Introduction à la Cybersécurité dans le milieu scolaire

1.0 Mai 2025

Webinaire numérique de la Drane

RÉGION ACADÉMIQUE PAYS DE LA LOIRE
Liberté
Égalité
Fraternité

Délégation régionale académique au numérique éducatif

Drane Nantes

Table des matières

Objectifs

- Sensibilisation à la cybersécurité dans le milieu scolaire
- Identifier les bonnes pratiques pour éviter les erreurs courantes.
- Répondre aux questions concrètes des enseignants.

Introduction

Accueil et présentation :

-  Présentation des intervenants
  - **Pierre Pecorella**, chargé de mission à la *Drane* p.34 - Numérique responsable et pilotage de l'espace pédagogique
  - **Jean-François Corbineau,** chargé de mission à la *Drane* p.34 - Accessibilité numérique et formation

CRCN Édu

Cadre de référence des compétences numériques pour l'éducation[1]

Domaine	Intitulé	Sous-domaine
1-ENVIRONNEMENT PROFESSIONNEL	Respecter la législation (en particulier le RGPD), les principes éthiques et de sécurité inhérents à l'utilisation des technologies numériques	1.4. Agir en faveur d'un numérique sûr et responsable

Domaine du CRCN édu concernant la cybersécurité

I Le point sur vos connaissances

1. Testez vos connaissances sur la cybersécurité

Exercice 1 : Hameçonnage

[solution n°1 p. 30]

Qu'est-ce que l'hameçonnage ?

- Une méthode pour sécuriser les mots de passe des élèves.
- Une technique utilisée par des cybercriminels pour tromper les utilisateurs afin qu'ils divulguent des informations personnelles.
- Un logiciel éducatif pour enseigner la cybersécurité.

1. CRCN Édu - https://eduscol.education.fr/document/47366/download

Un type de virus informatique qui infecte les ordinateurs des écoles.

Exercice 2 : Création de mot de passe

[solution n°2 p. 30]

Quelle est la meilleure pratique pour créer un mot de passe sécurisé pour un compte d'email scolaire ?

Utiliser le nom de l'école suivi de l'année en cours.

Créer un mot de passe complexe avec des lettres, des chiffres et des symboles, et le changer au moindre soupçon

Utiliser le même mot de passe pour tous les comptes.

Écrire le mot de passe sur un post-it et le coller sur l'ordinateur.

Exercice 3 : Double authentification

[solution n°3 p. 31]

Que signifie l'authentification à deux facteurs (2FA) dans le contexte des comptes scolaires

Un processus qui nécessite deux mots de passe différents pour se connecter.

Une méthode qui demande une vérification supplémentaire, comme un code envoyé par SMS, en plus du mot de passe.

Un logiciel qui authentifie automatiquement tous les utilisateurs sans mot de passe.

Un système qui permet à deux personnes de se connecter simultanément à un même compte.

Exercice 4 : Hacker

[solution n°4 p. 32]

Quelle technique d'attaque consiste à tester toutes les combinaisons possibles de mots de passe ?

Déni de service

force brute (b*rute force*)

L'attaque de l'homme du milieu (HDM) (*Man in the middle*)

Exercice 5

[solution n°5 p. 32]

Qu'est-ce qu'un logiciel malveillant (malware) dans le contexte scolaire ?

Un programme informatique utilisé pour améliorer la sécurité des ordinateurs scolaires.

Un logiciel éducatif pour enseigner la programmation aux élèves.

Un programme informatique nuisible visant à endommager ou voler des données

Un type de matériel informatique

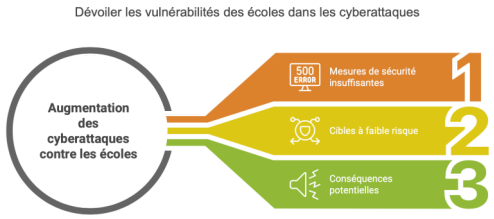
II Contexte

1. Pourquoi ce sujet est important ?

Statistiques

Établissements scolaires ciblés : *+75 % d'attaques en 2023* *Source de statistiques* p.34

Selon les dernières études, les écoles sont devenues une cible privilégiée, avec une augmentation des attaques de **75 % sur un an**. La raison ? Une sécurité souvent dépassée (comme ce vieux serveur oublié au fond du placard à fournitures).



Les vulnérabilités des écoles dans les cyberattaques

Rançongiciel (Ransomware) : la star des cyberattaques

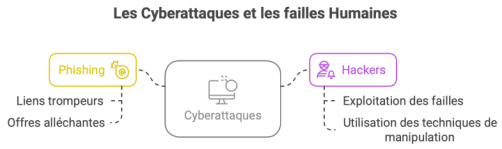
Depuis 2022, **4 établissements** d'enseignement secondaires de l'académie ont subi une cyberattaque par rançongiciel.

Le concept est simple : les hackers encryptent vos données et demandent une rançon (souvent en bitcoins) pour la restitution.

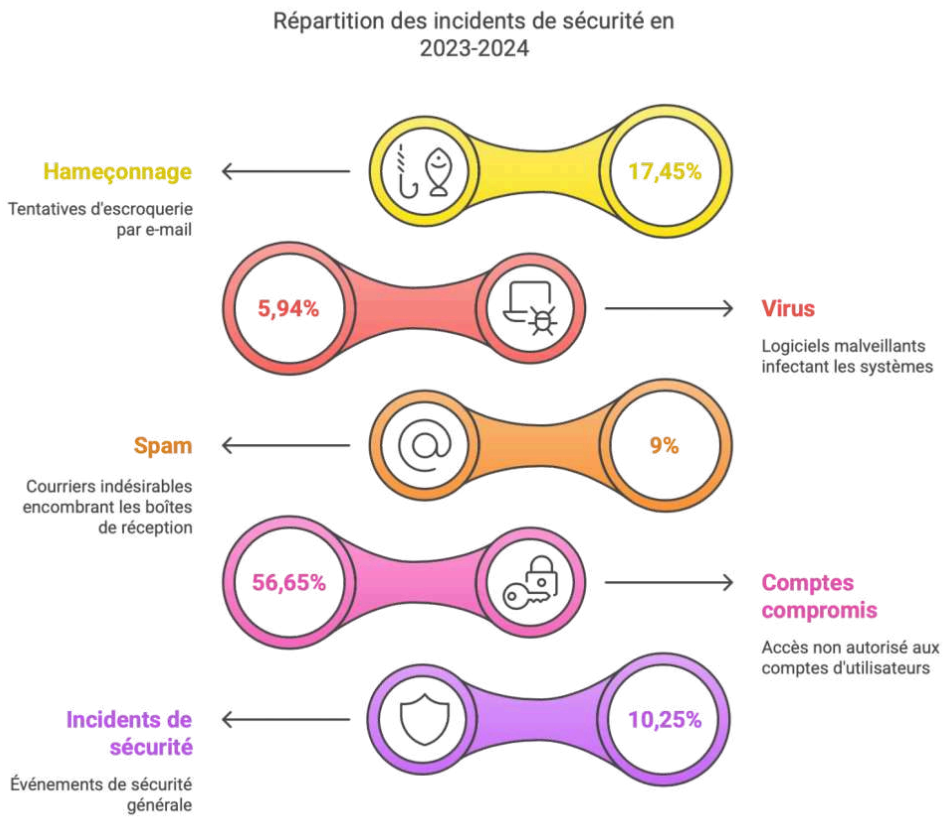
Concept de rançongiciel (ransomware)

Les hackers adorent les failles humaines : **la majeure partie des cyberattaques débutent par un simple mail de *phishing***.

Une invitation à cliquer sur un lien pour « votre quota est atteint, cliquez ici ! » ? Et hop, le piège est tendu.



Les cyberattaques et les failles humaines



Graphique 1 Répartition des incidents de cyberattaque en 2023-2024 - Académie de Nantes

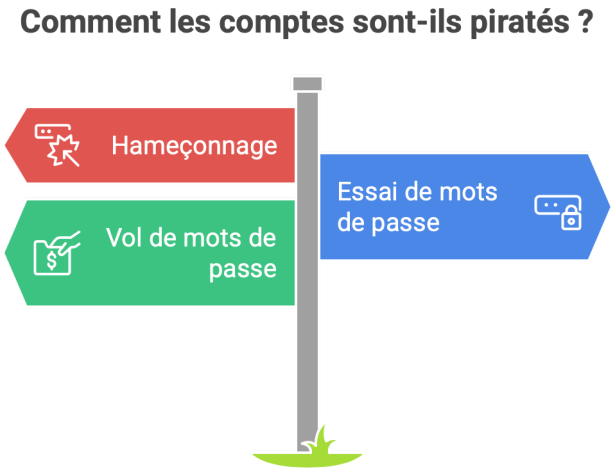


Image 1 Comment les compte sont piratés ?

Conséquences

Les cyberattaques ont des impacts potentiels, tels que :

- la perte de données,
- la perturbation des cours,
- les atteintes à la réputation de l'établissement.

Fondamental

La cybersécurité est essentielle pour garantir un environnement d'apprentissage sûr et protéger les informations sensibles.

