

Escape game



<https://dgxy.link/cybersecurity>

Livret pédagogique

L'escape game Cybersécurité est principalement destiné aux élèves de primaire et de collège, à partir du cycle 3. Il a pour vocation de sensibiliser ceux-ci aux enjeux de la cybersécurité, dans le cadre du CRCN.

Au travers des différentes ressources et activités proposées, il s'agira pour les élèves de construire des compétences et d'acquérir les premiers éléments d'acculturation numérique relatifs à cette thématique.

Ce livret pédagogique reprend le déroulement de l'escape en précisant les objectifs visés, la nature des supports utilisés et les notions ciblées dans les activités interactives. Il y est également précisé les codes de déverrouillage permettant de passer d'une mission à l'autre.

Le temps nécessaire pour réaliser l'escape game dans sa totalité est d'environ 1 heure. Mais cela peut varier en fonction des classes.

En classe, l'enseignant pourra rappeler l'importance de suivre attentivement les consignes, éventuellement de prendre des notes et de bien lire les « feedbacks » en cours d'activité. En effet, ces derniers contiennent des commentaires qui contribuent à la compréhension des notions. En fin d'activité, les codes de déverrouillage indispensables à la progression dans le jeu sont affichés. Les élèves devront y être attentifs.

L'escape game est ainsi composé de 7 missions : 6 missions thématiques et 1 mission finale qui reprend l'essentiel des notions abordées. Une fiche « Carte d'expert(e) en cybersécurité » est téléchargeable en fin de parcours ainsi que la fiche synthétique de la CNIL « Cyber réflexes – Se protéger sur internet ».

Domaines du CRCN :



Spécifiquement, le thème de la cybersécurité relève du domaine 4 du CRCN.

Le tableau de synthèse qui fournit des Repères pour l'évaluation des compétences numériques est disponible sur Eduscol :

<https://eduscol.education.fr/document/20395/download>

Ce document permet d'identifier que les 3 premiers niveaux de maîtrise sont travaillés tout au long de cet escape game.

Sommaire

	Thématiques	Activités	Codes
Mission 1	Les mots de passe	Quiz	data
Mission 2	L'environnement informatique	Quiz	cyber
Mission 3	La vie privée et les données personnelles	Quiz	identité
Mission 4	Le piratage	Question unique	282395
Mission 5	L'usurpation	Appariement	vigilance
Mission 6	Les bonnes pratiques	Question unique	numérique
Mission finale	Synthèse	Mots croisés	cryptologie

Activité 1

- Objectif visé : savoir construire un mot de passe solide

- Support utilisé : application GbdIm2p créée par Cyril Iaconelli, distribuée sous licence CC-BY (site web <https://www.lmdbt.fr/>)
 - Activité interactive : quiz H5P
 - 1 : Un mot de passe de 8 caractères est considéré comme solide ?
 - Réponse attendue :
 - Faux
 - 2 : "sympalecarnaval" n'est pas un bon mot de passe car : (plusieurs choix sont possibles)
 - Réponses attendues :
 - Il est composé de mots du dictionnaire.
 - Il n'y a pas de majuscules.
 - Il n'y a pas de caractères spéciaux ni de chiffres.
 - 3 : Stocker tous ses mots de passe dans un carnet est une excellente idée.
 - Réponse attendue :
 - Faux
 - Seuil de réussite : 75%
 - Code obtenu dans le feedback : **data**
-

Mission 2

- Objectif visé : connaître les dispositifs de protection des matériels informatiques.
- Support utilisé : vidéo 1 jour, 1 question « C'est quoi une cyberattaque ? »
- Activité interactive : quiz H5P
 - Quels outils ou applications permettent de protéger un ordinateur ?
 - Réponses attendues :
 - Un antivirus

- Un mot de passe administrateur
- Un pare-feu
- Le système d'exploitation de mon appareil me propose de faire une mise à jour de sécurité.

Quelles sont les bonnes habitudes à adopter ?

- Réponses attendues
 - Je l'installe aussitôt
 - Je programme l'automatisation des mises à jour
 - Seuil de réussite : 75%
 - Code obtenu dans le feedback : **cyber**
-

Mission 3

- Objectif visé : comprendre les enjeux de la protection de la vie privée et des données personnelles
- Support utilisé : vidéo 1 jour, 1 question « Quels sont les dangers d'internet ? »
- Activité interactive : quiz H5P
 - Hier soir, Marc s'est rendu compte qu'un coéquipier de son équipe de tennis avait mis en ligne des photos de lui sans lui demander la permission...
 - Réponse attendue :
 - B. Marc lui demande de les effacer
 - Quand Virginie va sur Internet, elle hésite toujours pour « accepter les cookies » ...
 - Réponse attendue
 - A. Elle devrait les refuser
 - Quand Adrien fait du paddle à la mer, il envoie souvent des photos à son ami Manu.

