élèves

Guide

POUR UTILISER L'ENT

NET CENTRE

Lycée Gustave Eiffel

Lycée Gustave Eiffel

ÉLÈVES

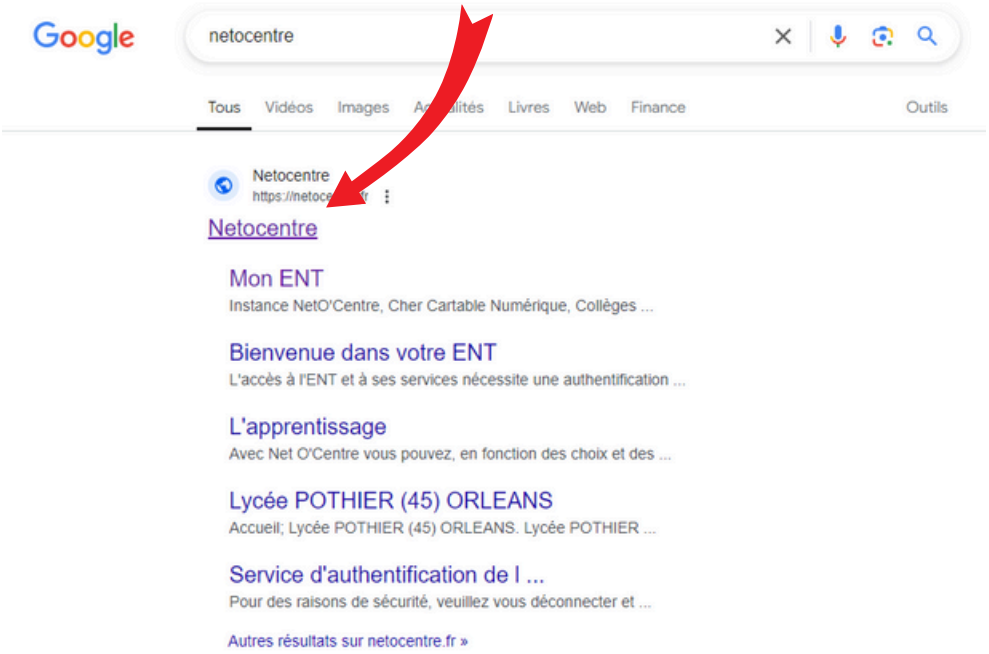
NET CENTRE

SE CONNECTER
À L'ENT DU LYCÉE

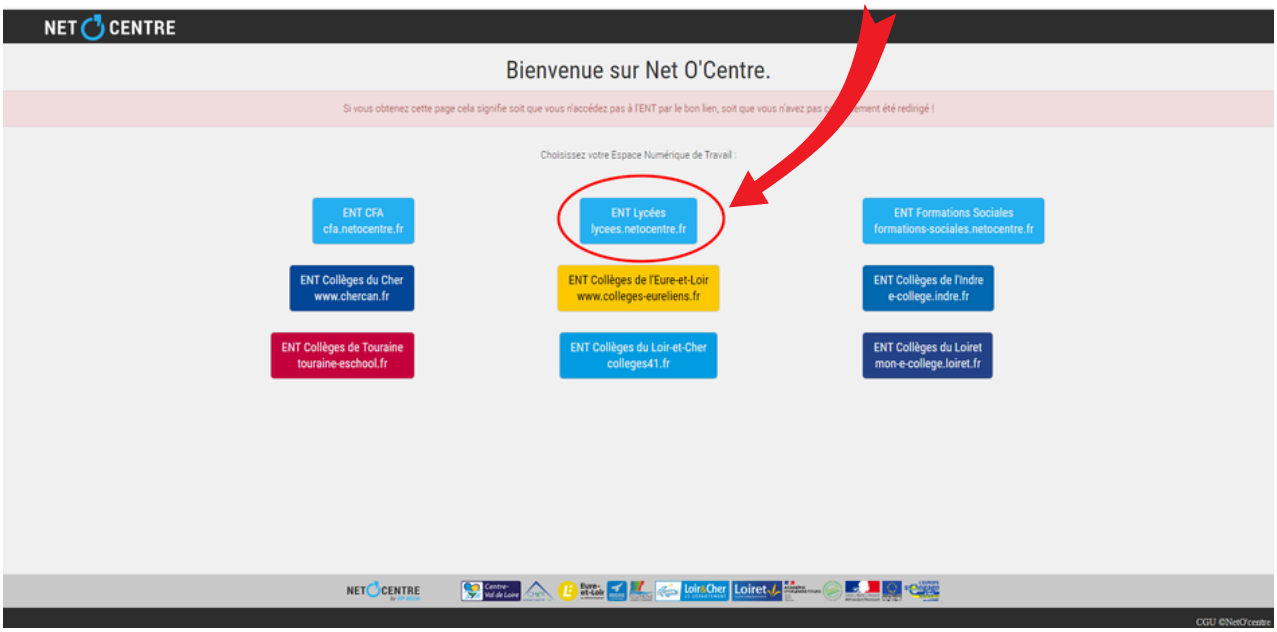
L'espace numérique de travail est un ensemble intégré de services et de ressources numériques (messagerie, Pronote…). L'ENT de la région Centre pour les lycées s'appelle Net O'Centre.

L'ENT du lycée est différent de celui du collège !
Au lycée, on n'utilise plus Touraine e-school mais Net O'Centre.