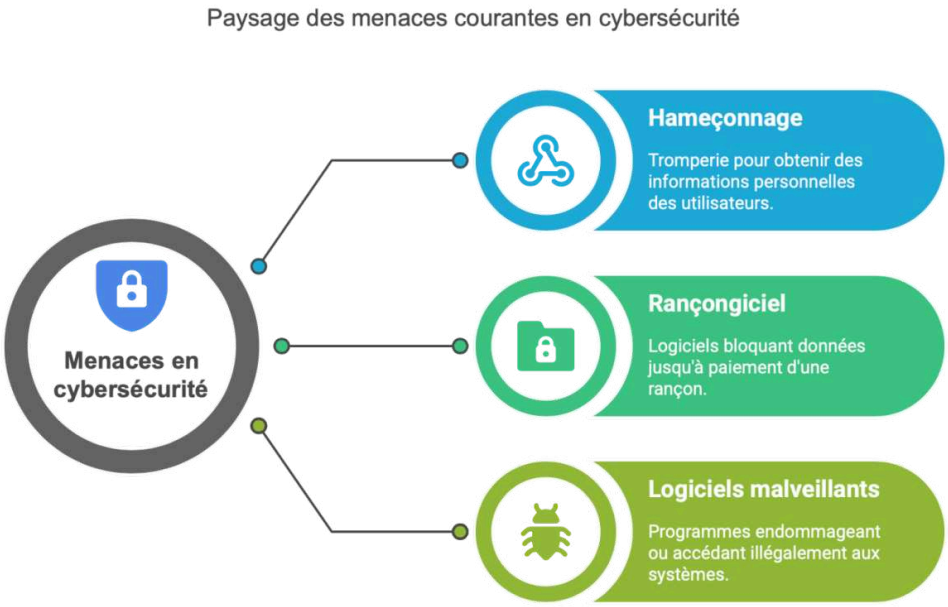
III Comprendre la Cybersécurité

La cybersécurité

Az Définition

la cybersécurité englobe les mesures prises pour protéger les systèmes informatiques, les réseaux et les données contre les cybermenaces

Les menaces courantes



Graphique 2 Les menaces courantes en cybersécurité

- **Hameçonnage** (*phishing)* : Techniques utilisées pour tromper les utilisateurs afin d'obtenir des informations personnelles.
- **Rançongiciel** (*Ransomware*) : Logiciels malveillants qui bloquent l'accès aux données jusqu'à paiement d'une rançon.
- **Logiciels malveillants** (*Malware*) : Logiciels conçus pour endommager ou accéder à des systèmes.

Les impacts des cyberattaques

Attention

- **Perturbation des cours :** Les systèmes en ligne deviennent inutilisables, empêchant les élèves d'accéder à l'*ENT* [p.34] ou de soumettre leurs devoirs sur ÉLÉA. Alerte à la bombe. Menaces d'attentat.

- **Perte de données :** Les informations sensibles concernant les élèves et enseignants peuvent être volées ou détruites, perturbant la gestion administrative
- **Atteinte à la réputation :** Une cyberattaque peut ternir l'image d'un établissement

Fondamental

Comprendre les menaces et leurs impacts est essentiel pour développer une culture de cybersécurité au sein de l'établissement.

IV Cas pratiques et exemples concrets

Objectifs

- Illustrer les concepts théoriques avec des exemples concrets.
- Engager les participants avec des situations qu'ils peuvent rencontrer au quotidien.

1. Exemple 1 : Hameçonnage ciblé

Scénario

« Un enseignant reçoit un email prétendument envoyé par l'administration, demandant de mettre à jour ses informations de connexion via un lien »

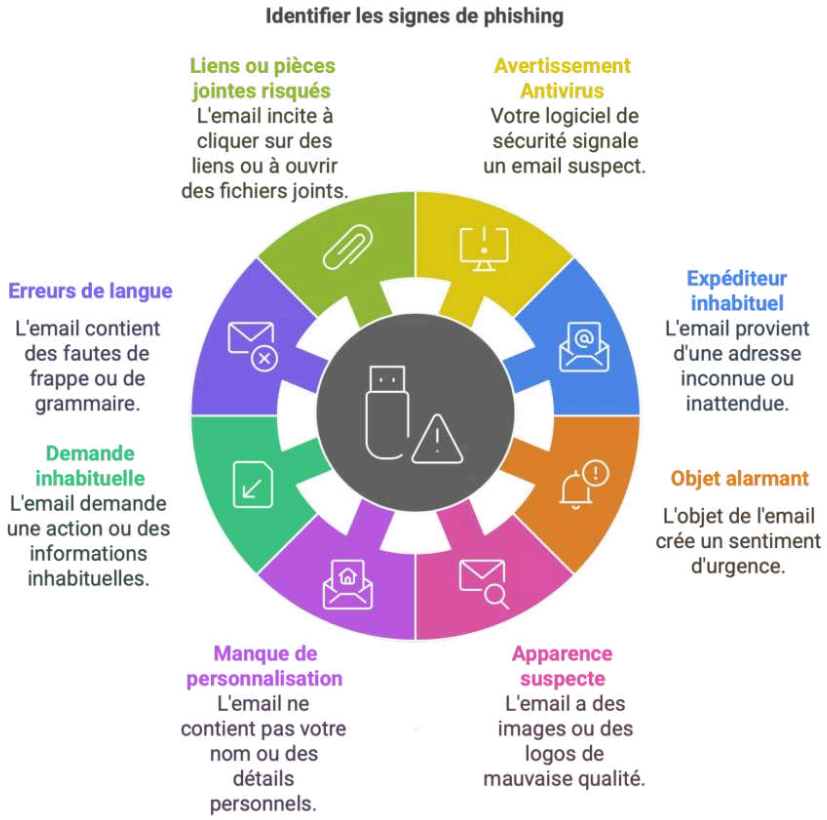
Questions de réflexion

- **Identification :** Comment l'enseignant peut-il identifier que cet email est suspect ?
- **Sensibilisation :** Quelles mesures devraient être mises en place pour sensibiliser le personnel aux tentatives de phishing ?

Solution

Méthode

Les enseignants doivent être formés pour reconnaître les tentatives de phishing et savoir comment réagir.



Graphique 3 Identifier les signes d'un hameçonnage

Image 2 Comment se protéger contre le hameçonnage ?

Ressources en ligne

- Comment reconnaître un mail de phishing ou d'hameçonnage ?[2] sur le site cybermalveillance.gouv.fr
- Que faire en cas de *phishing* ou hameçonnage ?[3] sur le site cybermalveillance.gouv.fr
- Victime d'une cybermailveillance 17Cyber : faire un diagnostic[4] sur le site cybermalveillance.gouv.fr

Image 3 Logo de la plateforme 17 Cyber

V Bonnes Pratiques en cybersécurité pour les enseignants

1. Les bonnes pratiques dans le cadre professionnel

Méthode

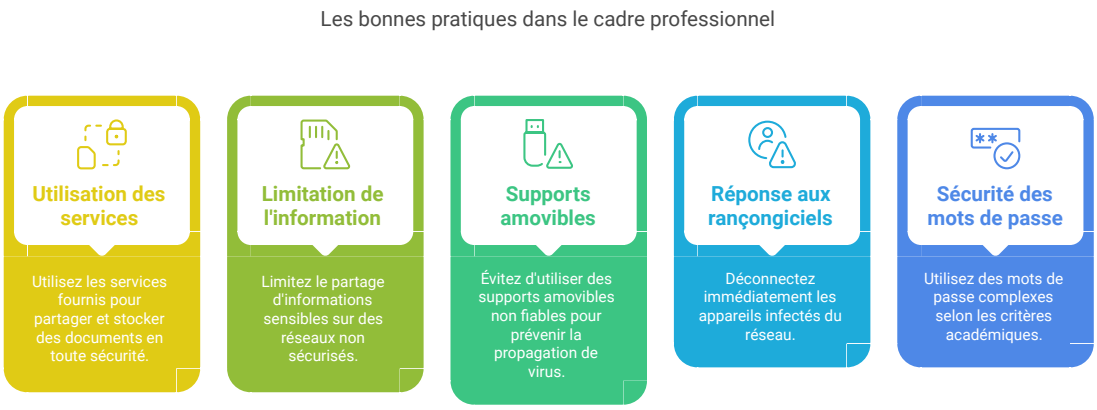


Image 4 Les bonnes pratiques dans le cadre professionnel

Protégez vous contre les pertes ou les altérations de vos données.

2. Comment reconnaître un mail de phishing ou d'hameçonnage ? - https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconnaitre-un-mail-de-phishing-ou-dhameconnage
3. Que faire en cas de phishing ou hameçonnage ? - https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing
4. Diagnostic 17Cyber - https://www.cybermalveillance.gouv.fr/diagnostic

- Sauvegarder régulièrement vos données pro sur plusieurs supports (disque externe, stockage en ligne comme Nuages)

Protégez la confidentialité de vos données

- Utilisez les services fournis par l'académie (portail.apps.education.fr[5] ou l'*ENT* p.34 e-lyco ou e-primo) pour partager et stocker vos documents professionnels.
- Limiter les échanges d'informations confidentielles ou sensibles lorsque vous êtes connectés à des réseaux non maîtrisés (lieu publics, à l'étranger...) en raison du risque important de capture des données par un tiers.

