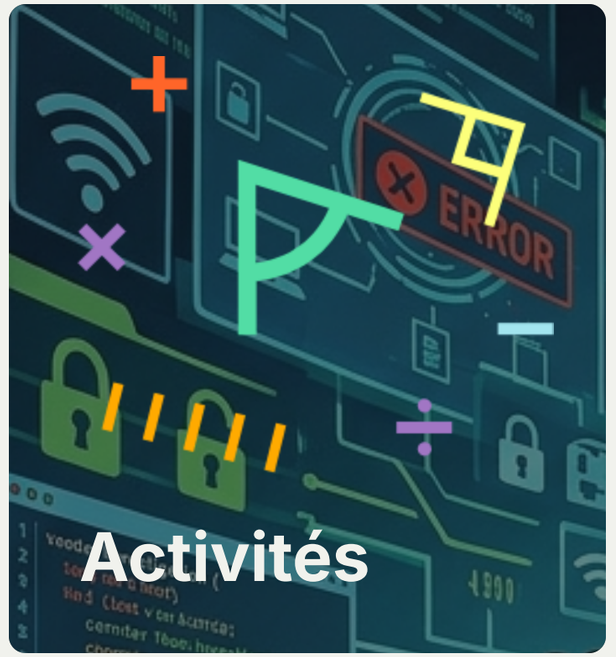
Les Cyber-Détectives sauvent l'école

Commencer

ENIGMATHICO

Cofinancé par
l'Union européenne

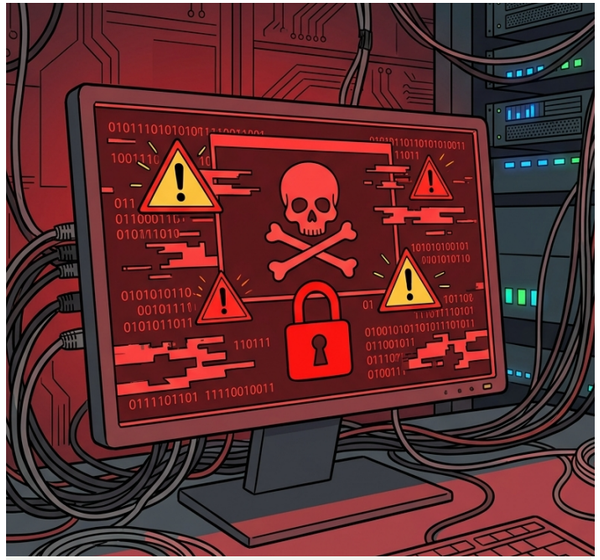


Activités

Glossaire

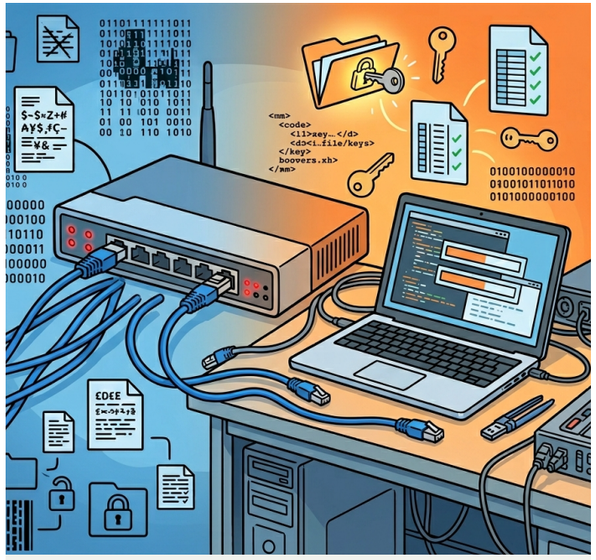
Bonus

Sommaire



Chapitre 1

Alerte rouge !



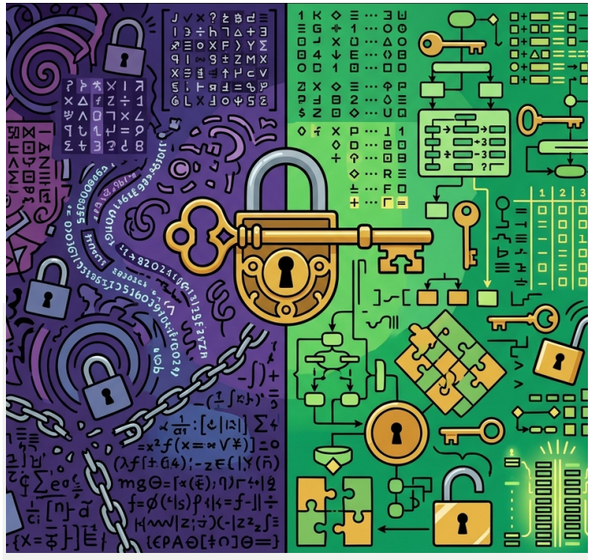
Chapitre 2

À la poursuite du hacker



Chapitre 3

Sauver les données



Chapitre 4

Reprendre le contrôle

Bonus

Les cryptomonnaies : comment ça marche ?



C'est quoi le Bitcoin ?



