FICHE PÉDAGOGIQUE : ENSEIGNANT.E

LA CYBERSÉCURITÉ INDUSTRIELLE

45 à 60 minutes autour du jeu INDUSTRIUM

Public : Collège (4e–3e) et Lycée (2de).
Matériel : Vidéoprojecteur, tableau, fiches élèves imprimées, quiz.
Esprit : Ludique, collaboratif, axé sur la prévention et la curiosité numérique.

- Comprendre ce qu'est une cyberattaque et ses conséquences
- Identifier les métiers de la cybersécurité industrielle
- Découvrir les bons réflexes numériques dans un environnement connecté
- Développer l'esprit critique face à l'information et la vigilance face aux risques numériques

Que se passe-t-il si **un hacker coupe la production d'une usine ?**

Introduction

Les usines du futur sont connectées, mais cela les rend aussi vulnérables.
Une simple clé USB, un e-mail piégé ou un mot de passe trop simple peuvent bloquer toute une chaîne de production, voire provoquer des dégâts matériels.
La cybersécurité industrielle consiste à protéger les systèmes de production contre les attaques, les erreurs humaines et les pannes informatiques.
Cette activité permet de comprendre l'importance de la vigilance numérique et de découvrir des métiers passionnants autour de la protection des données et des infrastructures.

Préparation

Organisez la classe et le matériel :

- Imprimez les fiches élèves et distribuez les.
- Agencez la classe de sorte à ce que les élèves puissent se déplacer facilement dans la salle pour constituer les équipes lors des activités.
- Préparez votre connexion à internet, et ouvrez les pages web proposées dans "Pour aller plus loin" , liens page 4.

Déroulé de la séance

45 à 60'

Activité 1 10' (Avant le jeu INDUSTRIUM)

Brève discussion d'introduction :

Question 1 - D'après vous, quelles sont les pannes ou les problèmes qui pourraient arriver dans une usine connectée ?

Question 2 - Pensez-vous qu'un virus informatique puisse arrêter une machine ?

Aide pour l'enseignant.e :

Quelques exemples pour aider les élèves à répondre :

- Une attaque informatique peut bloquer les écrans de commande ou modifier des paramètres machines.
- Une panne réseau peut interrompre la communication entre les robots.
- Un mail frauduleux peut infecter tout le système de production.
- Un mot de passe trop simple peut permettre à quelqu'un de se connecter à distance.

Exemples réels à citer simplement :

- Une entreprise de l'énergie a déjà été paralysée pendant plusieurs jours à cause d'un ransomware.
- En 2017, le virus WannaCry a bloqué des usines automobiles et des hôpitaux dans plusieurs pays.

Pour animer :

- Proposez un mini-sondage : "Qui d'entre vous réutilise partout le même mot de passe?"
- Demandez : "Que feriez-vous si votre téléphone ou votre ordinateur était bloqué ?" pour introduire la notion de réaction en cas d'attaque.

Question 3 - A votre avis, comment peut-on se protéger d'une cyberattaque ?

Aide pour l'enseignant.e

Risque	Mesure de protection	Explication simple
Virus ou logiciel malveillant	Installer un antivirus, faire les mises à jour.	Empêche les logiciels dangereux d'agir.
Mot de passe faible	Créer un mot de passe long et complexe (12 caractères minimum).	Difficile à deviner ou pirater.
Intrusion réseau	Pare-feu, segmentation des systèmes.	L'attaquant ne peut pas accéder à tout.
Erreur humaine	Sensibilisation et formation du personnel.	La vigilance reste le meilleur bouclier.
Clé USB piégée	Ne jamais brancher un support inconnu.	Évite l'introduction de virus externes.

SIEMENS

Pour animer :

- Faites un petit quiz rapide :
  "À votre avis, quel est le mot de passe le plus sécurisé ?" (Ex. : azerty / 123456 / MonCh@t!2025).
- Soulignez que les usines, comme nos ordinateurs, ont besoin d'"antivirus" et de mises à jour régulières.

Activité 2 ⏱ 30' (Pendant le jeu INDUSTRIUM)

Consigne:

Pendant le jeu, les élèves repèrent **les cartes liées à la cybersécurité.**

Aide pour l'enseignant.e :

Élaboration du mini plan :
L'objectif est d'amener les élèves à comprendre que le digital n'est pas une fin en soi, mais un outil d'amélioration.