Protégez vos données et celles des autres utilisateurs

- Limitez l'utilisation de supports amovibles non maîtrisés (disque externe, clé *USB* p.34) qui peuvent contenir et propager un virus.
- En cas d'infection par un rançongiciel, déconnectez immédiatement le poste de travail du réseau (wifi ou filaire) puis ouvrez un ticket d'incident de sécurité sur *AMIGO* p.34.
- Utilisez des mots de passe complexes en utilisant les critères académiques[6]

2. Se protéger dans les établissements scolaires

Méthode

Image 5 Les actions pour se protéger dans les établissements scolaires

- **Sauvegarde automatique** et quotidienne des documents enregistrés dans votre dossier personnel, ou dans les dossiers de classe sur le serveur pédagogique
- **Téléchargements de pièces-jointes** (PJ)
  - via des messageries électroniques externes (mail)
  - via des messageries électroniques internes (*ENT* p.34)

5. accueil portail apps.education - https://portail.apps.education.fr/signin
6. Choisir un mot de passe approprié - https://www.intra.ac-nantes.fr/choisir-un-mot-de-passe-appropriе-1588243.kjsp?RH=1479735136536

 **Action** : Scannez vos pièces-jointes (PJ) avec l'antivirus de l'ordinateur

- **Utilisation des disques durs ou clés *USB*** p.34

 **Action** : privilégier les clouds (Nuage entre enseignants, *ENT* p.34 avec les élèves)

- Tout le reste du système d'information (réseau pédagogique) ainsi que les accès à Internet sont surveillés par les outils mis en place (antivirus, pare-feu, proxy, etc.) par la collectivité et qui prend en charge cette sécurité numérique.De même pour l'*ENT,* p.34 le service web est sécurisé par son éditeur.

3. Se protéger chez soi

Méthode

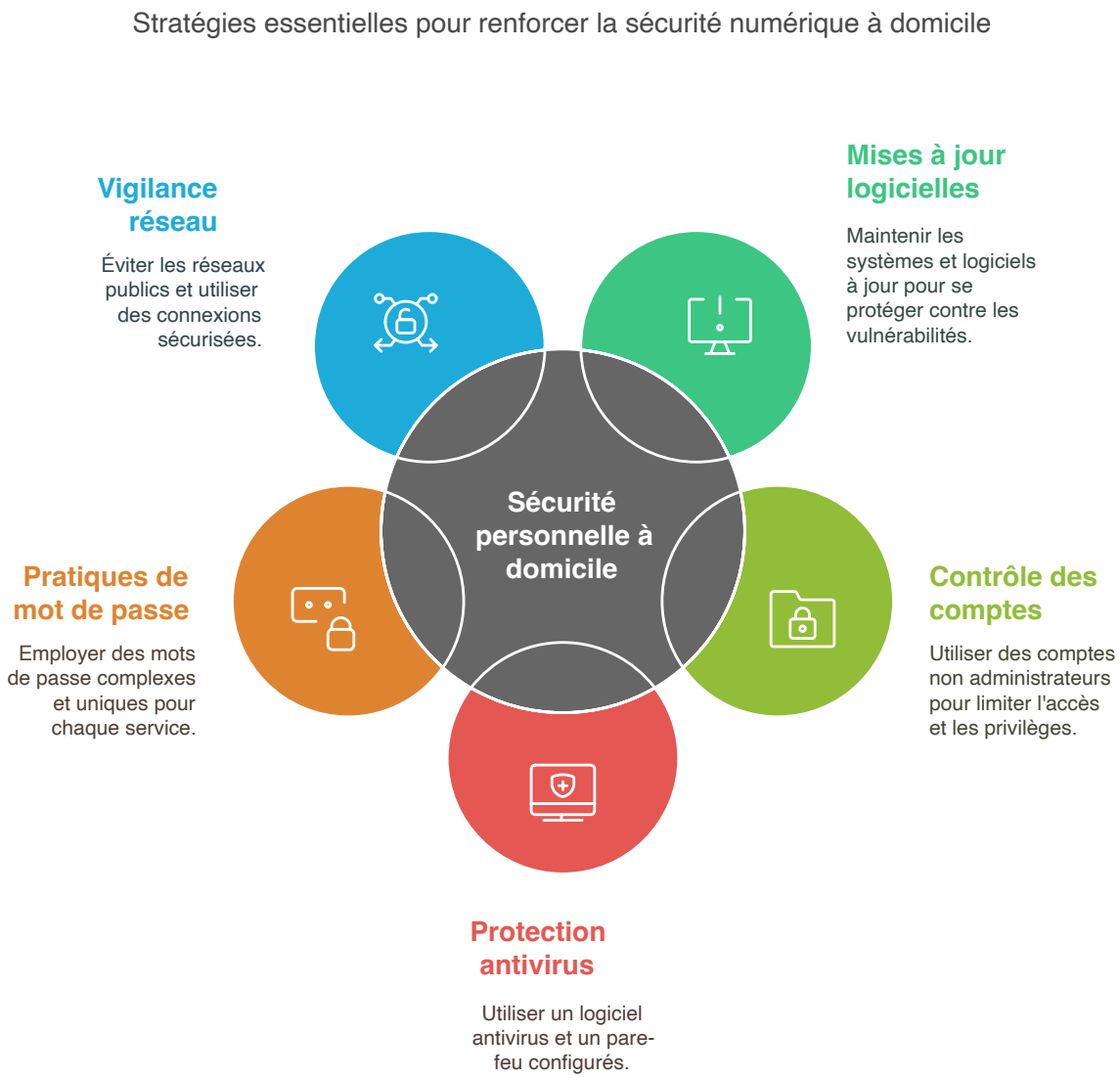


Image 6 Comment se protéger à la maison ?

- **Mise à jour logicielles** : maintenir le système d'exploitation (Windows, MacOS, GNU-Linux, Android, iOS) et les logiciels à jour sur tous les équipements (ordinateur, smartphone, tablettes)
- **Contrôle des comptes** :le compte d'usage de l'ordinateur n'est pas un compte avec des droits d'administrateur
- **Protection** : Utiliser un antivirus à jour, un parefeu configuré
- Se méfier des logiciels dont l'origine n'est pas garantie, lorsqu'il n'est pas diffusé par son éditeur officiel (cf. *les stealers* p.33)
- **Vigilance réseau** : Utiliser des réseaux sécurisés et éviter les réseaux wifi public
- **Pratiques de mot de passe** : Utiliser des mots de passe complexes et differents pour chaque service
- Faire des sauvegardes régulières sur au moins un support déconnecté d'internet
- Être vigilant aux liens et pièces jointes dans les messages électroniques
- Ne pas travailler sur des supports *USB* p.34 (uniquement usage de « transport » et de sauvegarde)

Fondamental

Séparer les usages personnels et professionnels

(cf. memo_usages_pro_perso.pdf)

Cyber conseils aux usagers

Ressources en ligne

Le site du gouvernement propose des conseils aux usagers[7]

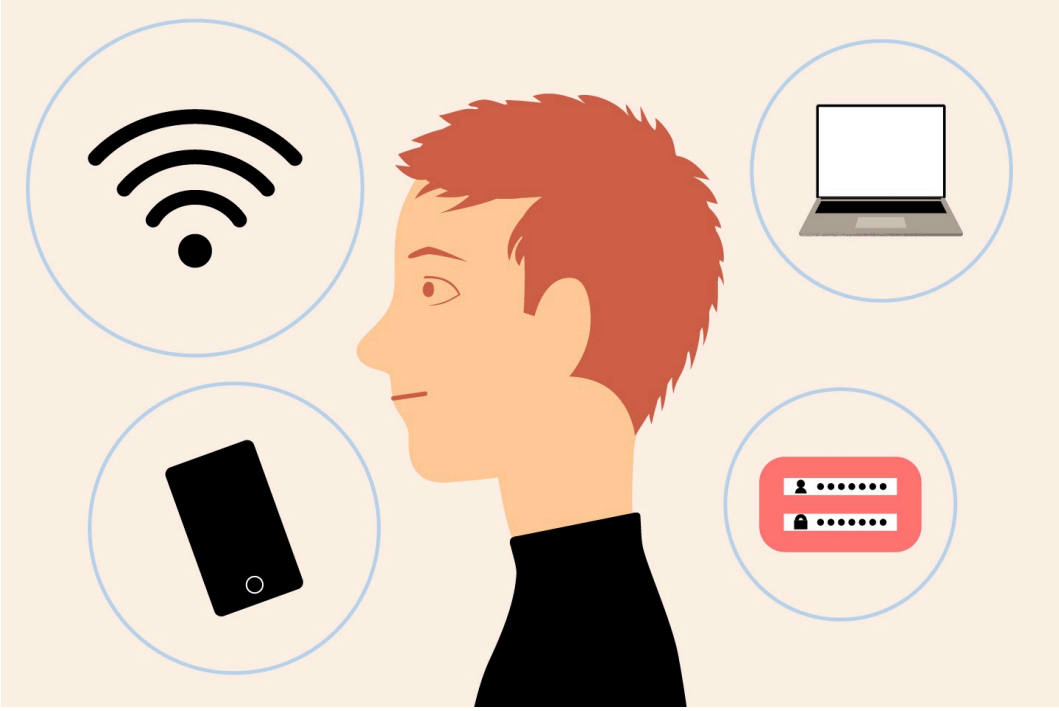


Image 7 Conseils aux usagers

VI Cas pratiques et exemples concrets #2

Objectifs

- Illustrer les concepts théoriques avec des exemples concrets.
- Engager les participants avec des situations qu'ils peuvent rencontrer au quotidien.