Cybersécurité et téléchargements



Activités - niveau 1



Activité 1

Anatomie d'un ordinateur



Activité 2

À la poursuite du routeur pirate



Activité 3

Sauver les données



Activité 4

Craque le code

Activités - niveau 2



Activité 1

Anatomie d'un ordinateur



Activité 2

À la poursuite du routeur pirate



Activité 3

Sauver les données



Activité 4

Craque le code

Glossaire



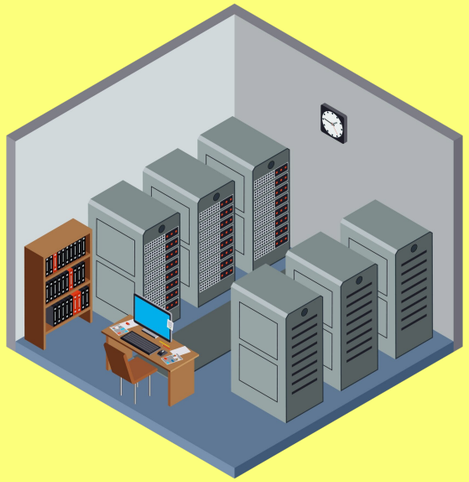
Un tableau de bord



Une cyberattaque



Un rançongiciel (ransomware)

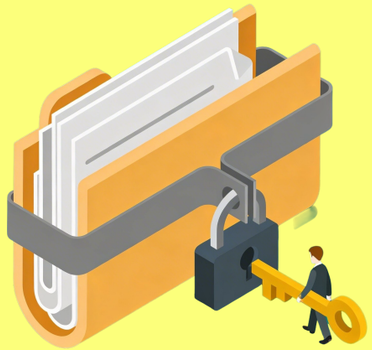


Une salle de serveurs

Glossaire



Un routeur



Le cryptage (ou le chiffrement)



L'ombre numérique



Un logiciel de déchiffrement

Glossary



Un pare-feu (firewall)

Un tableau de bord



Un **tableau de bord** est une page d’accueil qui rassemble des informations importantes. Au lieu de chercher dans plusieurs menus, tu as une vue d'ensemble claire et simple au même endroit.

Il regroupe différents éléments pour t'aider à t'organiser :

- **Des alertes** : tes nouveaux messages et notifications.
- **Un suivi** : ta progression dans ton travail et tes activités récentes.
- **Des outils** : tes paramètres pour régler et contrôler ton compte.
- **L'actualité** : les dernières mises à jour et les infos urgentes.

Le tableau de bord est conçu pour deux missions principales :

- **Voir** tout ce qu'il se passe en un seul coup d'œil.
- **Gérer facilement** : piloter ton travail et tes réglages sans perdre de temps.

Une cyberattaque



Une cyberattaque est une agression numérique pour voler des informations, piéger des utilisateurs ou paralyser des systèmes informatiques.

Les attaques les plus fréquentes

- **L'hameçonnage (phishing) :** De faux messages pour voler tes mots de passe.
- **Un virus :** Un programme malveillant qui abîme ou espionne un appareil numérique.
- **Le Sabotage :** Une technique pour bloquer un site web ou le mettre en panne.

Trois réflexes de protection

1. **Le Secret :** Garde tes mots de passe pour toi tout seul.
2. **La Méfiance :** Ne clique jamais sur un lien sans vérifier l'expéditeur.
3. **Alerter :** Un doute ? Un message étrange ? Parles-en tout de suite à un adulte.

Un rançongiciel (ransomware)



Le rançongiciel est un programme malveillant envoyé par des cybercriminels qui verrouillent des fichiers pour réclamer de l'argent (une rançon) en échange de leur déblocage.

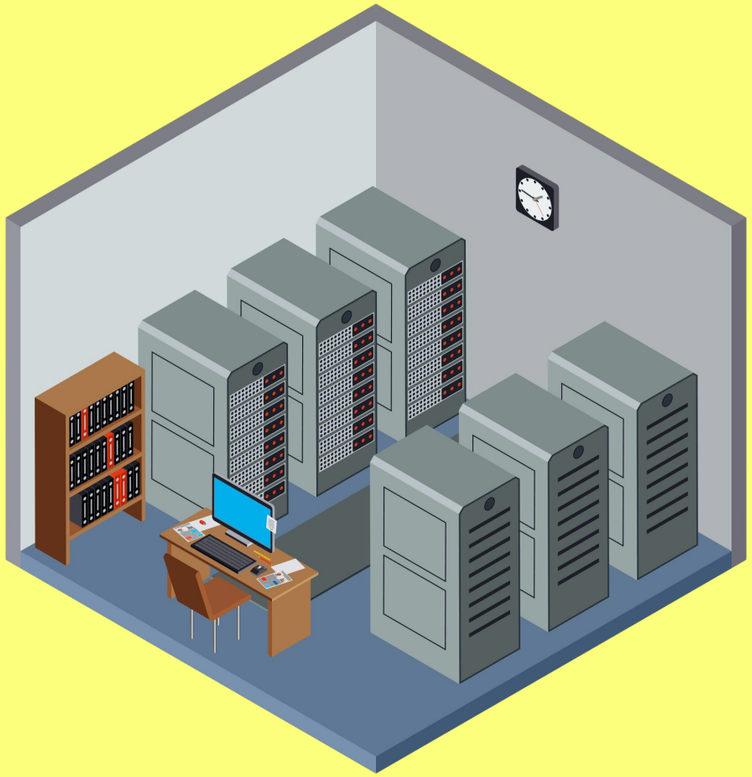
Comment fonctionne ce programme ?

- **Il bloque l'accès :** On ne peut plus ouvrir l'ordinateur ou la tablette.
- **Il rend les fichiers illisibles :** Il transforme le code de tes documents, photos et jeux (c'est du **chiffrement**).
- **Il menace :** Il affiche un message exigeant un paiement pour tout retrouver.

Trois réflexes de protection

1. **La Prudence :** Ne clique jamais sur un lien ou un fichier inconnu.
2. **L'Entretien :** Garde ton appareil et tes logiciels toujours à jour.
3. **Alerter :** Si un message te semble bizarre, appelle tout de suite un adulte.

Une salle de serveurs



C’est un lieu sécurisé qui abrite des ordinateurs particuliers que l'on appelle des serveurs. Contrairement aux ordinateurs de classe, ces machines fonctionnent jour et nuit pour faire tourner les services numériques de l'école.

