

Découverte de la cybersécurité

Deviens enquêteur du numérique

SecuritIE

Au programme

1. Comprendre : ce qu'est la cybersécurité, et pourquoi ça vous concerne
2. Observer : une clé USB qui agit toute seule sur un ordinateur
3. Enquêter : des activités en ligne
4. Découvrir : les métiers de la cyber

C'est quoi la cybersécurité

Protéger des informations et des appareils contre ceux qui veulent les voler, les bloquer, ou vous espionner.

Une image simple : votre ordinateur est un château. Le mot de passe est le pont-levis. Le faux message, c'est l'espion déguisé qui passe la porte en se faisant passer pour un ami.

"Moi, je n'intéresse personne"

C'est faux. Vous êtes une cible intéressante :

- Un compte de jeu avec des objets rares, c'est de l'argent réel.
- Vos contacts deviennent des victimes pour l'arnaqueur.
- Votre machine sert à attaquer d'autres personnes.
- Vos photos et vos infos servent au chantage ou à l'usurpation.

Vrai ou faux

À main levée

Vrai ou faux

1. Un antivirus suffit à être protégé.
2. Si le cadenas est présent dans la barre d'adresse, le site est forcément sûr.
3. Supprimer une photo d'Internet, c'est définitif.
4. On peut deviner un mot de passe de six chiffres en moins d'une seconde.

Les dangers du quotidien

Phishing · Mot de passe · Clé USB · Données personnelles

Phishing

Le pirate se fait passer pour quelqu'un de confiance pour vous pousser à cliquer, à payer, ou à donner une information.

"Ton compte sera supprimé, confirme tes informations ici."

"Tu as gagné un cadeau, clique vite."

"Salut c'est maman, nouveau numéro, tu peux m'aider ?"

C'est l'attaque la plus répandue. Il suffit de mentir de façon crédible.

Phishing : les signaux d'alerte

1. L'urgence : "vite", "dernière chance", "compte bloqué".
2. Le trop beau : un cadeau, un gain, une offre incroyable.
3. Le lien bizarre : un domaine qui n'est pas le vrai site.
4. Les fautes et les formules étranges.
5. On vous demande une information personnelle ou un code.

Le site de l'enquête : mode d'emploi

À partir de maintenant, vous allez enquêter sur le site.

- Ouvrez l'adresse affichée, choisissez votre **numéro de groupe**.
- Pour chaque étape, je vous donne un **code d'accès**.
- Chaque étape est un exercice : résolvez-le pour valider.
- À la fin, chaque groupe repartira avec **une partie du code de sortie**.

Adresse : **securitiie.iens.net/jan**

Activité 1 — Le piège à clic

Code d'accès

Sera bientôt révélé

Mots de passe : combien de temps pour le casser

Votre mot de passe	Temps pour un pirate
123456 (six chiffres)	instantané
marius (six lettres)	quelques secondes
Marius2010	quelques heures
JaimeLesFrites&Le5Mai!	des milliers d'années

Ce qui rend un mot de passe sûr

- **La longueur d'abord** : une phrase de passe longue vaut mieux qu'un mot court et compliqué.
- **De la variété** : majuscules, minuscules, chiffres, symboles.
- **Rien de personnel** : ni prénom, ni date, ni nom d'animal, ça se devine.
- **Unique** : un mot de passe différent par site important.
- **Un gestionnaire** le retient à votre place, et **la double authentification** ajoute un verrou.

Activité 2 — Créez un mot de passe solide

Code d'accès

Sera bientôt révélé

La clé USB piégée

Une clé USB, un câble ou un objet connecté peuvent faire bien plus que stocker des fichiers.

Vos données personnelles

Tout ce que vous publiez raconte votre vie à des inconnus :

- Une photo de votre quartier montre votre adresse.
- Votre anniversaire, votre animal se devinent.
- Un like, un commentaire montrent vos habitudes.

Un enquêteur, ou un pirate, sait recouper ces miettes.

Données personnelles : les bons réflexes

- Des comptes en privé.
- Réfléchir avant de publier : est-ce que je l'afficherais sur la porte du collège ?
- Ne pas accepter les inconnus.
- Ne pas publier ses amis sans leur accord.

Activité 3 — L'enquête

Code d'accès

Sera bientôt révélé

Le code de sortie

Chaque groupe détient une partie du code.

Mettez vos parties en commun, dans l'ordre des numéros de groupe, pour reconstituer le **code de sortie**.

Le premier groupe qui le valide a bouclé l'enquête.

Comment un pirate opère

Une attaque, c'est une enquête à l'envers :

1. Il observe : il récolte vos infos sur les réseaux.
2. Il piège : faux message, clé USB, faux site.
3. Il entre : il devine ou vole vos accès.
4. Il agit : il vole, bloque, revend, ou fait chanter

Les métiers de la cyber

Il n'y a pas un métier, il y en a plusieurs

- Analyste SOC : surveille les alertes jour et nuit.
- Hacker éthique : payé pour attaquer et trouver les failles.
- Analyste forensic : reconstitue l'attaque, comme vous aujourd'hui.
- Architecte sécurité : construit les défenses.
- Réponse à incident : les pompiers du numérique.

Les réflexes à garder

1. Des mots de passe longs et différents, avec la double authentification.
2. Un message qui presse ou qui fait rêver : on s'arrête, on vérifie.
3. Un objet USB inconnu : on ne branche pas.
4. Avant de publier : est-ce que je l'afficherais au collège ?

Merci

Des questions ?