



Pix 2023 2024 : Certification des 3èmes : planning, rappels, conseils...

publié le 24/05/2024 - mis à jour le 01/06/2024

Descriptif :

Dans le cadre de l'évaluation des compétences numériques, les élèves de 3e vont passer la certification PIX ce qui leur permettra d'attester leur niveau de compétences. Tout ce qu'il faut savoir est ici (...)

Sommaire :

- La certification PIX, ce qu'il faut savoir
- Examen officiel :
- Planning
- Comment se passe la certification ?
- Matériel à apporter et prérequis
- Rappels et conseils
- Etre certifiable ? Mais comment faire si je ne suis pas encore certifiable ?
- Aide si vous devez changer votre mot de passe EDUCONNECT

Dans le cadre de l'évaluation des compétences numériques, les élèves de 3e vont passer la certification PIX ce qui leur permettra d'attester leur niveau de compétences.

● La certification PIX, ce qu'il faut savoir



La certification Pix, ce qu'il faut savoir (Video Youtube)

● Examen officiel :

La charte des examens s'applique aux épreuves de certification PIX.

● Planning

- Voici l'organisation des différentes sessions dans notre collège ; elle se feront exceptionnellement cette année durant les séances de technologie :

classe	Date	Horaire	Salle
3eme 4	MARDI 28 MAI	10H40 - 12H30	Tech1
3eme 2	MERCREDI 5 JUIN	10H40 - 12H30	Tech1
3eme 3	LUNDI 10 JUIN	13H - 15H	Tech1
3eme 5	LUNDI 10 JUIN	15H - 17H	Tech1
3eme 1	MARDI 11 JUIN	13H - 15H	Tech1
3eme 6	MARDI 11 JUIN	15H - 17H	Tech1
3eme1234567	Rattrapage	VENDREDI 14 JUIN 8H30 - 10H30	Tech1

● Comment se passe la certification ?

- Par la plateforme publique Pix accessible via l'ENT Enej.

- Elle est organisée dans l'établissement, en classe entière dans la salle tech1 sous la responsabilité de 2 enseignants.
- Avant la passation, il vous sera expliqué en vidéoprojection le déroulement de la passation et les consignes à respecter, notamment la nature du test, la durée (1h45 maximum), les cas de fraude et leurs conséquences...)
- Lors de la session de certification vous devrez :
 - ▶ déposer à l'entrée de la salle tout ce qui n'est pas nécessaire pour l'examen : sacs, stylos/papiers et tout appareil de télécommunication.
 - ▶ déposer à votre emplacement votre pièce d'identité pour vérification
 - ▶ ne pas quitter la salle sans avoir émargé le document d'émargement.

● Matériel à apporter et prérequis

Matériel : Chaque élève devra être muni

- d'une pièce d'identité avec photographie
- d'écouteurs individuels filaires.

Prérequis : Comme déjà dit et écrit à de multiples reprises, il est indispensable de :

- **connaitre ses codes d'ouverture de session** informatique sur le réseau du collège
- **connaitre ses codes Educonnect**, pour accéder à l'ENT Enej puis PIX.
- **vérifier que son compte PIX fonctionne !**
- **être certifiable !** L'élève doit avoir validé au préalable, au cours des campagnes de test proposées, ou en autonomie, **au moins le niveau 1 dans 5 des 16 compétences du référentiel.** ; plus d'info ci-dessous

● Rappels et conseils

- Tout ce qu'il faut savoir sur PIX et les parcours de découverte demandés à tous les 5èmes, 4èmes, 3èmes en novembre 2023 est [ici, sur le site du collège](#)
- Il faut passer par l'ENT Enej puis "ressources" pour aller sur PIX : normalement tous les élèves du collège doivent être inscrits et donc reconnus.
- Si le compte pose problème, il est urgent de contacter le collège (PP ou professeur de technologie ou un des professeurs chargés du numérique)

● Etre certifiable ? Mais comment faire si je ne suis pas encore certifiable ?

Pas de panix ! voila la stratégie à suivre avant la séance de certification :



JE VAIS PASSER MA CERTIFICATION PIX

...ET JE NE SUIS PAS ENCORE CERTIFIABLE !
VOICI DES CONSEILS POUR LE DEVENIR RAPIDEMENT.

1. JE ME CONNECTE À MON COMPTE PIX

Je dois utiliser mon compte habituel, celui qui servira le jour de la certification.



J'en profite pour m'assurer que je connais mes identifiants



2. JE CONSULTE MON PROFIL DANS L'ONGLET *COMPÉTENCES*

Pour passer la certification, je dois atteindre le niveau 1 pour au moins 5 compétences parmi les 16 affichées sur mon profil.

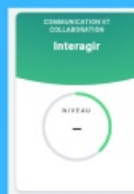


3. J'IDENTIFIE LES COMPÉTENCES À TRAVAILLER



Je repère les compétences sur lesquelles j'ai déjà travaillé : plus le cercle coloré est rempli et plus je suis proche du niveau 1.

Je travaille donc en priorité ces compétences.



4. JE RÉPONDS AUX QUESTIONS AU MOINS JUSQU'AU NIVEAU 1

Je réponds aux questions qui me sont posées.