Sans lui poser la question, Manu peut savoir précisément sur quelle plage Adrien se trouvait.

- Réponse attendue
 - Vrai
 - Isabelle regarde un tuto de bricolage. Quel sera le sujet du tuto suivant ?
 - Réponse attendue
 - A. La dernière perceuse à percussion qui vient de sortir.
 - Que fais-tu si tu reçois un message d'un inconnu ?
 - Réponse attendue
 - C. Comme dans la rue, tu ne réponds jamais à un message d'une personne inconnue.
 - Michel joue souvent en réseau sur son jeu préféré. Le prochain tournoi est avec des inconnus...
 - Réponse attendue
 - B. Mauvaise idée.
 - Seuil de réussite : 75%
 - Code obtenu dans le feedback : **identité**
-

Mission 4

- Objectif visé : savoir ce qu'est un piratage informatique
- Support utilisé : vidéo 1 jour, 1 question « C'est quoi le piratage informatique ? »
- Activité interactive : question unique
 - Comment s'appelle la personne qui réalise une cyberattaque ?
 - Réponse attendue :
 - Pirate

- Code à former avec les lettres mobiles composant le mot « pirate » : **282395**
-

Mission 5

- Objectif visé : savoir ce que sont les messages indésirables et frauduleux
 - Supports utilisés : vidéo Vinz et Lou sur Internet : « Spam attack » et vidéo « La famille tout écran « Comment éviter les arnaques du web ? »
 - Activité interactive : appariements Learning apps (associer chaque mot à sa définition)
 - Spam : courrier indésirable envoyé en masse à des fins publicitaires ou commerciales.
 - Arnaque : technique malveillante utilisée par un pirate pour très souvent récupérer de l'argent.
 - Hameçonnage / Phishing : technique malveillante utilisée par un pirate pour récupérer, par la tromperie, des données personnelles.
 - Malveillant(e) : qui a l'intention de nuire à quelqu'un
 - Usurpation : action illicite qui vise à se faire passer pour quelqu'un d'autre
- Code obtenu dans le feedback : **vigilance**
-

Mission 6

- Objectif visé : identifier les bonnes pratiques en matière de numérique
- Activité interactive préalable : jeu de catégorisation Learning apps
 - Réponses attendues :
 - Plutôt sans risque !
 - Regarder des dessins animés sur Okoo (France TV)
 - Télécharger un patch de jeu vidéo sur le site officiel de l'éditeur.

- Acheter ou louer un film en VOD.
- Lire des articles sur Vikidia.
- Une page Youtube avec un(e) chanteur(euse) connu(e)
- Installer un bloqueur de publicités.
- Problématique !
 - Télécharger un patch de jeu vidéo sur un forum et désactiver son antivirus pour pouvoir l'installer.
 - Télécharger un film sur un site de torrent.
 - Ouvrir une pièce jointe avec ce genre d'extensions de fichiers : .pif, .com, .bat, .exe, .vbs, .lnk, .scr ou .cab.
 - Télécharger une vidéo de Youtube.
 - Télécharger une photographie sur le site d'un photographe professionnel.
- Support utilisé : Fiche Ministère de l'Intérieur « Les bonnes pratiques pour se protéger des stealers »
 - Question : mot anglais pour dire « dérobeur » ?
 - Réponse attendue : stealer
 - Code obtenu avec le cryptex : **numérique**


Mission finale

- Objectif visé : faire la synthèse sur l'essentiel des notions qui ont été abordées dans le jeu
- Activité interactive Learning apps : mots croisés (la saisie est forcée en majuscules, l'orthographe et la ponctuation sont exigées, notamment les accents, la cédille, le trait d'union)
 - 1 – Nom anglais pour désigner un pirate informatique : HACKER

- Indice : vidéo 1 jour 1actu « C'est quoi une cyber-attaque ? »
- 2 – Application qui filtre les connexions entrantes et sortantes d'une machine : PARE-FEU
 - Indice : vidéo 1 jour 1actu « C'est quoi une cyber-attaque ? »
- 3 - Somme d'argent exigée par un pirate pour arrêter une cyberattaque : RANÇON
 - Indice : vidéo 1 jour 1actu « C'est quoi une cyber-attaque ? »
- 4 - Programme informatique malveillant : VIRUS
 - Indice : vidéo « Les programmes malveillants »
- 5 - Ensemble des ordinateurs d'une école, d'une entreprise : RÉSEAU
 - Indice : C'est pas sorcier « Qu'est-ce qu'un réseau »
- 6 - Logiciel qui détecte un programme malveillant : ANTIVIRUS
 - Indice : vidéo « Les programmes malveillants »