1. Exemple 2 : Utilisation d'un Réseau Wi-Fi Public

Scénario

« Lors d'une sortie scolaire, des enseignants et des élèves se connectent à un réseau Wi-Fi public dans un café pour accéder à des ressources pédagogiques. Certains élèves commencent à partager des informations personnelles sur les réseaux sociaux. »

Questions de réflexion

- **Risques :** Quels sont les risques associés à l'utilisation d'un réseau Wi-Fi public pour accéder à des informations sensibles ?
- **Recommandations :** Quelles recommandations pourriez-vous donner aux enseignants et aux élèves pour utiliser Internet en toute sécurité lors de sorties scolaires ?

7. https://www.info.gouv.fr/risques/cyber-conseils-aux-usagers

Solution

Méthode

L'utilisation de réseaux Wi-Fi publics présente des risques importants, et il est crucial d'éduquer les élèves sur les meilleures pratiques pour naviguer en toute sécurité.

Graphique 4 Comment sécuriser les connexions wifi publics

Graphique 5 Les types d'attaques courantes sur les réseaux Wi-Fi publics

⚠ Attention

Ces différentes attaques peuvent avoir des conséquences graves pour les victimes, allant de la perte de données personnelles à des préjudices financiers importants, en passant par l'atteinte à la réputation pour les professionnels dont les informations sensibles seraient compromises.

VII Une plateforme ludique ouverte à tous

Une compétence numérique dédiée

Présentation de pix

Pour sensibiliser aux enjeux de la cybersécurité et pour permettre à chacun de développer des compétences nécessaires à sa sécurité numérique personnelle et professionnelle, Pix permet à tout citoyen, qu'il soit débutant ou déjà à l'aise avec le numérique, de tester, développer et certifier ses compétences de façon ludique.

Des défis ludiques pour accompagner le développement des compétences nécessaires à la sécurité numérique de tout un chacun, accessibles à tous sur pix.fr[8]

8. La plateforme pix - https://pix.fr/

Les domaines du référentiel des compétences numériques

Focus

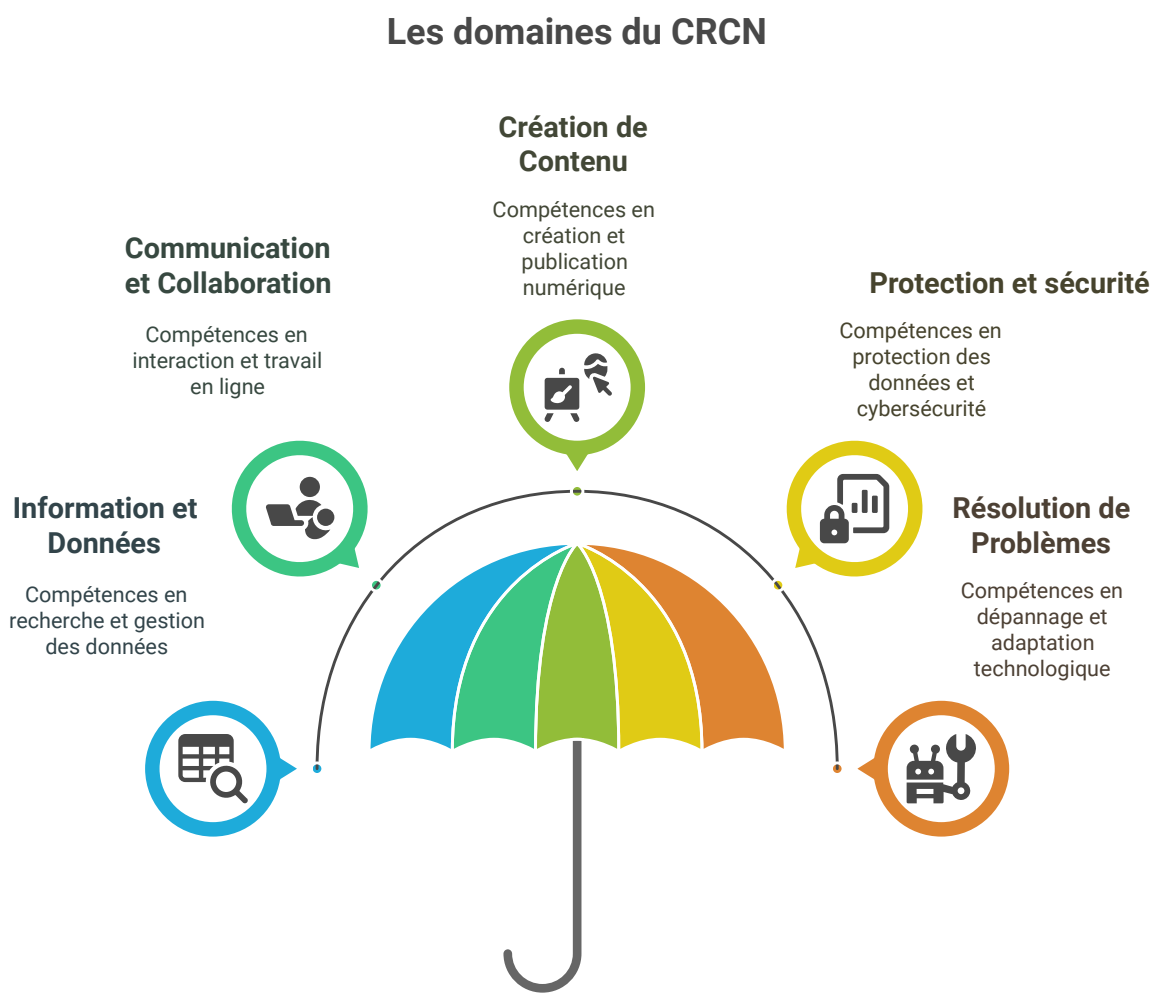


Image 8 Les domaines du référentiel des compétences numériques (CRCN)

Le domaine n°4 : Protection et Sécurité

La sécurité numérique est essentielle pour protéger les informations personnelles et professionnelles.

Les compétences comprennent :

- **Protection des données** : Savoir comment sécuriser ses informations personnelles et professionnelles.
- **Reconnaissance des menaces** : Identifier les risques liés à la cybersécurité, comme le phishing et les malwares.
- **Comportement responsable en ligne** : Adopter des pratiques sûres lors de l'utilisation d'Internet.

1. Des épreuves (niveau 1 à 7)

- Les compétences testées sur la plateforme pix

L'accueil de la plateforme PIX

2. Un référentiel de compétences

Le référentiel de compétences sur la sécurité de l'environnement et des pratiques numériques réalisé par Pix en partenariat avec l'*ANSSI* p.34 et Cybermalveillance, s'adresse aux professionnels de l'enseignement et de la formation pour les appuyer dans l'accompagnement de leurs apprenants

- Consulter la page « Éducation à la cybersécurité[9] » dans la rubrique de la *Drane* p.34
- *(cf. Télécharger le référentiel des compétences sur la sécurité Pix et de l'ANSSI.)* (cf. p.30)

VIII Cas pratiques et exemples concrets #3

Objectifs

- Illustrer les concepts théoriques avec des exemples concrets.
- Engager les participants avec des situations qu'ils peuvent rencontrer au quotidien.

1. Exemple 3 : Gestion des données des élèves

Scénario

« Un enseignant utilise un logiciel de gestion des notes qui stocke des informations personnelles sur les élèves. Il partage son mot de passe avec un collègue pour faciliter l'accès, mais ce dernier ne respecte pas les bonnes pratiques de sécurité. »

9. Éducation à la cybersécurité - https://www.pedagogie.ac-nantes.fr/numerique-et-enseignement/numerique-responsable/securite-numerique/securite-numerique-1599443.kjsp

Questions de réflexion

- **Risques :** Quels sont les risques liés au partage de mots de passe et à la gestion des données personnelles des élèves ?
- **Politiques :** Quelles politiques devraient être mises en place pour protéger les données des élèves dans l'école ?

L'essentiel

Le partage de mots de passe et la gestion des données personnelles des élèves dans un contexte éducatif présentent plusieurs risques importantsà la fois en termes de **sécurité informatique** et de respect des réglementations sur **la protection des données**.