<u>À quoi servent ces ordinateurs ?</u>

Ils remplissent plusieurs missions essentielles :

- **Gérer la connexion :** Ils pilotent le réseau Wi-Fi pour que tout le monde puisse accéder à Internet.
- **Stocker en sécurité :** Ils conservent les documents des professeurs et les données des élèves afin de pouvoir les retrouver.
- **Héberger les outils de travail :** Ils font fonctionner le portail de l’école et parfois les sites pour consulter les notes ou les devoirs.
- **Partager les ressources :** Ils permettent à chaque ordinateur de classe d'accéder facilement aux fichiers partagés.

Un routeur



Le **routeur** est un boîtier qui relie des appareils (ordinateur, tablette, téléphone) à Internet. Il leur permet aussi de communiquer entre eux.

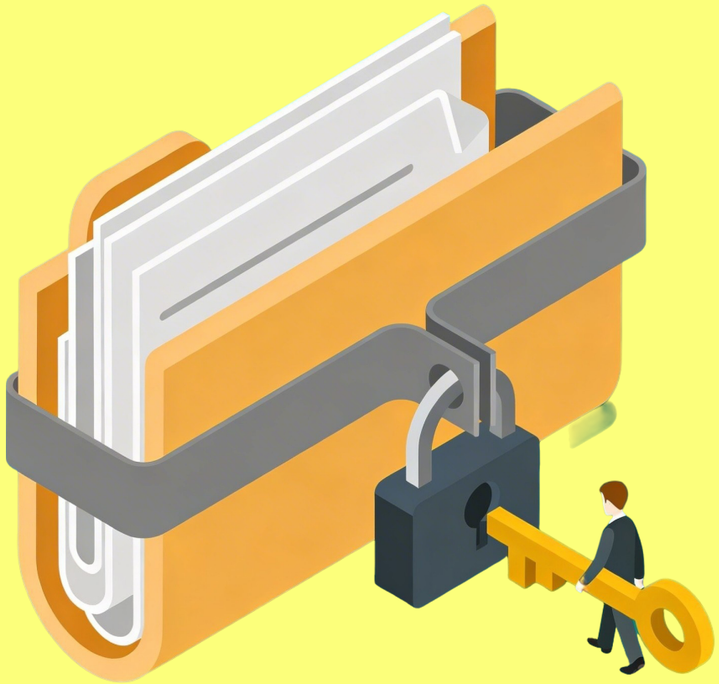
Il agit comme un **aiguilleur** : il dirige les informations (messages, photos, vidéos) vers le bon appareil pour que tout arrive à destination rapidement et sans erreur.

À quoi sert-il au quotidien ?

- **À la maison :** Il permet à toute la famille d'utiliser Internet en même temps sur différents écrans.
- **À l'école :** Il connecte tous les ordinateurs des classes au réseau Wi-Fi de l'établissement.

En résumé, dès que tu ouvres un site ou que tu envoies un message, c'est **le routeur qui s'assure que les données prennent le bon chemin**.

Le cryptage (ou le chiffrement)



Le cryptage (aussi appelé chiffrement) est l'action de **transformer un message normal en un message secret et illisible** pour tout le monde, sauf pour la personne qui possède **le code (appelé la clé)** pour le relire.

Sur internet et sur nos ordinateurs, on protège les fichiers et les données importantes en les chiffrant (cryptant), ce qui signifie que :

- Les informations sont transformées en un code secret,
- Elles ressemblent à des données aléatoires ou illisibles,
- Seule une personne ou un ordinateur possédant la bonne clé peut les ouvrir.

Ainsi tes données sensibles ou tes mots de passe sont protégés.

L'ombre numérique



L’ombre numérique, ce sont toutes les informations collectées automatiquement sur toi lorsque tu navigues sur Internet, souvent sans que tu le saches.
Contrairement à **l'empreinte numérique** (ce que tu choisis de poster), l'ombre se crée toute seule dès que tu es connecté.

Elle contient :

- Les sites que tu visites,
- Les vidéos que tu regardes,
- Les publicités sur lesquelles tu cliques,
- Les applications que tu ouvres.

<u>À quoi sert-elle ?</u>

Ces données sont principalement utilisées pour :

1. **Personnaliser ton écran :** Te proposer des vidéos ou des publicités qui correspondent à tes goûts.
2. **Analyser tes habitudes :** Comprendre comment et pourquoi tu utilises ton appareil.

Un logiciel de déchiffrement



Un logiciel de déchiffrement est un **programme** utilisé pour **déverrouiller des fichiers ou des données chiffrés (codés)** afin qu'ils puissent être lus à nouveau (contrairement aux outils de chiffrement, il retransforme un code secret en informations normales).

Il fonctionne en :

- Utilisant une clé spéciale ou un mot de passe,
- Reconvertissant les données codées en fichiers lisibles,
- Ouvrant des informations telles que des textes, des images ou des documents.

Il est utilisé pour :

- Accéder à des informations protégées ou verrouillées,
- Récupérer et lire des fichiers sécurisés en toute sécurité.

Les logiciels de déchiffrement permettent de retransformer des données cachées sous une forme que vous pouvez comprendre.

Un pare-feu (firewall)



Le **pare-feu** est un **logiciel de sécurité** qui agit comme un bouclier. Il surveille les informations numériques qui entrent et sortent d'un ordinateur ou sur un réseau.

Comment fonctionne-t-il ?

- Il filtre les accès, et **bloque les connexions suspectes** ou dangereuses.
- Il laisse **circuler librement les données de confiance**.
- Il surveille le trafic, et vérifie l'identité de chaque information qui tente de passer.

Le pare-feu est utilisé pour :

- Faire barrage : **il arrête les virus** et les cyberattaques avant même qu'ils n'atteignent ton appareil.
- **Protéger ta vie privée** : il empêche des personnes malveillantes de venir fouiller dans tes fichiers personnels.