- Code obtenu dans le feedback : **cryptologie**

« Goodie »



**EXPERT(E) EN
CYBERSÉCURITÉ**

Photo :

Nom :
Prénom :

École ou
Collège :

Classe :

Date :

Signature :

<https://nuage03.apps.education.fr/index.php/s/akqmL5zcEcj3ZwS>



Fiche synthèse de la CNIL « Cyber réflexes, se protéger sur internet »

CYBER RÉFLEXES

Se protéger sur Internet

1 DES MOTS DE PASSE SOLIDES ET DIFFÉRENTS POUR CHAQUE COMPTE TU CHOISIRAS

Un mot de passe c'est comme une clé propre à chaque porte, elle te protège de l'intrusion. Si tu te fais voler un mot de passe que tu utilises pour différents sites web ou applications, ils pourront tous être piratés !

BONNES PRATIQUES

- Utiliser des mots de passe suffisamment longs, complexes et surtout différents pour chaque compte.
- Les garder secrets et privilégier un gestionnaire de mots de passe sécurisé pour les conserver.

2 LES MISES À JOUR DE TES APPAREILS SANS TARDER TU FERAS

Les failles de sécurité de tes logiciels, applications et matériels sont comme des portes laissées ouvertes pour les pirates. Ils peuvent les utiliser pour accéder à tes données personnelles ou les voler.

BONNES PRATIQUES

- Faire les mises à jour des logiciels, applications et appareils, dès qu'elles te sont proposées pour corriger leurs failles de sécurité.
- Activer les options de mises à jour automatiques chaque fois que c'est possible.

3 EN LIGNE, LE MOINS POSSIBLE SUR TON IDENTITÉ TU DIRAS

Publier et partager des données personnelles sur Internet (nom, prénom, adresse mail, photos, vidéos, vocaux...) peut les exposer à une utilisation malveillante.

BONNES PRATIQUES

- Éviter de divulguer tes données personnelles et celles de tes connaissances.
- Vérifier les paramètres de confidentialité de tes comptes pour définir ce qui peut être visible par les autres.

4 EN LIEU SÛR, UNE COPIE DE TES DONNÉES TU CONSERVERAS

Copier tes données, c'est les sauvegarder pour éviter de les perdre en cas de piratage, de vol, de panne ou de casse de tes appareils.

BONNE PRATIQUE

- Penser à faire régulièrement des sauvegardes de tes données sur un autre support (clé USB, disque externe, cloud...) pour pouvoir les retrouver en cas de problème.

5 DES MESSAGES INATTENDUS ET ALARMANTS TOUJOURS TU TE MÉFIERAS

L'hameçonnage ou phishing, ce sont des messages (courriels, SMS, réseaux sociaux) ou appels d'escrocs qui se font passer pour un organisme familier (banque, administration...). Ces arnaques visent à te voler des informations personnelles et bancaires, te faire télécharger un virus ou directement l'escroquer.

BONNES PRATIQUES

- Toujours te méfier et ne pas te précipiter pour cliquer ou répondre.
- Vérifier toujours l'information par toi-même, en te connectant à ton compte sur le service concerné.

6 LES CONTENUS PIRATÉS OU NON OFFICIELS TU ÉVITERAS

Des virus qui peuvent pirater tes appareils ou tes comptes sont souvent présents dans les logiciels ou jeux piratés, les extensions de triche de jeux vidéo, les sites de streaming illégaux...

BONNES PRATIQUES

- Ne pas télécharger des contenus illégaux ni des solutions non officielles.
- Installer uniquement des applications depuis les sites ou magasins officiels des éditeurs.

RÉPUBLIQUE FRANÇAISE
 MINISTÈRE DE LA JUSTICE

CYBER MALVEILLANCE GOUVERNEMENT

CNIL
 COMMISSION NATIONALE
 INFORMATIQUE ET LIBERTÉS

CYBER MOIS

PLUS DE CONSEILS SUR
 CNIL.FR
 CYBERMALVEILLANCE.GOUV.FR

https://www.cnil.fr/sites/cnil/files/2023-10/poster_cyber-reflexes2023.pdf



Parcours Éléa

Cet escape game a fait l'objet d'une déclinaison en parcours sur la plateforme de e-éducation Éléa, disponible pour tous les enseignants de l'académie de Normandie, permettant ainsi le suivi personnalisé du travail de l'élève par l'enseignant.

Pour plus d'informations, vous pouvez vous rendre sur le site de la DRANE de Normandie « Enseigner avec le numérique » :

<https://drane.ac-normandie.fr/>