Risques liés au partage de mots de passe

Attention

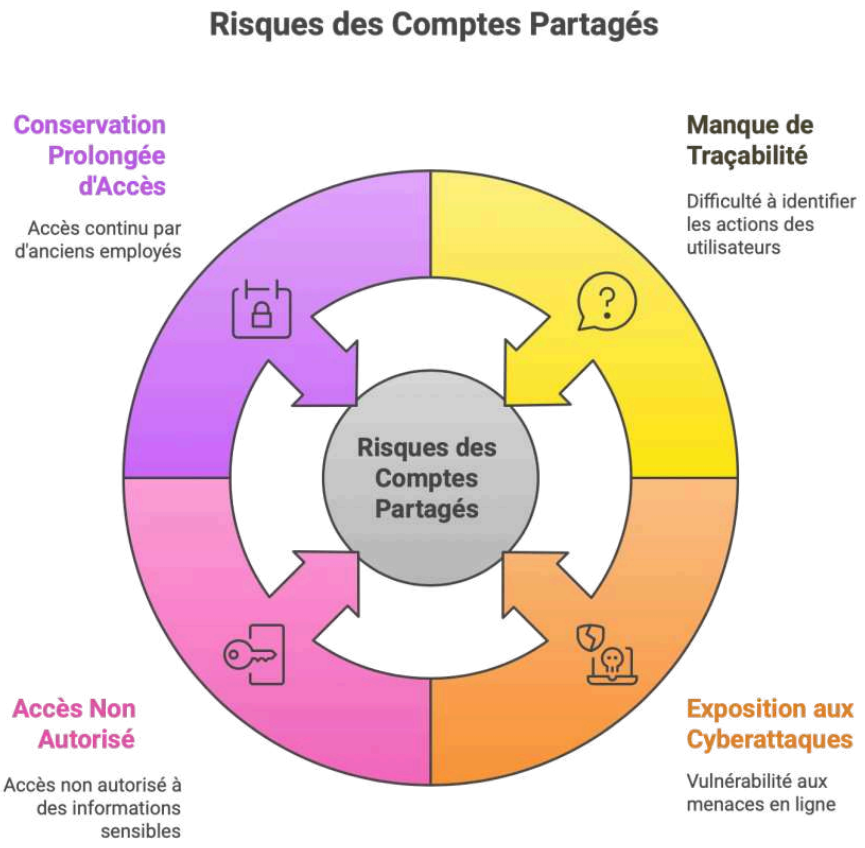


Image 9 Risque liés au partage de mot de passe

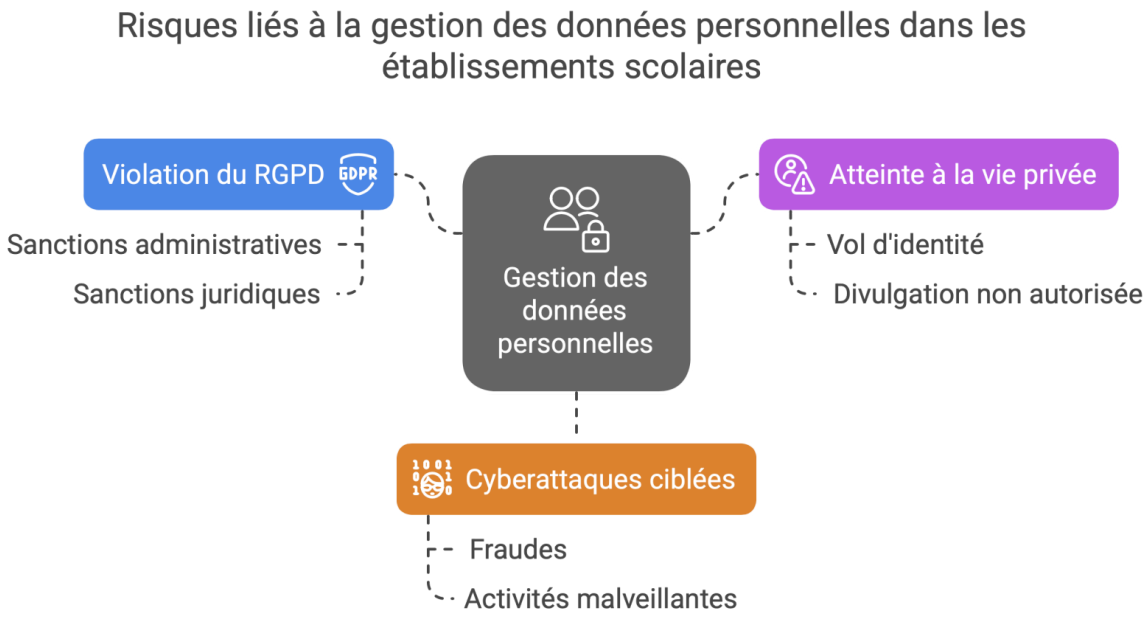
- **Manque de traçabilité** : Lorsque plusieurs personnes utilisent le même compte, il devient impossible d'identifier clairement qui a effectué une action spécifique. Cela complique la gestion des responsabilités en cas d'incident ou de violation.
- **Exposition aux cyberattaques** :

1. Les mots de passe partagés peuvent être interceptés via des plateformes non sécurisées (emails, messageries).
2. Une mauvaise gestion (comme l'utilisation d'un mot de passe faible ou sa réutilisation) expose les comptes à des attaques par force brute ou phishing.

- **Accès non autorisé** : Une personne non habilitée pourrait accéder à des informations sensibles, ce qui constitue une violation des droits d'accès et un risque pour la confidentialité.
- **Conservation prolongée d'accès** : D'anciens collègues ou employés pourraient conserver l'accès aux comptes partagés, augmentant le risque de compromission

Risques liés à la gestion des données personnelles

⚠ Attention



Graphique 6 Les risques liés à la gestion des données personnelles

Violation du *RGPD* [p.34] :

- Les informations personnelles des élèves (noms, notes, etc.) sont protégées par le Règlement Général sur la Protection des Données (RGPD). Leur traitement doit être documenté dans un registre et respecter des principes stricts de finalité et de proportionnalité.
- Toute fuite ou utilisation abusive peut entraîner des sanctions administratives et juridiques pour l'établissement scolaire.

Atteinte à la vie privée :

- Une mauvaise gestion ou un accès non sécurisé peut exposer les élèves à des risques comme le vol d'identité ou la divulgation non autorisée d'informations sensibles (statut académique, données financières).

Cyberattaques ciblées :

- Les établissements scolaires sont souvent ciblés par des cybercriminels cherchant à exploiter les données personnelles pour des fraudes ou d'autres activités malveillantes.

Bonnes pratiques recommandées Méthode

- **Utilisation de comptes individuels** : Chaque utilisateur doit avoir son propre identifiant et mot de passe pour garantir une traçabilité complète
- **Gestionnaire de mots de passe** : Utiliser un outil sécurisé pour partager les accès lorsque cela est nécessaire, tout en minimisant les risques liés au partage direct

L'essentiel

En résumé, le partage non sécurisé de mots de passe et une gestion inappropriée des données personnelles exposent les établissements scolaires à des risques juridiques, techniques et éthiques majeurs. Adopter des solutions sécurisées et respecter les réglementations est essentiel pour protéger ces informations sensibles.

Ressources en ligne

- Recueil et mises à disposition des données personnelles[10] sur le site de canopé
- La protection des données personnelles à l'École[11] sur le site malettedesparents.education.gouv.fr
- La protection des données sur etna[12]
- Le responsable de traitement et ses obligations sur etna[13]
- Règlement général sur la protection des données (RGPD) sur etna[14]

IX Comment répondre aux menaces ?

10. Recueil et mises à disposition des données personnelles - https://www.reseau-canope.fr/les-donnees-a-caractere-personnel/recueil-et-mises-a-disposition-des-donnees-personnelles.html
11. La protection des données personnelles à l'École - https://mallettedesparents.education.gouv.fr/professionnels/ID208/la-protection-des-donnees-personnelles-a-l-ecole
12. Protection des données - https://www.intra.ac-nantes.fr/protection-des-donnees-1102957.kjsp?RH=intra&RF=1519387565419
13. Le responsable de traitement - https://www.intra.ac-nantes.fr/responsable-de-traitement-1345157.kjsp?RH=1519387565419&RF=1519387565419
14. Le RGPD - https://www.intra.ac-nantes.fr/le-rgpd-1118495.kjsp?RH=1519387565419

Virus informatique : que faire ?

Méthode

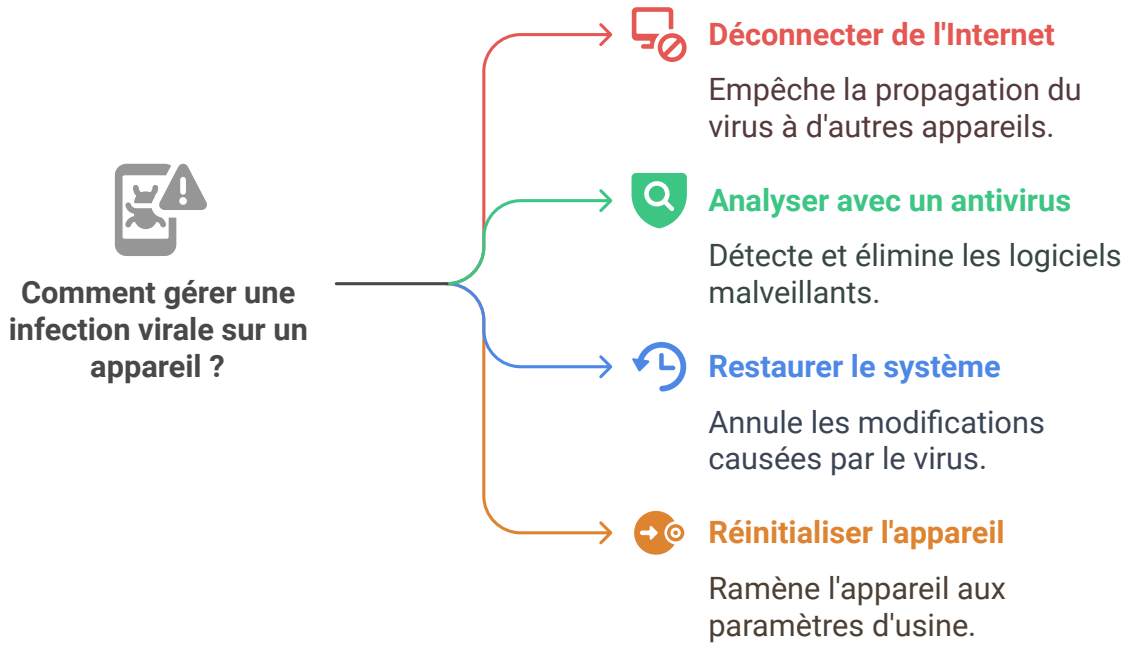


Image 10 Comment supprimer un virus de mon ordinateur ?