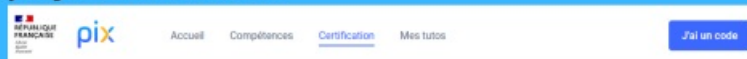
Quitter ➡



Je peux cliquer sur *Quitter* dès que j'atteins le niveau 1 pour travailler ensuite une autre compétence.

5. JE VÉRIFIE QUE JE SUIS BIEN CERTIFIABLE

Après avoir réussi au moins 5 compétences au niveau 1, je clique sur *Certification* pour vérifier que je suis certifiable.



Maintenant, je peux continuer à travailler les autres compétences, l'objectif est d'atteindre les 16 !

● Aide si vous devez changer votre mot de passe EDUCONNECT

NE PAS UTILISER :

- Des dates personnelles, de proches ou célèbres (Anniversaires, événements, etc.).
- Des références personnelles (Immatriculations anciennes ou actuelles de la voiture, etc.).
- Des noms ou surnoms (Personnes, animaux, jeux et jouets, objets fétiches, etc.).
- Des mots du dictionnaire (En français ou dans toute autre langue).
- Des suites de touches au clavier (AZERTY, QWERTY, YTREZA, 123456, 159753, etc.).
- Des répétitions (000111222333444).

Un bon mot de passe en 2024 :

- 15 caractères aléatoires minimum (Actuellement, l'idéal est de dépasser 20 caractères lorsque c'est possible).
- Majuscules.
- Minuscules.
- Chiffres.
- Caractères spéciaux.
- Usage unique (1 compte = 1 mot de passe).
- Renouvellement annuel pour les comptes peu importants.
- Renouvellement trimestriel pour les comptes à haut risque (Bancaires, fiscaux, etc.).

Trop dur à mémoriser ce nouveau mot de passe ? Vous pouvez utiliser un gestionnaire de mots de passe (C'est un coffre-fort numérique) qui génère des mots de passes et les sécurise. Vous n'avez plus qu'à en mémoriser un seul de 20 à 30 caractères pour utiliser le service. Certains services modifient les mots de passe dès qu'ils ont été utilisés une seule fois pour une meilleure sécurité.

Voir ce lien [Francenum.gouv.fr](https://francenum.gouv.fr).

Pourquoi ?

Les attaques informatiques sont nombreuses, quotidiennes, de plus en plus intenses au niveau international. Chaque jour, la France et d'autres pays d'Europe notamment, subissent de lourdes attaques, mais également des entreprises d'envergure mondiale qui sont souvent citées comme ayant des fuites de données sur les réseaux pirates. Les mots de passe des utilisateurs (Privés et professionnels) sont la première vulnérabilité des systèmes de sécurité.

En rendant les Intelligences Artificielles accessibles et avec des machines de plus en plus puissantes, il devient très facile pour beaucoup d'informaticiens en herbe de "casser" des mots de passe. Un mot de passe en 8 caractères, comme il était conseillé il y a encore cinq ans, est cassé en quelques minutes, voir en quelques secondes s'il est trop simple. En dessous de 15 caractères, il ne suffit que de quelques dizaines de minutes pour qu'un robot casse un mot de passe. Plus le mot de passe est complexe, plus le robot abandonne vite et passe à quelqu'un d'autre.

Comment fonctionnent les robots casseurs de mot de passe sur Internet ?

C'est bien simple, ils testent des mots de passe en série (Ils peuvent en tester des centaines par seconde sur plusieurs comptes en même temps). Mais ils ne testent pas au hasard !! Je ne vais pas citer les actions de piratage (Hameçonnage, rootkits, etc.) qui touchent plutôt la sécurité anti-virus informatique, uniquement la captation de données personnelles et techniques courantes.

Ils utilisent la totalité des informations piochées sur les réseaux sociaux (Les vôtres, mais aussi ceux de vos amis, famille, et personnes et comptes en lien avec vous). D'où l'importance d'être vigilants sur les informations visibles publiquement sur vos comptes et ceux des personnes en lien.

Ces algorithmes sont désormais capables de lire facilement des données prises en photo ou dans une vidéo. Il faut donc éviter de stocker des photos de vos identifiants, sauf si vous utilisez un coffre-fort

numérique (Des applications existent et sont gratuites). Ils utilisent (Depuis toujours) des dictionnaires de mots, et des bases de données rassemblant tous les mots de passe déjà cassés et connus ("Password" et "motdepasse", "azerty12345", "123456" sont testés parmi les premières tentatives).

Il est assez simple de sécuriser ses données personnelles et d'avoir des mots de passe puissants. Des outils existent pour aider celles et ceux qui se sentent peu à l'aise avec des ordinateurs et des smartphones. Internet contient des ressources pour y arriver en peu de temps.

Vous souhaitez des informations sur le piratage et les façons de se protéger ou faire des signalements ?

Cybermalveillance.gouv.fr



**Académie
de Poitiers**

Avertissement : ce document est la reprise au format pdf d'un article proposé sur l'espace pédagogique de l'académie de Poitiers.

Il ne peut en aucun cas être proposé au téléchargement ou à la consultation depuis un autre site.