1 Taper "netocentre" dans la barre de recherche Google et cliquer sur Netocentre :

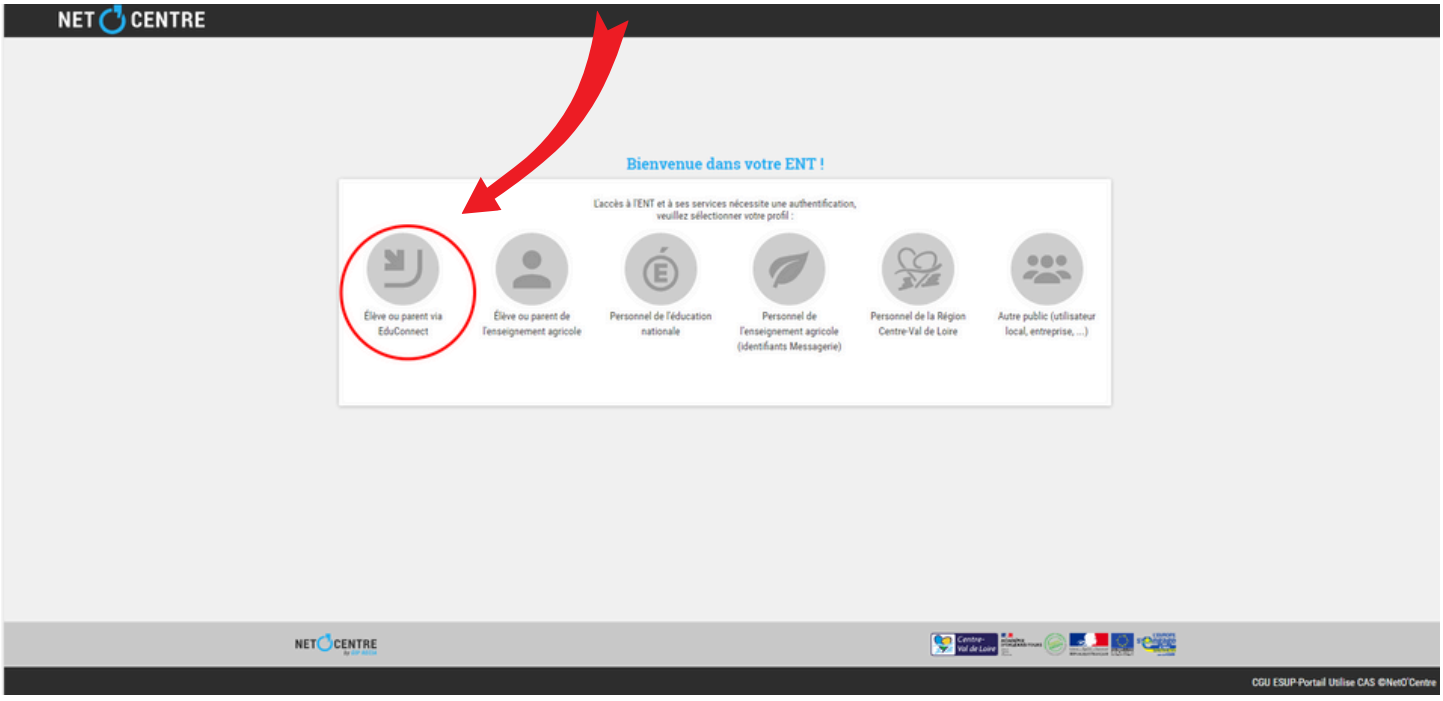


2 Choisir l'ENT lycées :



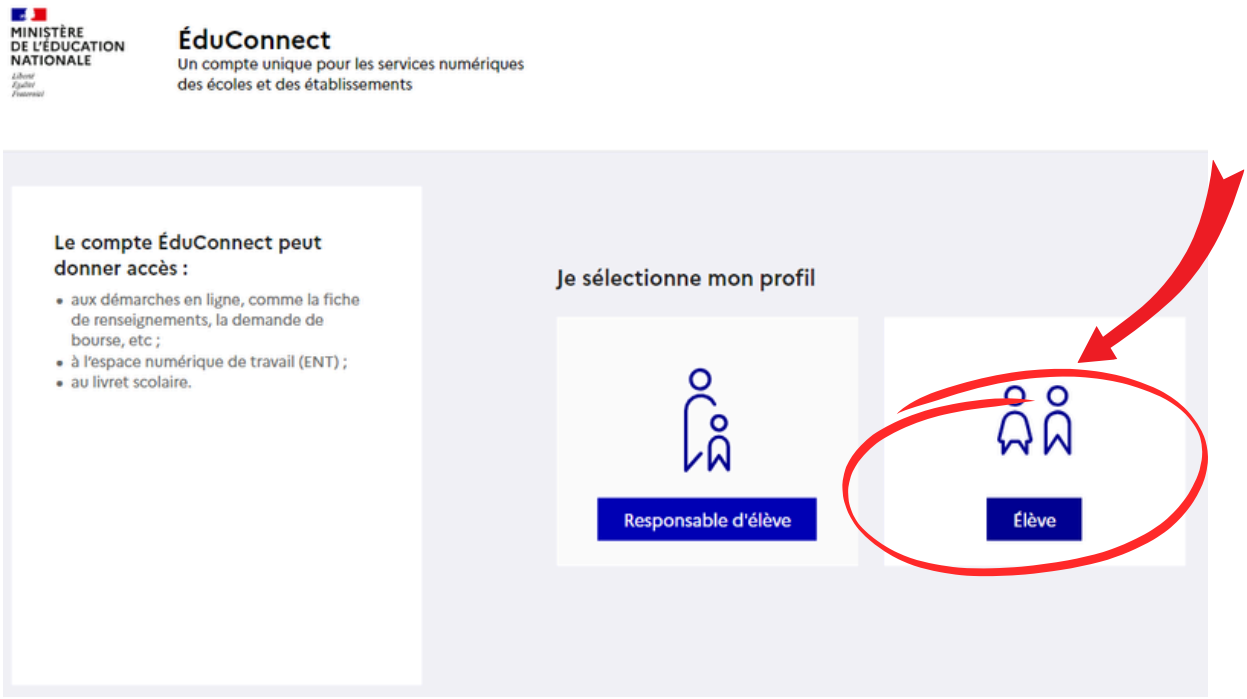
3 La page de l'ENT se charge. Il faut ensuite cliquer sur "Se connecter" en haut à droite :