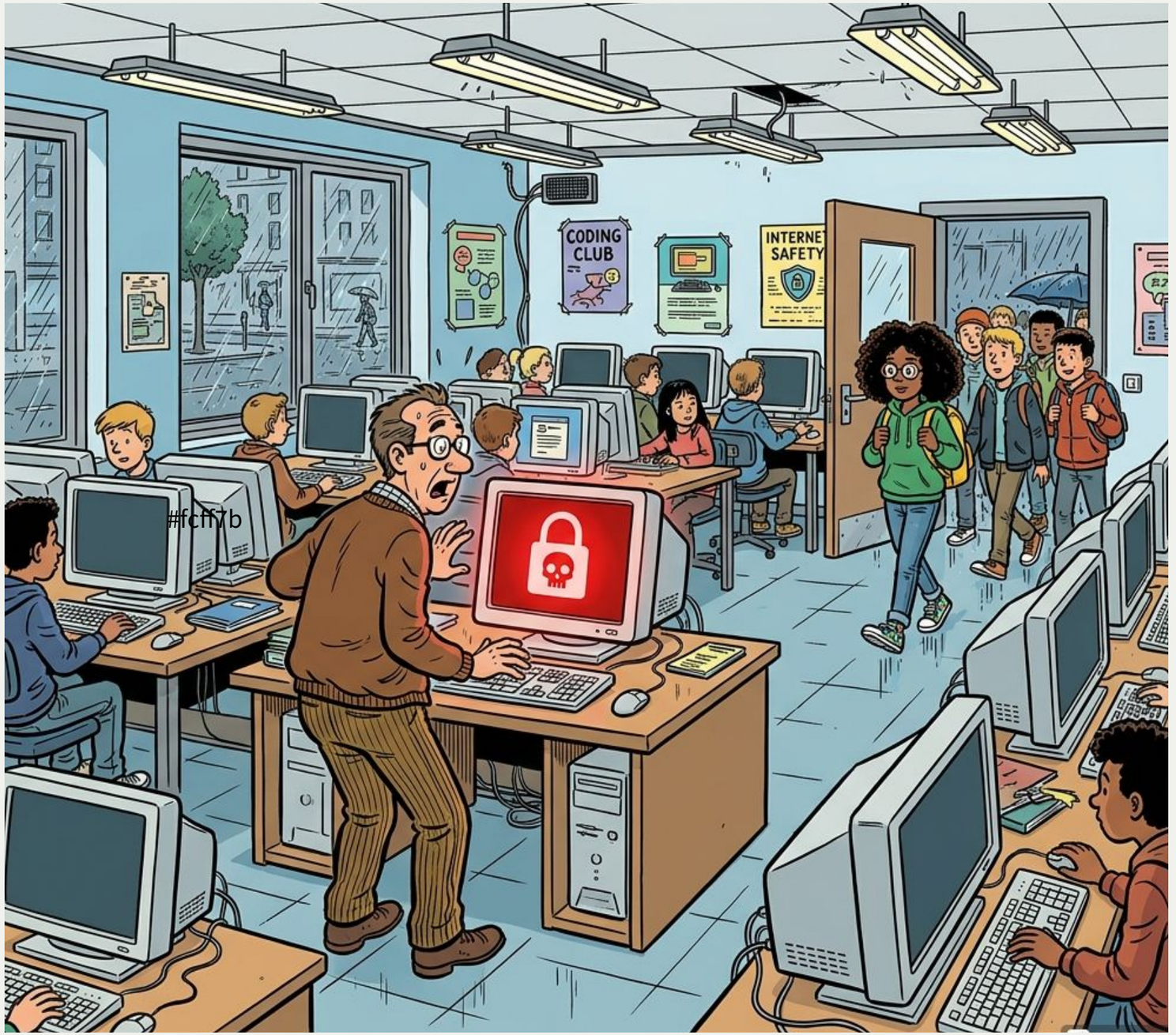
C'est la première ligne de défense de ton ordinateur.

Chapitre 1

Alerte rouge !