Pour plus d'information, consulter l'article « virus informatique, que faire ?[15]» sur le site cybermalveillance.gouv.fr

15. Virus informatique, que faire ? - https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/virus-informatiques

Piratage de compte que faire ? Méthode

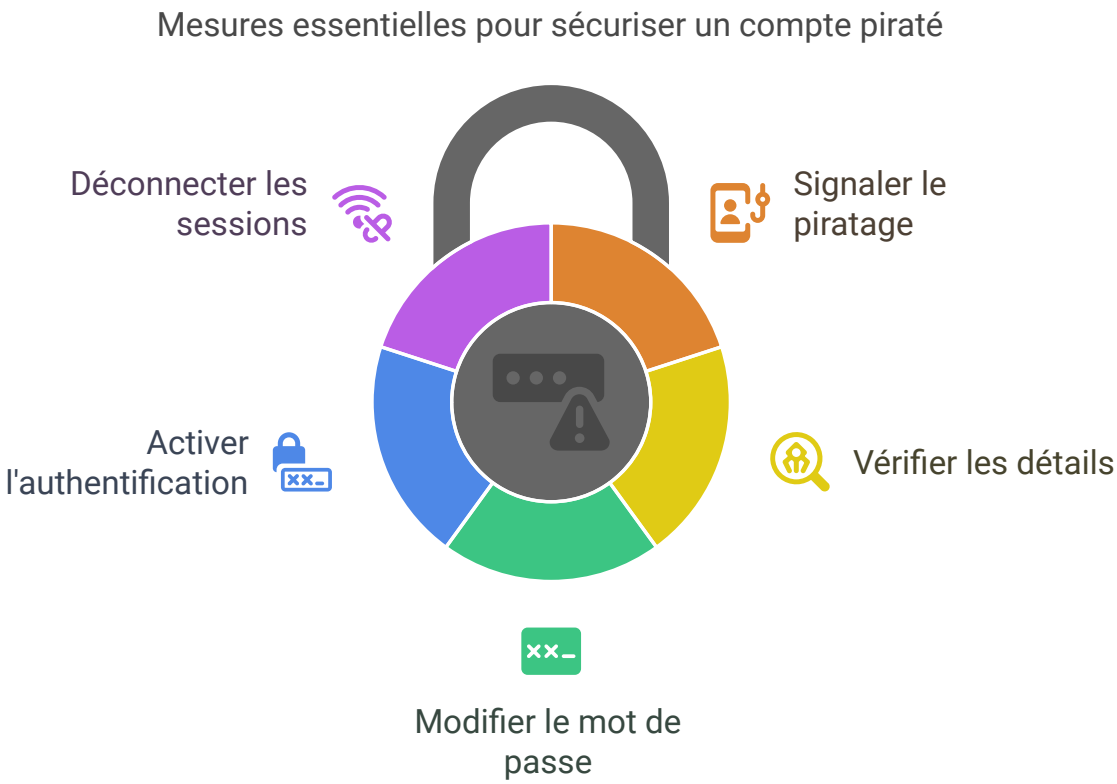


Image 11 Mesures indispensables pour sécuriser un compte qui a été piraté

Pour plus d'information, consulter l'article « Piratage de compte, que faire[16] ?» sur le site cybermalveillance.gouv.fr

16. Piratage de compte, que faire ? - https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/piratage-de-compte

Que faire en cas d' hameçonnage (*phishing*) ?

Méthode

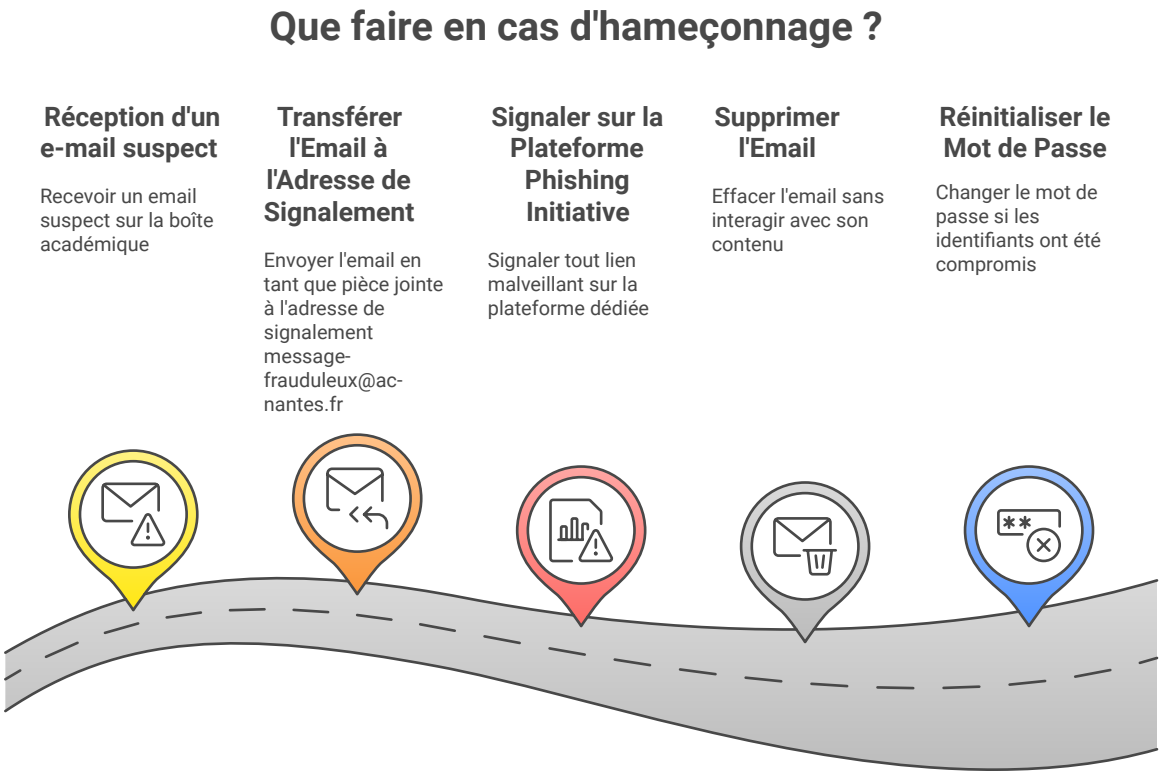


Image 12 Que faire en cas d'hameçonnage ?

X Conclusions et ressources

Résumé rapide des points importants pour éviter de se faire pirater

L'essentiel

Image 13 Les règle simples pour éviter de se faire pirater

- Ne téléchargez pas de programmes ou modules (plug-ins) depuis des sites non-officiels.
- Utilisez **un anti-virus** à jour et ne le désactivez jamais.
- Méfiez-vous des **messages inattendus**.
- N'utilisez pas le même mot de passe partout.
- Imaginez **des mots de passe robustes** et activez **les authentifications renforcées** quand c'est possible.
- Appliquez **les mises à jour de sécurité** sur tous vos appareils (PC, tablettes, téléphones, etc.) dès qu'elles vous sont proposées.
- N'enregistrez pas vos mots de passe dans un ordinateur partagé et pensez à vous déconnecter en partant.

Procédure à respecter en cas de cybertattaque

Méthode

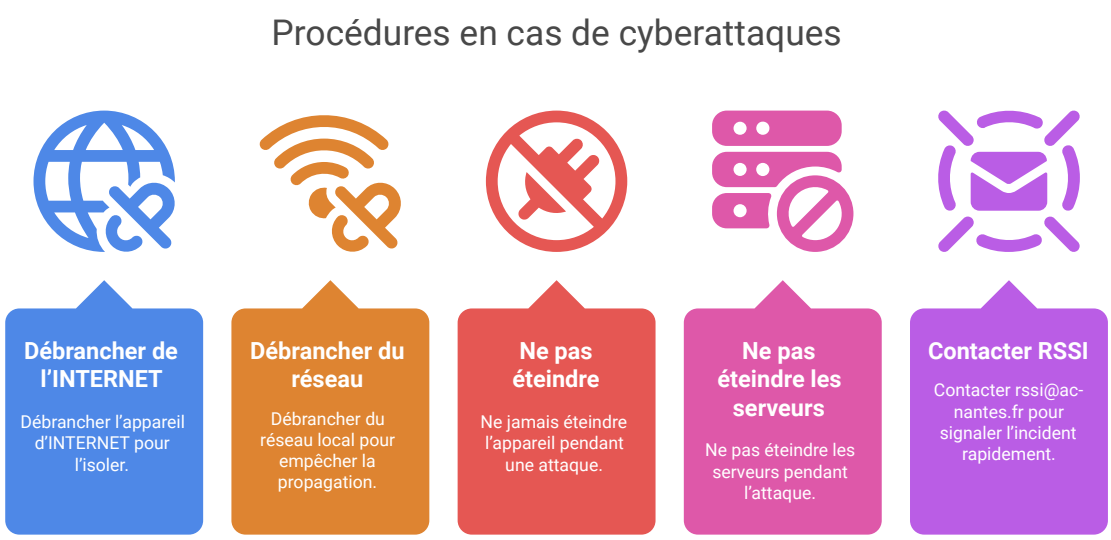


Image 14 Les procédures en cas de cyberattaque

Partage de ressources pédagogiques

L'essentiel

- Page éducation à la cybersécurité[17] de la Drane Nantes
- La page sécurité numérique [18]sur etna
- Des ressources pour sensibiliser les élèves[19] sur le site cybermalveillance.gouv.fr : page dédiée a actualiser les connaissances et monter en compétences sur la cybersécurité

17. https://www.pedagogie.ac-nantes.fr/numerique-et-enseignement/numerique-responsable/securite-numerique/securite-numerique-1599443.kjsp
18. Sécurité numérique - https://www.intra.ac-nantes.fr/securite-numerique-999035.kjsp?RH=1699603013038&RF=1476883514572
19. Médiation et inclusion numérique - https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/outils-acteurs-mediation

Le jeu de carte de la fresque des cybercitoyennes et cybercitoyens

Focus

La fresque des cybercitoyennes et cybercitoyens réalisé grâce à l'expertise en cybersécurité d'Advens et le partenariat avec l'académie de Nantes, a pour but de sensibiliser les adolescents de 11 à 14 ans à la sécurité numérique.