4 Choisir ensuite le profil "Elève" :



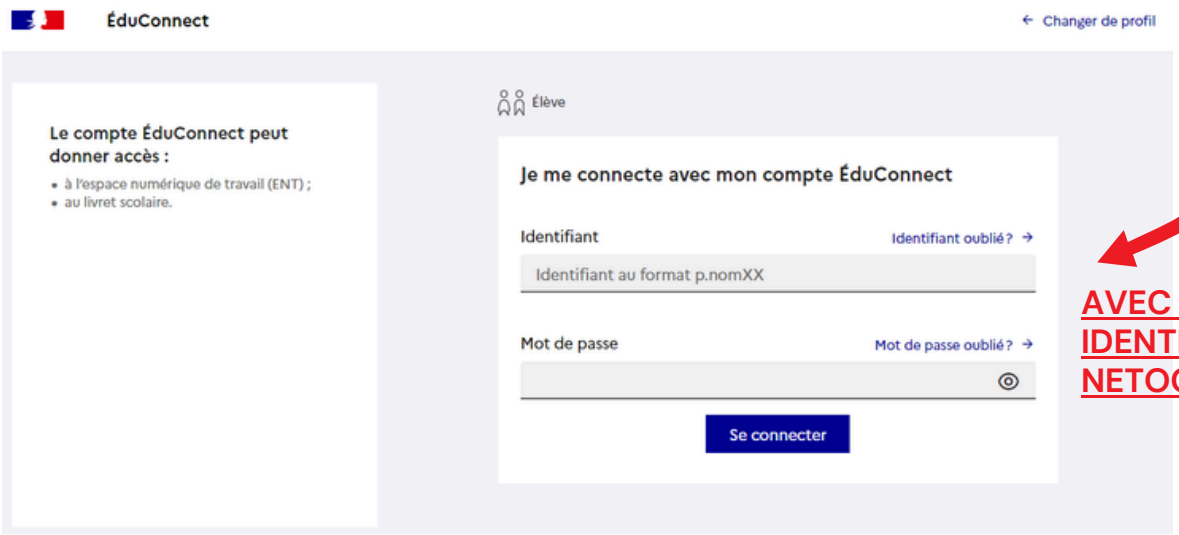
5

L’identification se fait ensuite avec le guichet Educonnect proposé par l'Éducation Nationale.
Choisir le profil “Elève” :



6

La connexion se fait avec les identifiants ENT.
Ce sont les mêmes que l’année scolaire précédente, même si l’élève était au collège (sauf établissement dans le privé).