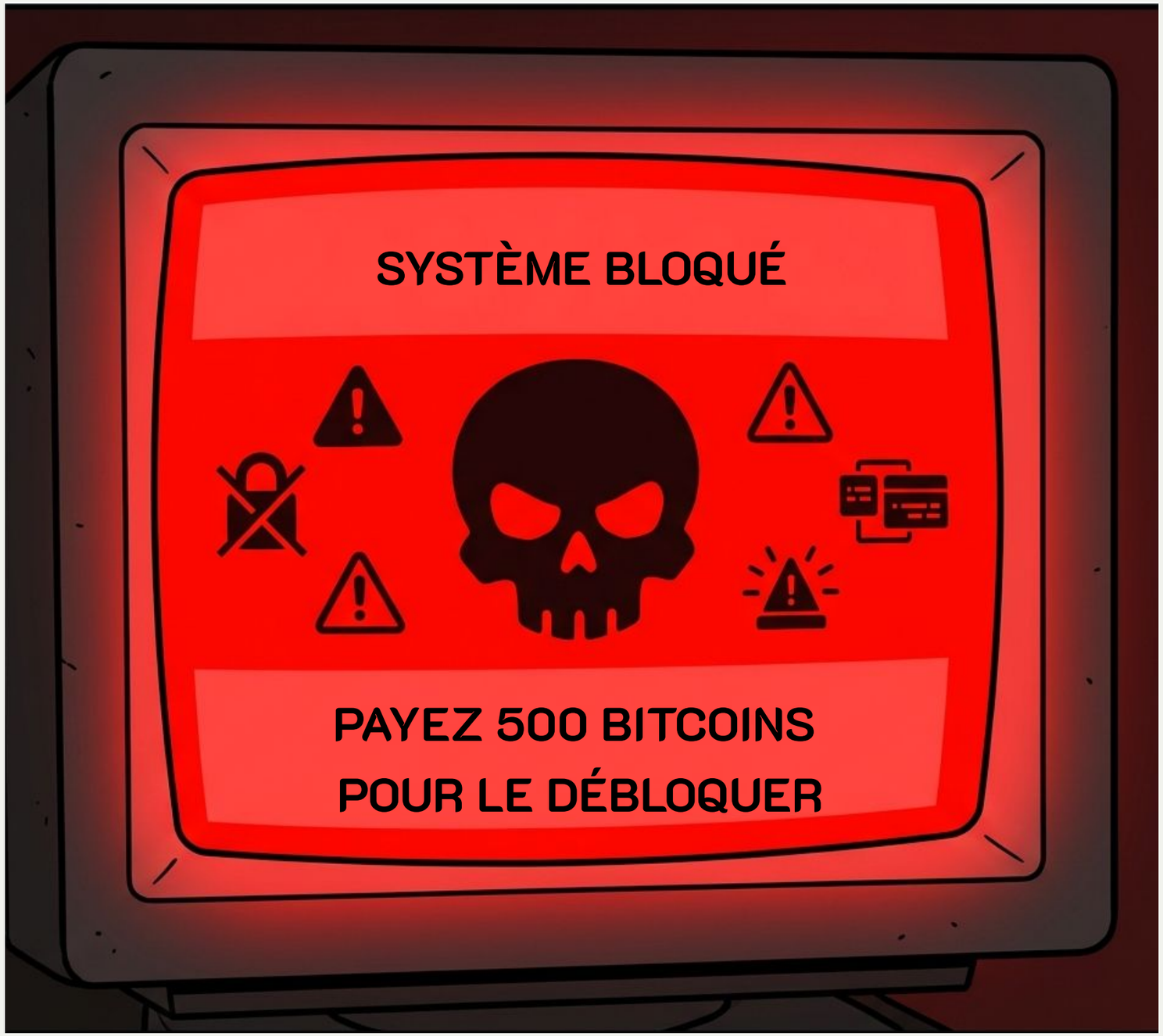


Tout commença un lundi pluvieux, au collège de Maple Grove. Tandis que les élèves s’installaient dans la salle informatique, les lumières se mirent à vaciller.
Alors que M. Parker tentait d’accéder **au tableau de bord** des élèves, l’écran vira brusquement au rouge écarlate.



SYSTÈME BLOQUÉ
PAYEZ 500 BITCOINS POUR LE DÉBLOQUER

M. Paker hoqueta de surprise :
— Que se passe-t-il ?
Ça ressemble à une **cyberattaque** !



M. Parker se précipita hors de la classe pour prévenir le directeur.

Un à un, tous les ordinateurs de l’école arrêtèrent de fonctionner. Plus d’internet. Plus d’applications d’apprentissage. Même la sonnerie restait silencieuse !

Dans les couloirs, c'était la pagaille.



Au fond de la salle, les élèves échangèrent des regards éberlués. Zara, passionnée de programmation, fronça les sourcils.

— Notre école vient d'être victime d'un **rançongiciel**, déclara-t-elle.

— Un rançon-quoi ? demanda Toby, qui préférait de loin les jeux vidéo à la technique.

— C’est un logiciel malveillant, expliqua Zara. Il verrouille tous les systèmes informatiques.



— Le rançongiciel est un acte criminel. Il faut payer une rançon pour récupérer nos outils informatiques, ajouta Lin, l'expert en sécurité du groupe. C'est vraiment grave.

David, qui aimait les énigmes, se leva à son tour :

— Nous devons trouver une solution avant que l'école ne soit complètement paralysée.