Consulter l'article sur le jeu de carte de la fresque des cybercitoyennes et cybercitoyens[20] sur le site pédagogique

Logo de la fresque des cybercitoyens

Image 15 Les cartes du jeu de la Fresque des cybercitoyens

Se former

Ressources en ligne

- Parcours M@gistère « agir pour contribuer à ma sécurité numérique et à celle de mon organisation[21] » : parcours libre en autoformation de moins de 2h en 3 modules.
- SensCyber[22] par cybermlaveillance.gouv.fr : découvrir les mécanismes des principales menaces sur Internet et apprendre à mieux se protéger.

20. https://www.pedagogie.ac-nantes.fr/numerique-et-enseignement/numerique-responsable/la-fresque-des-cybercitoyennes-et-des-cybercitoyens-1611437.kjsp?RH=1592825884342
21. https://magistere.education.fr/local/magistere_offers/index.php?v=formation#offer=1266
22. https://www.cybermalveillance.gouv.fr/sens-cyber/apprendre

- le cyber guide famille[23] : pour sensibiliser aux risques numériques et aux bonnes pratiques, et accompagner les parents et les enfants dans leurs gestes quotidiens
- Le MOOC de l'ANSSI SecNum[24] : le cours en ligne de Secnumacadémie de l'ANSII sur la sécurité numérique dans un environnement professionnel
- Défis et enjeux de la cybersécurité[25] sur FUN : Ce *MOOC* p.34 vous propose de découvrir les aspects à la fois sociétaux mais aussi techniques de la cybersécurité, à travers 7 thématiques différentes.
- Des ressources sur la sécurité numérique[26] sur le site de la Drane de Versailles
- Des podcasts de culture numérique [27]sur le site de la Drane de Versailles

En savoir plus

- ANSSI : Guide d'hygiène informatique[28] (2017)
- ANSSI : Guide attaques par rançongiciel, tous concernés[29] (2020)
- Cybermalveillance : Dispositif national d'assistance aux victimes d'actes de cybermalveillance, de prévention et sensibilisation aux risques numériques et d'observation de la menace[30]
- CNIL : La sécurité des données personnelles (PDF - 310 ko) [31](2018)
- Canopé : Les données à caractère personnel[32] (2018)
- Drane Nantes / *PDSI* p.34 / *DPD* p.34 : Le livret des notions clés du RGPD [33] (2023)
- Campus Cyber : Wiki du Studio des Communs [34](2022)
- La lettre EduNum N°19 sur la cybersécurité (PDF - 4,1 Mo)[35] (mars 2023)

Les références

Texte légal

- République française – Légifrance. LOI n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public[36] (2022)

Ressources annexes

23. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cyber-guide-famille-cybersecurite
24. https://secnumacademie.gouv.fr/
25. https://www.fun-mooc.fr/fr/cours/defis-et-enjeux-de-la-cybersecurite/
26. Sécurité numérique - https://drane-versailles.region-academique-idf.fr/spip.php?mot369&debut_articles=12#pagination_articles
27. Numérique et vous : une série de podcasts de culture numérique - https://drane-versailles.region-academique-idf.fr/spip.php?rubrique37
28. https://cyber.gouv.fr/publications/guide-dhygiene-informatique
29. https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes
30. https://www.cybermalveillance.gouv.fr/
31. https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_guide_securite_personnelle.pdf
32. https://www.reseau-canope.fr/fileadmin/user_upload/Projets/RGPD/RGPD_WEB.pdf
33. https://www.intra.ac-nantes.fr/les-notions-cles-du-rgpd-1544183.kjsp?RH=1592825884342
34. https://wiki.campuscyber.fr/Wiki_du_campus_cyber
35. https://eduscol.education.fr/document/47573/download?attachment
36. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045294275

Le référentiel « sécuriser l'environnement et les pratiques numériques»

Le référentiel des compétences numériques dédié à la cybersécurité a également été co-créé par PIX, l'ANSSI et cybermalveillance.gouv.fr

Solutions des exercices

Solution n°1

[exercice p. 3]

Qu'est-ce que l'hameçonnage ?

Une méthode pour sécuriser les mots de passe des élèves.

✓ Une technique utilisée par des cybercriminels pour tromper les utilisateurs afin qu'ils divulguent des informations personnelles.

Un logiciel éducatif pour enseigner la cybersécurité.

Un type de virus informatique qui infecte les ordinateurs des écoles.

« L'hameçonnage ou phishing en anglais est le principal mode opératoire utilisé par les cybercriminels pour dérober des informations personnelles et/ou bancaires aux internautes. »

Source : Article *Hameçonnage*[37] de Wikipédia en français. (Contenu soumis à la licence CC-BY-SA 4.0[38])

Les autres options sont incorrectes : l'hameçonnage n'est ni une méthode de sécurisation ni un logiciel éducatif ou un type de virus.

Solution n°2

[exercice p. 4]

Quelle est la meilleure pratique pour créer un mot de passe sécurisé pour un compte d'email scolaire ?

Utiliser le nom de l'école suivi de l'année en cours.

✓ Créer un mot de passe complexe avec des lettres, des chiffres et des symboles, et le changer au moindre soupçon

Utiliser le même mot de passe pour tous les comptes.

Écrire le mot de passe sur un post-it et le coller sur l'ordinateur.

37. Article hameçonnage - https://fr.wikipedia.org/wiki/Hame%C3%A7onnage)
38. licence CC BY SA - https://creativecommons.org/licenses/by-sa/4.0/deed.fr)

la sécurité de l'accès à tous ces services professionnels repose aujourd'hui essentiellement sur les mots de passe. Face à leur profusion, la tentation est forte d'en avoir **une gestion trop simple**.

Une telle pratique serait **dangereuse**, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès.

Un mot de passe sécurisé doit être **complexe** et inclure **une combinaison de caractères** (lettres majuscules/minuscules, chiffres, symboles).

Les autres options sont dangereuses : utiliser un mot de passe simpliste (comme le nom de l'école) ou réutiliser le même mot de passe pour tous les comptes augmente les risques d'accès non autorisé. Écrire son mot de passe sur un post-it est également déconseillé car cela compromet sa confidentialité.

Vérifier sa politique de mots de passe [39]sur le site de la CNIL

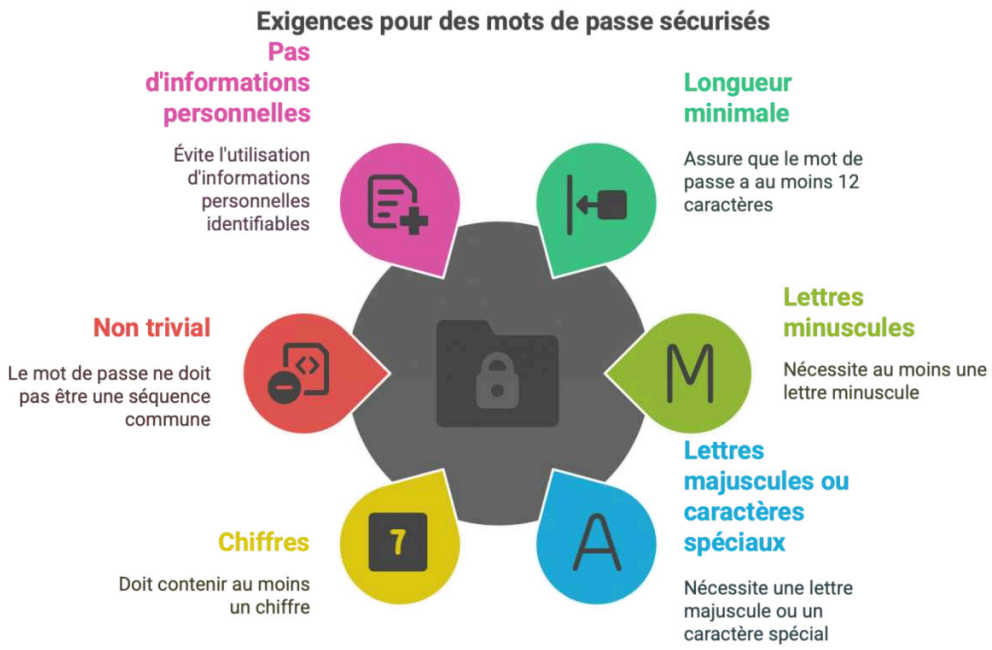


Image 16 Bien choisir son mot de passe

Solution n°3

[exercice p. 4]

Que signifie l'authentification à deux facteurs (2FA) dans le contexte des comptes scolaires

Un processus qui nécessite deux mots de passe différents pour se connecter.