AVEC LES IDENTIFIANTS ENT NETOCENTRE

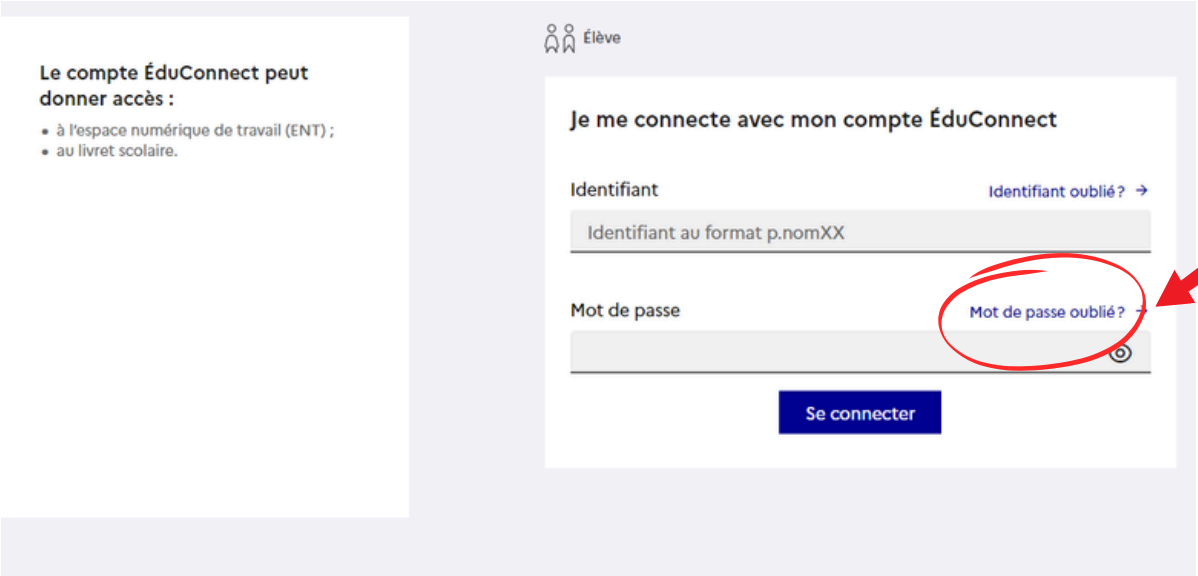
ÉLÈVES

NET CENTRE

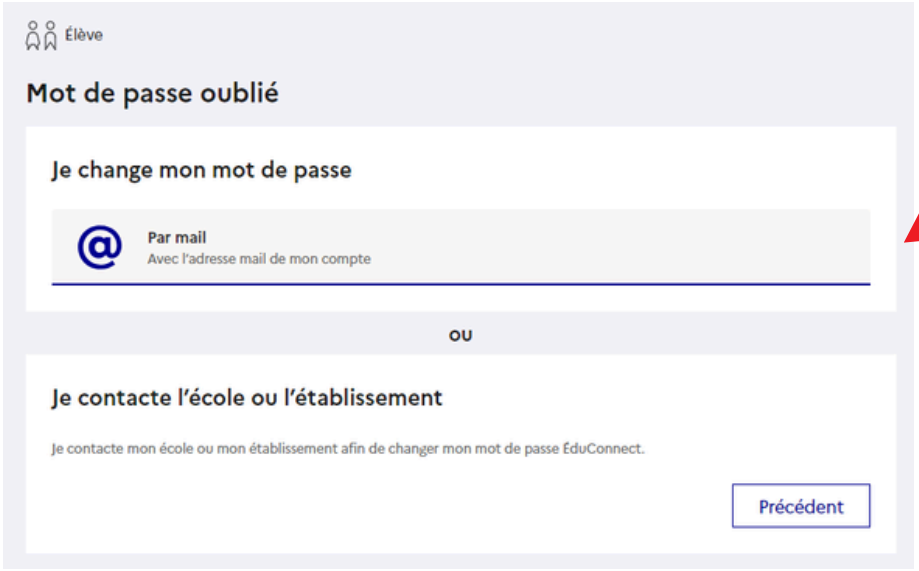
ENT

MOT DE PASSE PERDU

1 Si vous avez oublié votre mot de passe pour vous connecter à l'ENT, vous pouvez en recréer un en cliquant sur "Mot de passe oublié" de la page d'authentification Educonnect.

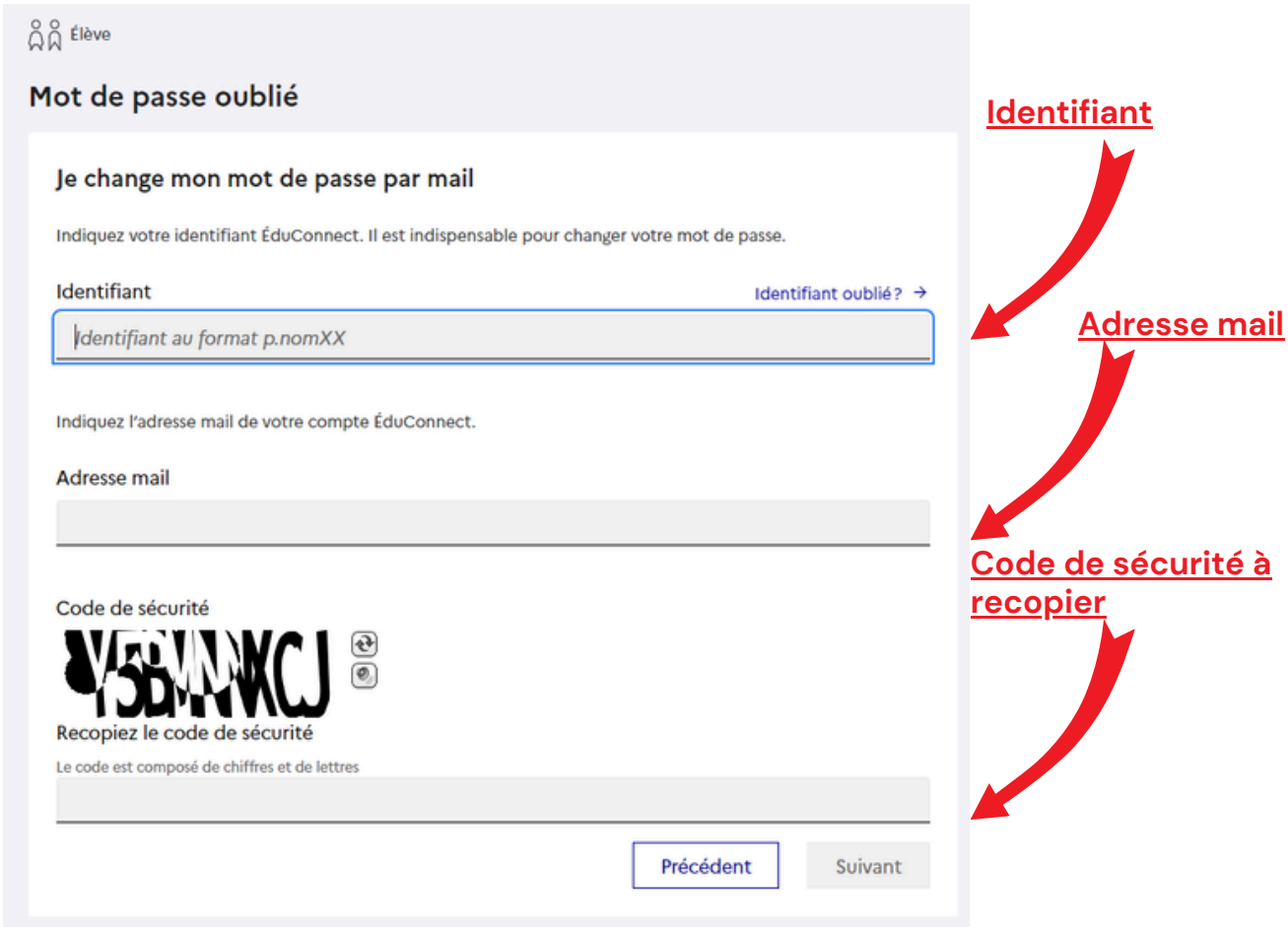


2 Vous pouvez le récupérer par mail si vous avez bien renseigné votre adresse mail dans votre compte EduConnect. Cliquer sur "Par mail".