Activité 1

Anatomie d'un ordinateur



Niveau 1

Matériel

Feuille de mission
Les cartes Matériel informatique

Télécharger

Activité 1

Anatomie d'un ordinateur



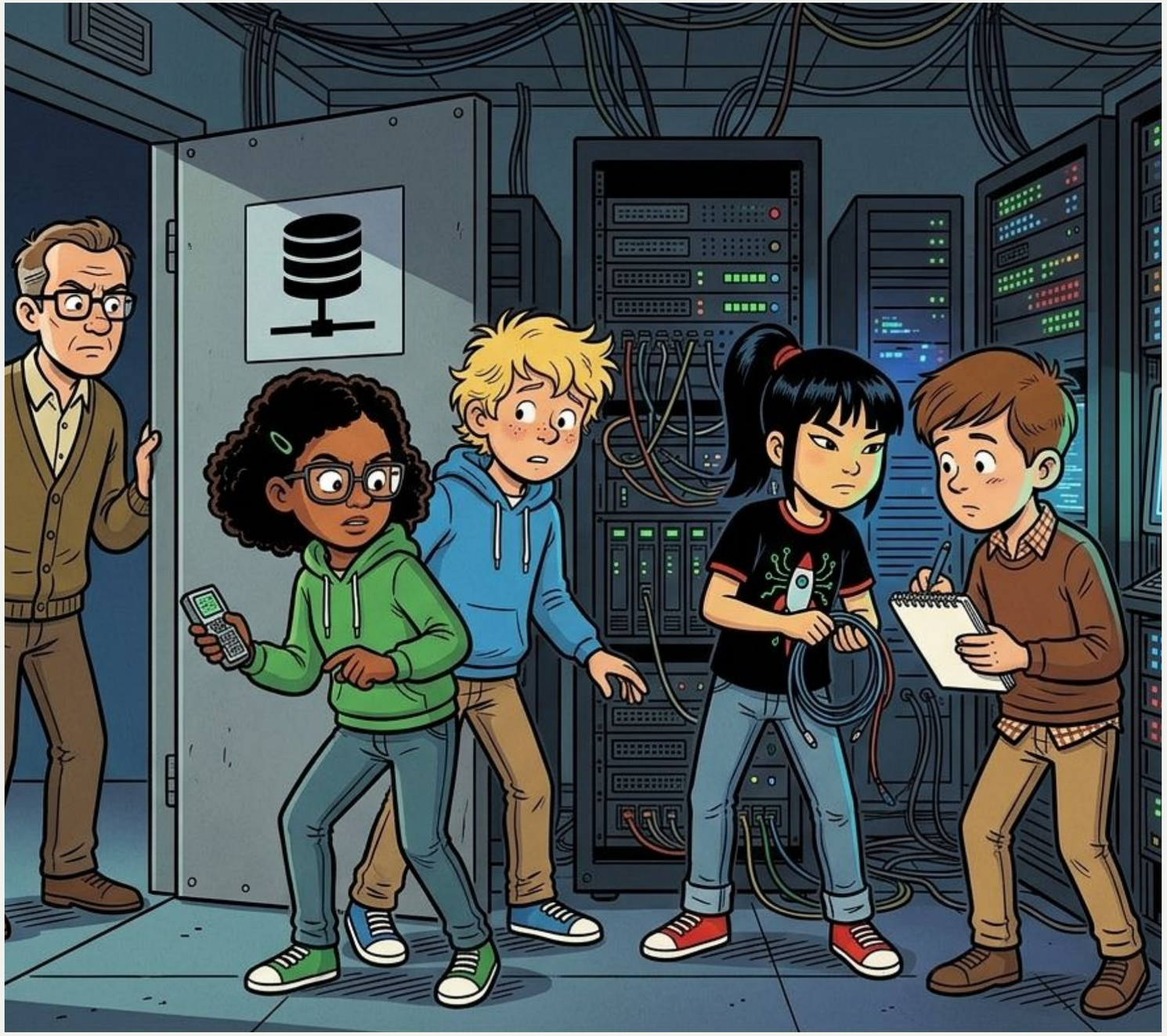
Niveau 2

Matériel

Feuille de mission
Les cartes Matériel informatique

Télécharger

Les Cyber-Détectives décidèrent alors de mener l'enquête. Sous l'œil vigilant de M. Parker, ils se faufilèrent dans **la salle des serveurs**, en promettant de ne toucher à aucun équipement sans autorisation.



Lin lança un scan du réseau sur son ordinateur portable.

— Un appareil étrange est connecté au Wi-Fi de l’école, murmura-t-elle. Il est identifié comme… "Imprimante_Invité". Mmmm… Ce n'est pas un appareil de l’école.



Ils décidèrent de suivre le signal Wi-Fi, qui les mena jusqu’au cagibi de l’agent d’entretien.

— Ici !



Caché derrière les produits d’entretien, un petit ordinateur était relié par une série de câbles à un **routeur** pirate.

— Quelqu'un l'a installé ici en secret, chuchota Zara.

L'équipe devait absolument neutraliser l'appareil avant que d'autres données ne soient dérobées.