Pistes de réponses possibles :

1. Installer des capteurs intelligents pour suivre la consommation d'énergie et détecter les anomalies.
2. Créer un "jumeau numérique" de l'usine pour tester les changements avant de les appliquer en vrai.
3. Former les opérateurs aux nouveaux outils (tablettes, logiciels de supervision, programmation de robots).
4. Utiliser des données pour mieux planifier les arrêts de production ou la maintenance.
5. Automatiser certaines étapes tout en gardant un contrôle humain pour la sécurité et la qualité.

Pour animer :

- Attribuez à chaque groupe un rôle : directeur technique, ingénieur digital, opérateur, chef d'équipe.
- Chaque groupe doit présenter ses 3 actions en les justifiant (ex. "gain de temps", "moins d'erreurs", "plus de sécurité").

Activité 3 ⏱ 45' (Après le jeu INDUSTRIUM)

Consigne:

Chaque équipe imagine une cyberattaque fictive sur une usine et propose un plan d'action pour la contrer.

Aide pour l'enseignant.e :

Élaboration du scénario d'attaque - chaque groupe imagine :

- Le type d'attaque (virus, piratage, sabotage, vol de données).
- Ses conséquences (arrêt de la production, pertes financières, fuite de données, atteinte à la sécurité).
- Les solutions à mettre en place.

Exemples simples pour inspirer les élèves :

- "Un pirate envoie un e-mail piégé au service maintenance : un virus bloque les robots."
  → Solutions : sensibiliser, filtrer les mails, faire des sauvegardes.
- "Un employé branche une clé USB trouvée sur le parking."
  → Solutions : politique d'interdiction, formation du personnel, bornes sécurisées, antivirus.
- "Une panne du réseau coupe la communication entre les lignes de production."
  → Solutions : redondance réseau, maintenance préventive, surveillance automatique.

Pour animer :

- Demandez aux groupes de donner un nom de code à leur attaque (“Opération Bugzilla”, “Cyberstorm”, “Mission VirusX”).
- Encouragez la créativité mais gardez un ton humoristique pour éviter tout climat anxiogène.

Débat : Faut-il tout connecter dans une usine ?

Aide pour l’enseignant.e :

L’objectif est de pousser les élèves à réfléchir aux limites du “tout numérique”.

Arguments “Oui, il faut connecter”	Arguments “Non, il faut rester prudent”
Meilleure efficacité, suivi en temps réel.	Plus on connecte, plus on crée de portes d’entrée pour les hackers.
Maintenance plus rapide, alertes automatiques.	Dépendance aux réseaux et aux logiciels.
Meilleure coordination entre sites et équipes.	Perte d’autonomie si le système tombe en panne.

Pour animer :

- Divisez la classe en deux camps et laissez 5 minutes de préparation.
- Aidez les élèves à trouver des exemples du quotidien : “Serait-il raisonnable de connecter tout chez soi (voiture, frigo, serrure...) ?”
- Concluez : “**Le numérique est un formidable outil, mais il doit toujours être accompagné de vigilance.**”

Activité ludique complémentaire

Défi 1 - Inventer le mot de passe le plus fort du monde.

Pistes de réponses possibles :

- azerty → trop simple. ❌
- M@chine2025!Secure → mélange de lettres, chiffres, majuscules, symboles. ✅
- MonUsineNeTombeJamais! → long, personnel et mémorisable. ✅

Rappel : **plus un mot de passe est long, plus il est sûr.**

Défi 2 - Trouver 3 bons réflexes de cybersécurité pour les élèves et pour une usine.

Pistes de réponses possibles :

1. Ne pas ouvrir un mail suspect → ni en classe, ni au travail.
2. Sauvegarder régulièrement les fichiers importants.
3. Utiliser un mot de passe différent pour chaque compte.
4. Ne jamais brancher une clé USB inconnue.
5. Mettre à jour les logiciels et antivirus.

Pour aller plus loin

- Jeu en ligne : “FORINDUSTRIE, l’Univers extraordinaire” (possible de faire jouer la classe entière dans une compétition nationale gratuite) : cliquer ici ou entrez ce lien dans votre moteur de recherche : https://www.forindustrie.fr/

- 📘 Fiches métiers ONISEP : Experte en cybersécurité : cliquer ici ou entrez ce lien dans votre moteur de recherche : https://oniseptv.onisep.fr/video/experte-en-cybersecurite-dans-mon-job-les-metiers-du-numerique

- 🧠 Lecture : The Conversation – “La guerre silencieuse des hackers éthiques” : cliquer ici ou entrez ce lien dans votre moteur de recherche : https://theconversation.com/la-guerre-silencieuse-des-hackers-ethiques-253582

SIEMENS