Par mail

3 Ensuite, renseigner l'identifiant, l'adresse mail et recopier le code de sécurité.



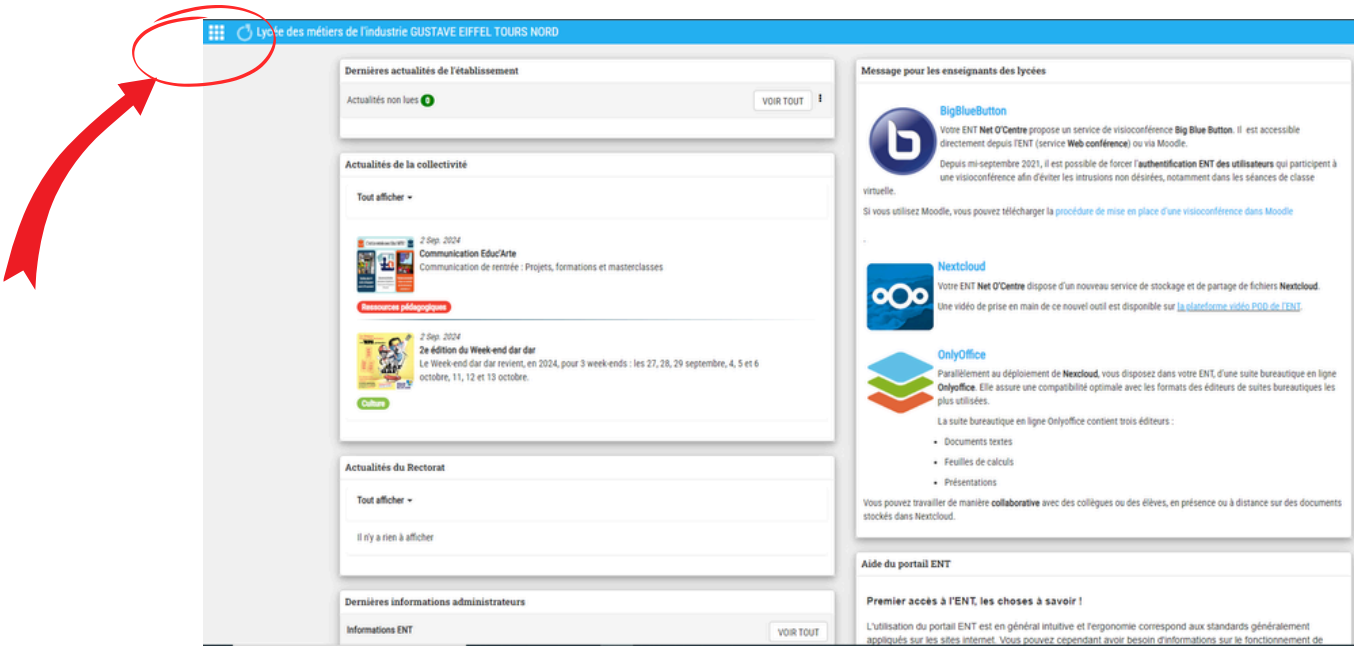
Un lien est envoyé par mail pour changer le mot de passe.

La démarche est la même pour l'identifiant oublié.

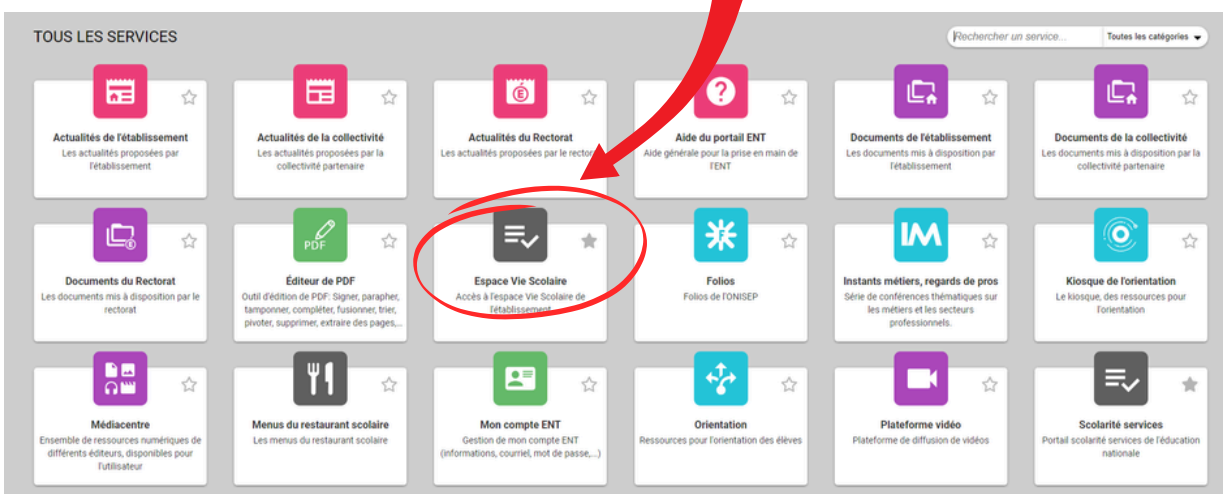
4 Si vous n'avez pas reçu le lien par mail, il faut contacter le lycée qui procédera au changement du mot de passe.