Activité 2

À la poursuite du routeur pirate



Niveau 1

Matériel

Feuille de mission

Télécharger

Activité 2

À la poursuite du routeur pirate



Niveau 2

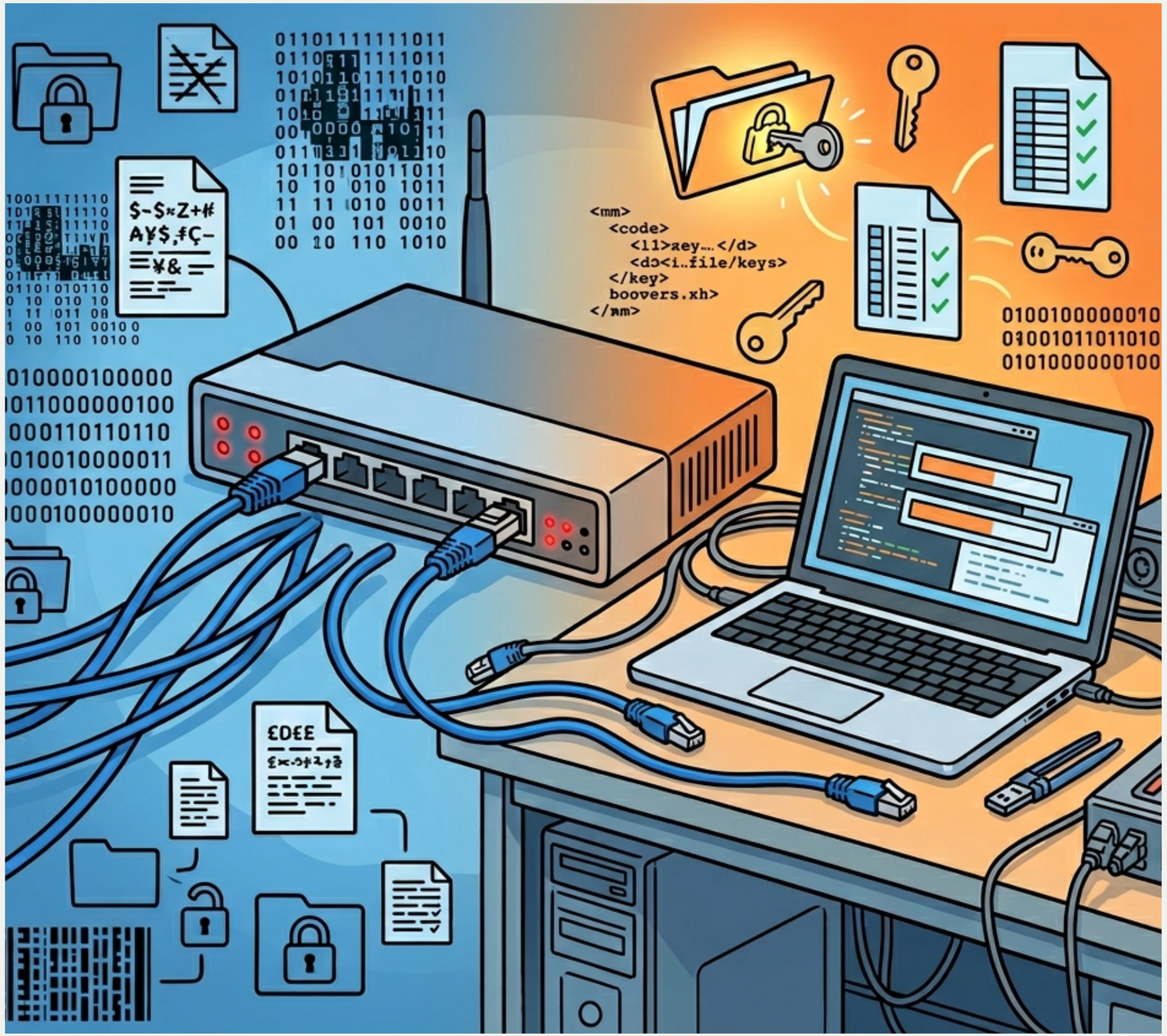
Matériel

Feuille de mission

Télécharger

Chapitre 2

À la poursuite du hacker



Une fois le routeur éteint, David le débrancha avec précaution ; tandis que Zara, penchée sur son clavier, isolait l’ordinateur du réseau principal de l'école.

— Nous avons empêché l'attaquant de voler davantage d'informations, expliqua-t-elle. Mais le mal est fait. Maintenant, nous devons **récupérer nos données**.



— Waouh ! Vous êtes incroyables tous les deux ! Le message de rançon a disparu ! s’exclama Lin.

— Maintenant, nous devons analyser les dégâts, ajouta Zara. L'intrus a volé certaines de nos informations sur l'usage d'Internet et des réseaux sociaux depuis le serveur de l'école.



Chapitre 3

Sauver les données



Sur internet, chacun laisse derrière lui une **ombre numérique** faite de données et d’informations personnelles. Et ces informations sont une monnaie précieuse.

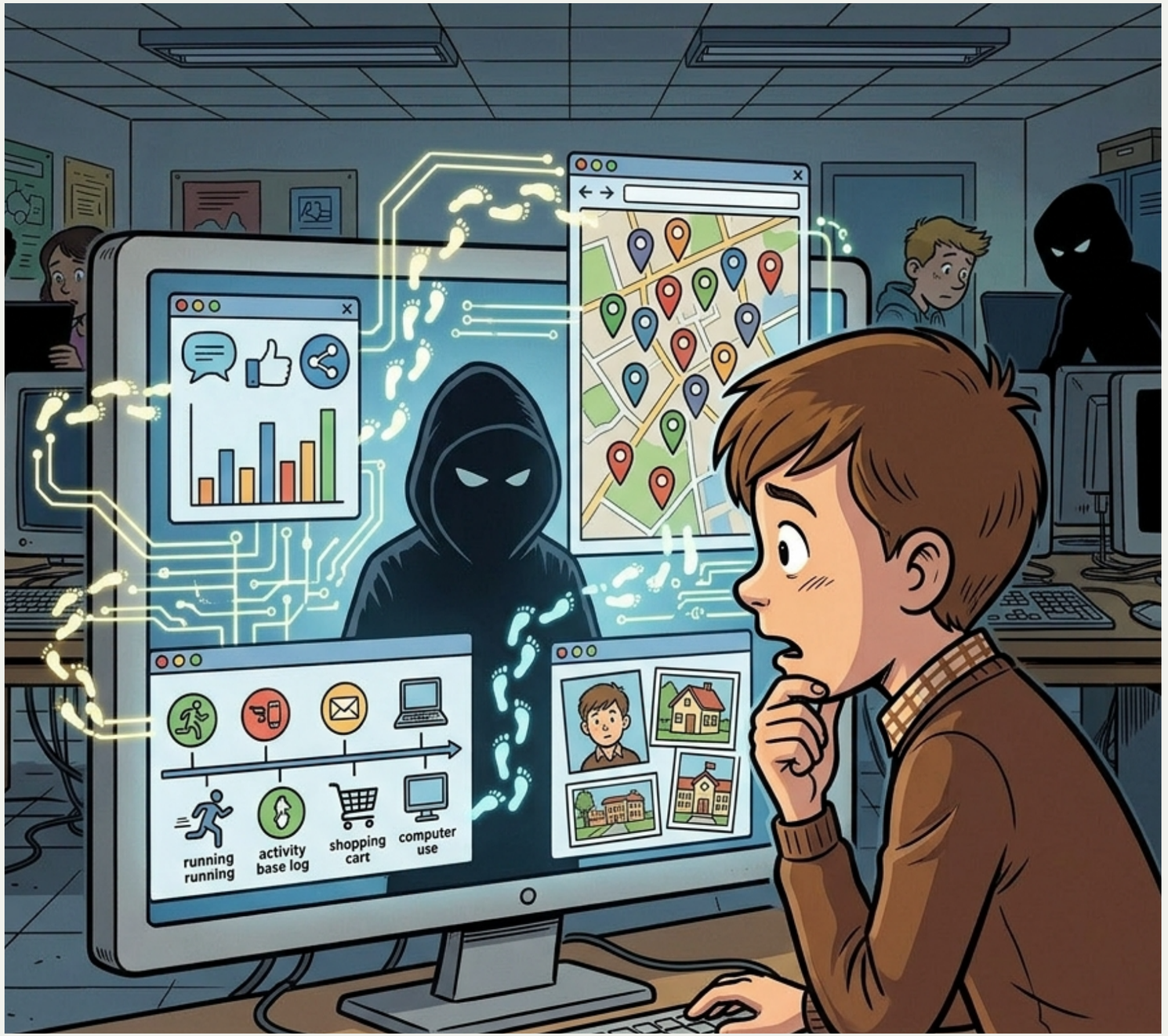
Un mot de passe divulgué n’est pas qu'une simple suite de caractères. C’est le premier domino d'une réaction en chaîne, la clé capable de déverrouiller un coffre-fort d'informations privées.



