthode pour se protéger : le cryptage des données :

Exercice : Vous êtes professeur et vous souhaitez envoyer le code d'entrée du portillon du collège à votre collègue qui l'a oublié. Comment faire pour être sûr qu'aucune autre personne ne puisse s'approprier le code ?

Ouvrir la fiche ressource "Méthode de cryptage césar"
En utilisant ce document et la clé 6, coder le message suivant : le code est quarante vingt-deux (4022)

Alphabet normal : ……

Alphabet de César (←6) ……

Réponse : ……

Est-ce que cela suffit pour chiffrer notre message et sécuriser la conversation ?

Que mettent en place les entreprises pour se protéger ?

On a vu dans les questions précédentes que les moyens pour se protéger existent bien mais qu'ils ne sont malgré tout pas complètement fiables face à des hackers de plus en plus performants.
Les entreprises ou banques, qui ont des milliers de données à protéger, ont décidés de faire appel à des professionnels pour analyser les failles de leurs systèmes et ainsi permettre de mieux les protéger… On les appelle les hackers éthiques.

Visionner les vidéos ci-jointes ;
https://www.youtube.com/watch?v=iVrmzwbl8oo
https://www.youtube.com/watch?v=s8Rs0cfDT90

Qu'est ce qu'un hacker éthique et quel est son rôle ?

Quelles compétences doit avoir un hacker éthique ?

Quel niveau d'étude pour devenir hacker éthique ?