ACCÉDER À PRONOTE

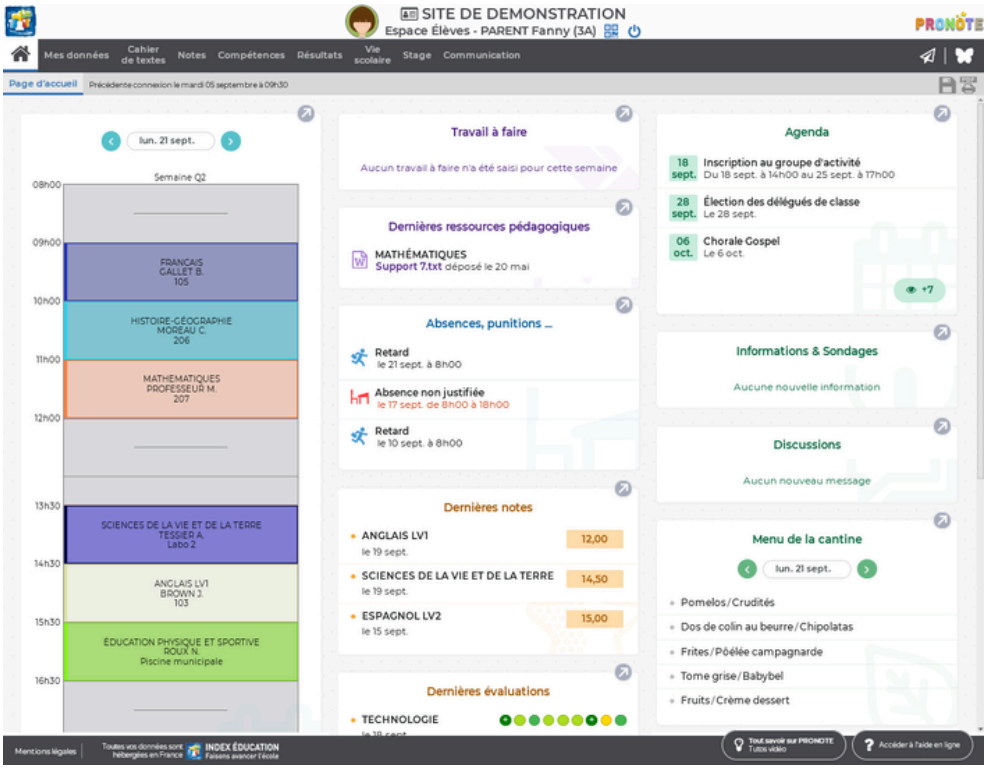
1 Une fois connecté à l'ENT, l'utilisateur accède à sa page d'accueil et va pouvoir utiliser les services mis à sa disposition par l'établissement.
L'accès aux services se fait en cliquant sur en haut à gauche :



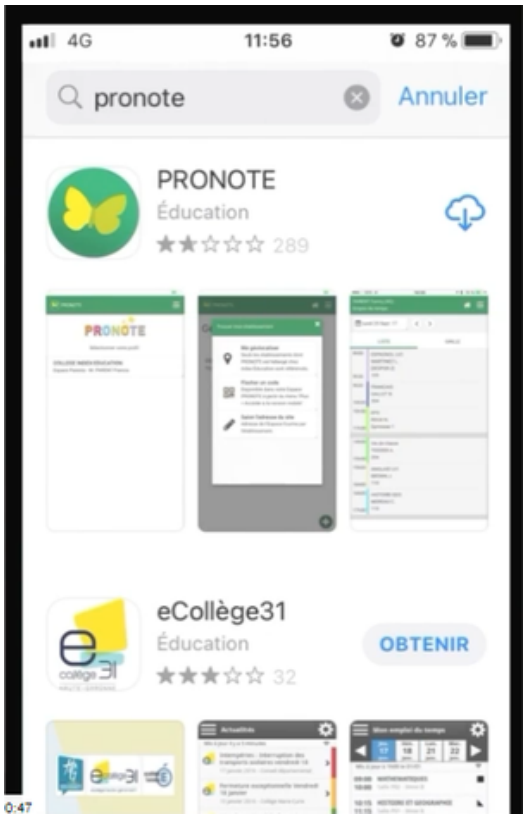
2 Pour accéder à Pronote, il faut cliquer sur la brique "Espace vie scolaire" :



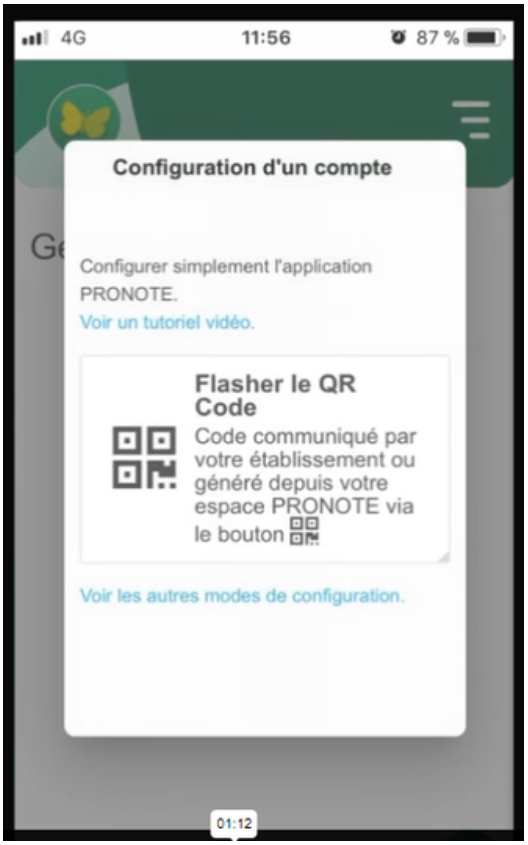
3 L’espace “Elève” donne accès à l’emploi du temps, au travail à faire, et aux informations transmises par le lycée :