Pour l’administration de l’école, les données de Zara n'étaient que de simples fichiers : des notes d'évaluations, des listes de présence et un carnet de santé. Mais entre les mains d’un pirate, ces informations se transformaient en une redoutable menace.

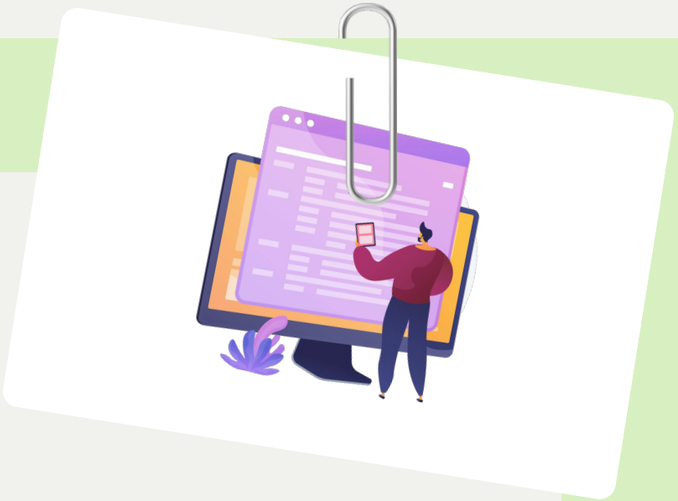
En fixant l’écran, David s'exclama :

— Je n’aurais jamais imaginé laisser autant de traces de moi sur Internet !



Activité 3

Sauver les données



Niveau 1

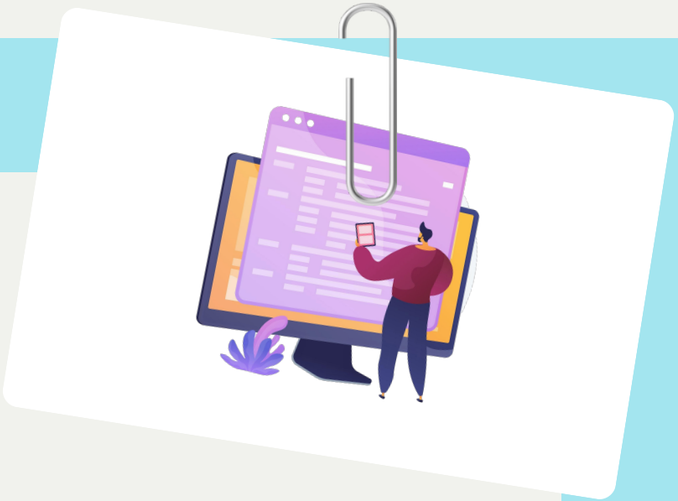
Matériel

Feuille de mission

Télécharger

Activité 3

Sauver les données



Niveau 2

Matériel

Feuille de mission

Télécharger

— Nos données sont sauvées ! s'écria Zara. Mais nous n'avons toujours pas accès au **tableau de bord** de l'école…

— Ouf ! J’ai eu tellement peur que les dossiers de l’établissement soient perdus pour de bon, avoua David avec un grand soupir de soulagement.



Chapitre 4

Reprendre le contrôle



Le pirate informatique avait verrouillé les fichiers de l’école avec un code long et complexe. Zara en téléchargea un échantillon dans son **logiciel de déchiffrement**.

— C’est un système très sophistiqué, observa-t-elle avec inquiétude. Mais regardez bien… il y a un motif qui se dessine.

David se pencha sur l'écran, les yeux écarquillés.

— C’est une séquence qui se répète ! s'exclama-t-il. C’est un grand classique du chiffrement !



Activité 4

Craque le code



Niveau 1

Matériel

Feuille de mission

Télécharger

Activité 4

Craque le code



Niveau 2

Matériel

Feuille de mission

Télécharger

Ensemble, ils parvinrent à craquer le code. Cela leur prit plus d'une heure et un paquet entier de biscuits de secours, mais ils réussirent enfin à déverrouiller les fichiers.

— Et paf ! Prends ça, espèce de vandale numérique ! s'exclama Zara, ravie. On a stoppé ton attaque !

— Allez, maintenant, on renforce le **pare-feu** pour qu'il ne puisse plus jamais revenir, ajouta Toby avec un clin d'œil. C'est super amusant, en fait !



Le lendemain, l'enquête de police révéla que l'auteur des faits était un ancien élève de l'établissement. Renvoyé quelques mois plus tôt, il avait agi par simple désir de vengeance.



Quelques jours plus tard, un évènement fut organisé pour honorer les Cyber-Détectives. Sous les applaudissements, M. Parker leur remit un badge étincelant !

— Grâce à votre ingéniosité et à votre courage, nous avons stoppé une menace majeure, déclara-t-il fièrement. Désormais, nous allons renforcer toute la cybersécurité de l'école.

Les quatre amis se tapèrent dans la main, le sourire aux lèvres.

— Est-ce qu'on aura droit à des points bonus pour avoir sauvé tout l'établissement ? plaisanta Toby.

Tout le monde éclata de rire, mais Zara, elle songeait déjà à leur prochaine énigme.





ENIGMATHICO

Cofinancé par
l'Union européenne

Financé par l'Union européenne. Les points de vue et avis exprimés n'engagent toutefois que leur(s) auteur(s) et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne sauraient en être tenues pour responsables.