✓ Une méthode qui demande une vérification supplémentaire, comme un code envoyé par SMS, en plus du mot de passe.

Un logiciel qui authentifie automatiquement tous les utilisateurs sans mot de passe.

39. Vérifier sa politique de mots de passe - https://www.cnil.fr/fr/verifier-sa-politique-de-mots-de-passe

Un système qui permet à deux personnes de se connecter simultanément à un même compte.

L'authentification à deux facteurs (2FA) est une mesure de sécurité renforcée qui ajoute une étape supplémentaire à la connexion. En plus du mot de passe, l'utilisateur doit fournir une preuve supplémentaire comme un code envoyé par SMS ou généré par une application dédiée. Cela réduit considérablement les risques d'accès non autorisé.

Les autres options ne décrivent pas correctement le 2FA : il ne s'agit pas d'utiliser deux mots de passe différents ni d'une connexion simultanée par deux personnes ou d'une authentification automatique sans mot de passe.

Solution n°4

[exercice p. 4]

Quelle technique d'attaque consiste à tester toutes les combinaisons possibles de mots de passe ?

Déni de service

✓ force brute (b*rute force*)

L'attaque de l'homme du milieu (HDM) (*Man in the middle*)

Dans le cas d'une attaque par « **brute force** », l'attaquant va tester toutes les combinaisons possibles : AAAA, AAAB, AAAC etc…

Actuellement, avec la puissance de calcul des ordinateurs, si le mot de passe fait moins de 6 caractères et même s'il est composé de lettres majuscules et minuscules, de chiffres et de caractères spéciaux, il est possible de le **trouver presqueinstantanément.**

Cependant dans la réalité, les attaquants vont plutôt utiliser des dictionnaires composés des mots de passe les plus probables. Par exemple : Azerty1234, Soleil, etc…

(cf. Campagne Hack Academy - JENNY[jQ_BzKKSzqE])

Solution n°5

[exercice p. 4]

Qu'est-ce qu'un logiciel malveillant (malware) dans le contexte scolaire ?

Un programme informatique utilisé pour améliorer la sécurité des ordinateurs scolaires.

Un logiciel éducatif pour enseigner la programmation aux élèves.

✓ Un programme informatique nuisible visant à endommager ou voler des données

Un type de matériel informatique

Un logiciel malveillant (malware) est un programme informatique conçu pour nuire ou exploiter un système informatique. Il peut prendre plusieurs formes, comme:

- des *virus* p.34,
- des *vers* p.33,
- des *chevaux de Troie* p.33,
- des *logiciels espions* p.33 (*Spyware*).

Dans un contexte scolaire, le malware peut compromettre la sécurité des données sensibles des élèves et des enseignants, ou perturber le fonctionnement des systèmes informatiques.

Les autres options sont incorrectes : le malware n'est pas un programme de sécurité ni un outil éducatif ou de gestion.

Glossaire

Cheval de Troie (Trojan horse)

Un **cheval de Troie** (*Trojan horse* en anglais) est un type de logiciel malveillant, qui ne doit pas être confondu avec les virus ou autres parasites. Le cheval de Troie est un logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante. Son but est de faire entrer cette fonctionnalité malveillante sur l'ordinateur et de l'installer à l'insu de l'utilisateur.

Logiciel espion

Un **logiciel espion**, un **mouchard** ou un **espiogiciel** (de l'anglais ***spyware***) est un logiciel malveillant qui s'installe dans un ordinateur ou autre appareil mobile, dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données.

Le terme de *logiciel espion*, dont l'usage est préconisé par la commission générale de terminologie et de néologie en France, contrairement à l'anglicisme *spyware* ou au terme québécois *espiogiciel*, est une traduction du mot anglais *spyware*, qui est une contraction de *spy* (espion) et *software* (logiciel).

Stealer

Un infostealer est un terme d'informatique désignant une forme de logiciel malveillant créé dans le but de pénétrer les systèmes d'information et d'y voler des informations sensibles. Il peut notamment s'agir d'informations de connexion, d'informations financières ou d'autres données personnelles. Les informations volées sont ensuite mises en paquet, envoyées à l'attaquant et vendues sur des marchés illicites à d'autres cybercriminels. Wikipédia(FR)[40]

Ver informatique

Un **ver informatique** est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet. Il a la capacité de se dupliquer une fois qu'il a été exécuté. Contrairement au virus, le ver se propage sans avoir besoin de se lier à d'autres programmes exécutables. (Source : wikipédia[41] , fr)

40. Infostealer - https://fr.wikipedia.org/wiki/Infostealer
41. Ver informatique - https://fr.wikipedia.org/wiki/Ver_informatique

Virus informatique

Un **virus informatique** est un automate logiciel autoréplicatif. Certains sont inoffensifs, d'autres contiennent du code malveillant (ce qui entraine le classement du logiciel comme logiciel malveillant). Dans tous les cas, un virus informatique est conçu pour se propager sur d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés « hôtes » à la manière d'un virus biologique. Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Un virus se répand par tout moyen d'échange de données numériques, comme les réseaux informatiques ou les périphériques de stockage externes (clés USB, disques durs, etc.).

Abréviations

Amigo : Assistance mutualisée informatique du grand-Ouest
ANSSI : Agence nationale de la sécurité des systèmes d'information
DPD : Délégué à la protection des données
Drane : Délégation régionale au numérique éducatif
ENT : espace numérique de travail
MOOC : Massive open online course (cours en ligne ouvert à tous)
PDSI : Protection des données et des systèmes d'information
RGPD : Règlement général sur la protection des données
USB : Universal Serial Bus

Références

Source de statistiques	Dynamips : Synthèse des tendances et chiffres-clés pour 2024[42]

Index

Crédits des ressources

Bien choisir son mot de passe p. 31
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane - Nantes

42. Les cyberattaques contre les établissements scolaires : tendances et chiffres clés - https://www.dynamips.com/cyberattaques-etablissements-scolaires-tendances-chiffres-cles/

Les vulnérabilités des écoles dans les cyberattaques p. 5
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane Nantes

Concept de rançongiciel (ransomware) p. 5
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Canva - image générée par IA

Les cyberattaques et les failles humaines p. 5
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane Nantes

Répartition des incidents de cyberattaque en 2023-2024 - Académie de Nantes p. 6
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane - Nantes

Comment les compte sont piratés ? p. 6
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane Nantes

Les menaces courantes en cybersécurité p. 7
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane Nantes

Identifier les signes d'un hameçonnage p. 9
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane - Nantes

Comment se protéger contre le hameçonnage ? p. 9
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane - Nantes

Logo de la plateforme 17 Cyber p. 10
Attribution - @ cybermallveillance.gouv.fr[43]

Les bonnes pratiques dans le cadre professionnel p. 10
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane Nantes - réalisé avec l'IA

Les actions pour se protéger dans les établissements scolaires p. 11
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane Nantes - réalisé avec l'IA

Comment se protéger à la maison ? p. 13
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane Nantes - réalisé avec l'IA

Conseils aux usagers p. 15
Attribution - SIG

43. cybermallveillance.gouv.fr - https://www.cybermalveillance.gouv.fr/medias/2024/01/Assistant-cyber-en-ligne.png

Comment sécuriser les connexions wifi publics p. 16
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane-Nantes

Les types d'attaques courantes sur les réseaux Wi-Fi publics p. 16
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane Nante

Présentation de pix p. 17
Attribution - GIP Pix[44]

Les domaines du référentiel des compétences numériques (CRCN) p. 18
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane Nantes - réalisé avec l'IA

L'accueil de la plateforme PIX p. 19
Attribution - pix.fr

Le référentiel « sécuriser l'environnement et les pratiques numériques» p. 30
Attribution - PIX - ANSSI - Cybermalveillance.gouv.fr

Risque liés au partage de mot de passe p. 20
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane Nantes

Les risques liés à la gestion des données personnelles p. 21
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane Nantes

Comment supprimer un virus de mon ordinateur ? p. 23
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane Nantes - Réalisé avec l'IA

Mesures indispensables pour sécuriser un compte qui a été piraté p. 24
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane Nantes - réalisé par l'IA

Que faire en cas d'hameçonnage ? p. 25
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane Nantes - Réalisé avec l'IA

Les règle simples pour éviter de se faire pirater p. 26
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane - Nantes - réalisé avec l'IA

Les procédures en cas de cyberattaque p. 27
Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions - Drane - image générée par IA

Logo de la fresque des cybercitoyens p. 28
Attribution - https://fresquedescybercitoyens.fr/

---

44. la plateforme Pix - https://pix.fr

Les cartes du jeu de la Fresque des cybercitoyens p. 28
Attribution - Pas d'Utilisation Commerciale - Pas de Modification - Drane - Nantes