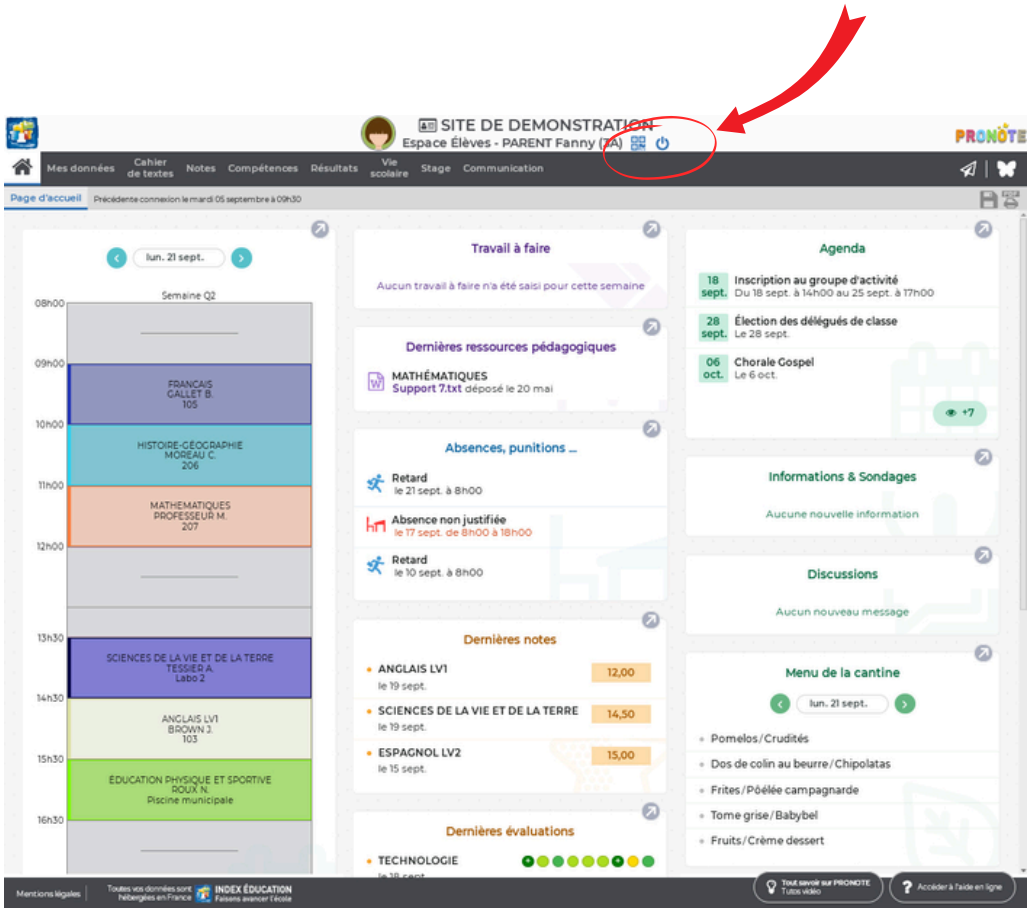


4 Pour installer l’application Pronote sur un smartphone, il faut télécharger Pronote depuis le store :



5 Pour ajouter et configurer un compte, il faut flasher le QR Code généré à partir de l'"Espace vie scolaire" accessible depuis l'ENT sur un ordinateur :



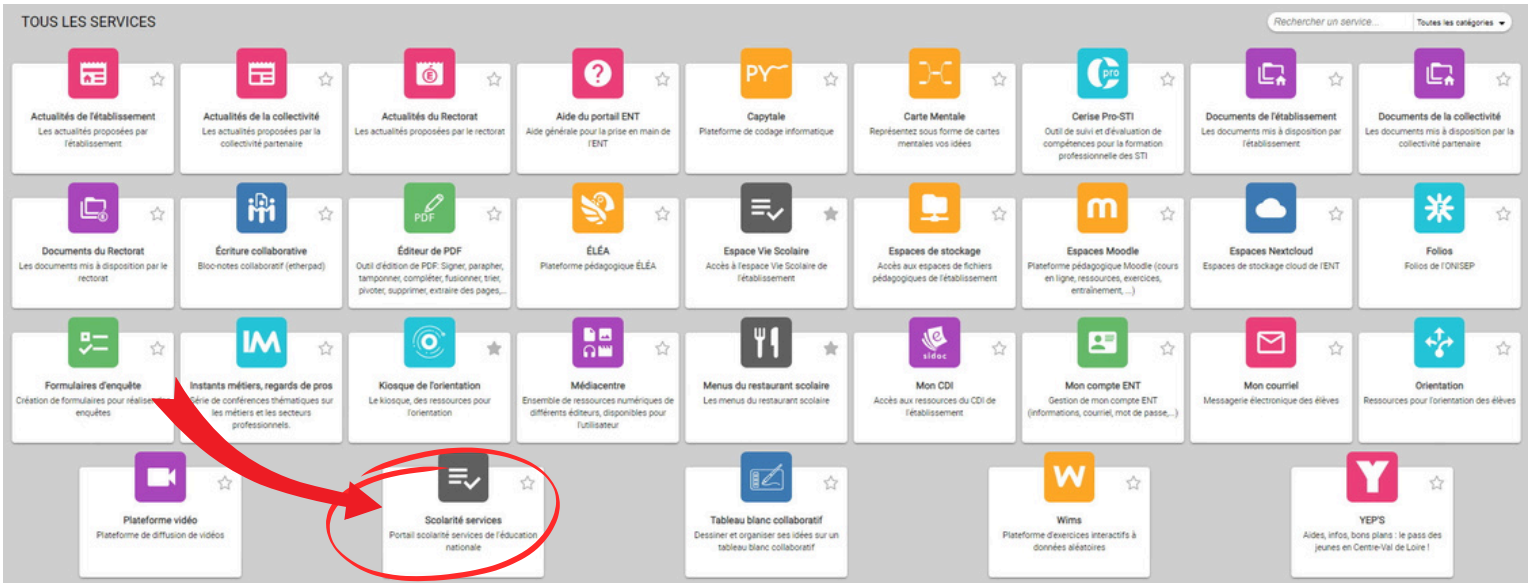


ÉLÈVES

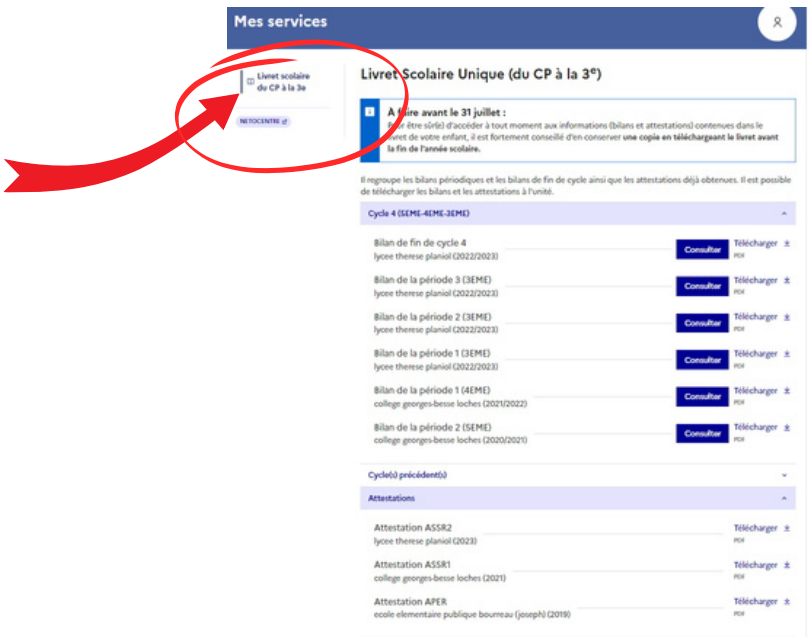
NET CENTRE

OBTENIR
SES BULLETINS, SON ASSR

1 Se connecter à l'ENT et cliquer sur la tuile "Scolarité services"



2 Les attestations ASSR et les bulletins sont disponibles dans l'onglet "Livret scolaire du CP à la 3e" :



10 conseils de la CNIL pour rester Net sur le web

1 Réfléchir avant de publier

Sur internet, tout le monde peut voir ce que tu publies : photos, vidéos, opinions, etc.

2 Respecter les autres

Tu es responsable de ce que tu publies sur les réseaux sociaux... Ne fais pas aux autres ce que tu ne voudrais pas que l'on te fasse.

3 Ne pas tout dire

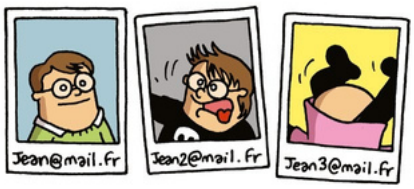
Donner le minimum d'informations sur soi en ligne, c'est se protéger ! Mieux vaut ne pas communiquer tes opinions, ta religion ou ton numéro de téléphone...

4 Sécuriser ses comptes

En paramétrant tes profils sur les réseaux sociaux, tu restes maître des informations que tu souhaites partager.

5 Créer plusieurs adresses mail

Tu peux par exemple utiliser une adresse pour les jeux vidéos, une pour tes amis et une autre boîte e-mail pour les réseaux sociaux.



6 Faire attention à tes photos et tes vidéos

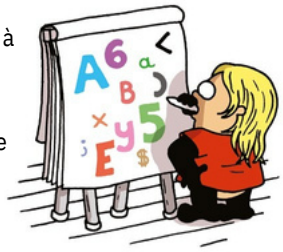
Envoyer, publier une photo ou une vidéo gênante de soi ou des autres, c'est risquer une diffusion incontrôlable.

7 Utiliser un pseudonyme

Seules les personnes à qui tu l'auras communiqué sauront qu'il s'agit de toi et suivront tes aventures sur le net.

8 Protéger ses mots de passe

Il faut qu'il soit difficile à deviner et différent pour chaque service. Évite d'utiliser ton surnom ou bien ta date de naissance par exemple. Et surtout, garde-le pour toi !



9 Nettoyer ses historiques

Pour éviter d'être tracé, il est conseillé d'effacer régulièrement tes historiques de navigation et d'utiliser la navigation privée si tu utilises un ordinateur ou un smartphone qui n'est pas le tien.

10 Surveiller sa réputation en ligne

Taper ton nom dans un moteur de recherche te permet de savoir ce qui est dit sur toi sur internet et quelles informations circulent.

Partage ces conseils avec tes amis et ta famille pour qu'ils protègent eux aussi leur vie privée !

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Retrouvez d'autres conseils sur www.cnil.fr

EFIL / www.efil.fr / 20150407 - Illustrateur : Martin Vidberg - Juin 2015

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.

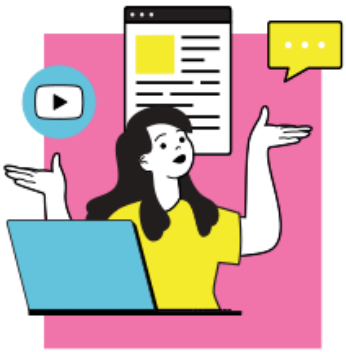
2 LES MISES À JOUR DE TES APPAREILS SANS TARDER TU FERAS

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

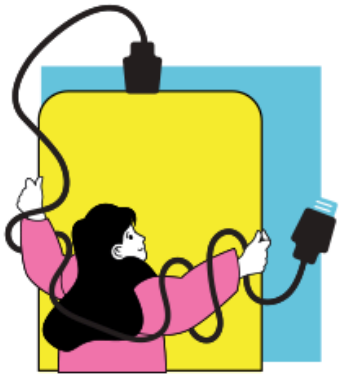


Publier et partager tes données personnelles sur Internet (nom, prénom, adresse mail, photos, vidéos, vocaux…) peut les exposer à une utilisation malveillante.

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 t'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
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

CYBER MOIS

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

Octobre 2023- CNIL