ACADÉMIE
DE VERSAILLES

Liberté
Égalité
Fraternité

LIVRET D'ACCOMPAGNEMENT

L'ACADÉMIE
vous accompagne

SÉCURITÉ NUMÉRIQUE L'AFFAIRE DE TOUS !

L'académie de Versailles
mobilise tous les acteurs de la communauté éducative pour

- Sensibiliser aux enjeux de la sécurité numérique
- Mettre à disposition des kits «clés en main »
- Créer des parcours d'auto-formation
- Découvrir les métiers de la cybersécurité
- Organiser des évènements pour fédérer

SENSIBILISER ÉDUQUER FORMER

DANE - DSI

SÉCURITÉ NUMÉRIQUE

RÈGLES D'HYGIÈNE NUMÉRIQUE

Protégez vos accès avec des mots de passe solides

- Utilisez des mots de passe **robustes** constitués d'au moins 12 caractères, contenant des lettres majuscules et minuscules, des chiffres et des caractères spéciaux. Exemple : Générer un mot de passe solide | CNIL ou Numérique et Vous : Le mot de passe (podcast) | DANE de Versailles
- Utilisez un mot de passe **différent** pour chacun des services que vous utilisez afin d'éviter une compromission globale de ceux-ci.
- **Renouvelez** fréquemment vos mots de passe (préconisation : 6 mois). Cela vous prémunira si des services en ligne sont compromis et que des comptes d'utilisateurs fuitent sur internet.
- Conservez votre mot de passe en **lieu sûr** (ex : coffre numérique avec le logiciel Keepass)
- Ne laissez pas de sessions ouvertes accessibles sur vos terminaux en votre absence. Pensez à **verrouiller votre session** ou à vous déconnecter avant de quitter votre poste de travail.

Utilisez votre messagerie avec précaution

- Vérifiez la **cohérence** entre l'expéditeur, le sujet, le contenu du message, les pièces jointes, ainsi que la cohérence entre l'adresse des liens et le texte affiché avant de l'ouvrir.
- Face à un message suspect, assurez-vous auprès de l'**émetteur** qu'il en est bien à l'origine en le contactant par un autre canal.
- N'utilisez votre messagerie professionnelle que dans le **cadre de vos échanges professionnels.**
- Évitez de rediriger des courriels depuis votre messagerie professionnelle vers une messagerie personnelle, et inversement.
- Ne relayez pas les messages non-professionnels de type **chaîne de lettres**, appels à solidarité, etc.

SÉCURITÉ NUMÉRIQUE

RÈGLES D'HYGIÈNE NUMÉRIQUE

Appliquez les mises à jour de sécurité sur vos appareils

- Appliquez les mises à jour du **système d'exploitation** de vos appareils, des logiciels et des applications dès qu'elles vous sont proposées. Vous corrigez ainsi les failles de sécurité qui pourraient être utilisées par des pirates pour s'introduire dans vos appareils, pour y dérober vos informations personnelles ou vos mots de passe, voire pour détruire vos données ou encore vous espionner.
- N'installez des applications ou des logiciels que depuis les sites ou les **magasins officiels**.

Utilisez un antivirus à jour

- Installez si besoin la version **financée par le ministère** : https://edu.trendmicro.fr/view/index.php
- Vérifiez régulièrement que les antivirus de vos **équipements sont bien à jour** et **faites des analyses** (scans) approfondies pour vérifier que vous n'avez pas été infecté.

En cas d'infection supposée

- Isoler au plus vite le poste infecté en le **déconnectant de tout réseau** (filaire et sans-fil).
- Isoler au plus vite tout support de sauvegarde externe (clé USB ou disque externe) ayant été raccordé au poste infecté dans le mois qui précède l'infection.

Terminal professionnel : **signaler l'incident à votre assistance** de proximité (référent numérique, collectivité territoriale, plate-forme CARIINA…).

Terminal personnel :

- **Ne payez pas la rançon** qui vous serait réclamée dans le cas d'une attaque par rançongiciel.
- Si vous disposez d'une sauvegarde de vos données, reformatez le poste infecté, réinstallez un système d'exploitation sain, puis procédez ensuite à la restauration de vos données.
- En l'absence de sauvegarde, effectuez un scan du terminal ou du support externe à l'aide d'un antivirus portable.
  Exemple : Analyse antivirus en ligne gratuite | Trend Micro

SÉCURITÉ NUMÉRIQUE

RÈGLES D'HYGIÈNE NUMÉRIQUE

Privilégiez les outils proposés par l'institution

- **Boite à outils** ARIANE , APPSEDU , outils des collectivités (ENT…)
- Saisissez vos identifiants professionnels uniquement sur des sites dont l'adresse est connue. **Ne vous fiez pas à l'apparence du site mais à son adresse.**

Séparez vos usages personnels et professionnels

- Utilisez uniquement vos **messageries professionnelles** (académique ou ENT) pour vos échanges dans la **pratique de votre métier**.
- N'utilisez pas vos adresses de messagerie professionnelles pour des usages personnels (exemple : sites e-commerce).
- **Evitez d'enregistrer dans le navigateur** d'un ordinateur appartenant au réseau d'un établissement scolaire, les identifiants de connexion à vos outils professionnels ou personnels.

Maîtrisez vos réseaux sociaux

- Sécurisez l'accès à vos réseaux sociaux avec un **mot de passe solide et différent** pour chacun d'entre eux.
- **Paramétrez les autorisations** sur vos informations et publications pour qu'elles ne soient pas inconsidérément publiques ou utilisées pour vous nuire.
- Activez la **double authentification** si celle-ci vous est proposée.

SÉCURITÉ NUMÉRIQUE

EXEMPLE D'INCIDENTS

Usurpation d'identité sur l'ENT

Chronologie de l'incident

- Un enseignant laisse malencontreusement sa session ouverte sur un ordinateur de l'établissement.
- Un élève récupère l'identifiant et le mot de passe du compte ENT de l'enseignant, enregistrés dans le navigateur.
- L'élève se connecte au compte ENT de l'enseignant depuis l'extérieur de l'établissement afin :
  - d'envoyer des messages d'insultes via la messagerie ;
  - de modifier des notes attribuées par l'enseignant.

Actions menées en réaction

- L'enseignant informe son chef d'établissement et déclare un ticket d'incident de sécurité sur la plate-forme CARIINA, pris en charge par le responsable de la sécurité des SI (RSSI) de l'académie.
- L'enseignant dépose plainte en commissariat ou en gendarmerie.
- Sur la base du dépôt de plainte, le RSSI recueille les éléments de preuve dans les journaux de l'ENT auprès de l'éditeur.
- Les éléments sont transmis à l'OPJ en charge de la plainte.
- Réquisition de l'OPJ auprès du FAI identifié et obtention de la localisation physique de l'adresse IP du contrevenant.

Verrouiller sa session lorsque l'on s'éloigne de son terminal.
Saisir ses identifiants en dehors de la vue d'autres personnes.

SÉCURITÉ NUMÉRIQUE

COMMENT SE FORMER ET S'ÉVALUER ?

Des ressources

Dès maintenant

- Certification PIX (https://pix.fr)
- Parcours PIX traitant de la cybersécurité (https://pix.fr/actualites/partenariat-pix-anssi-cybermalveillance/)
- MOOC de l'ANSSI (https://secnumacademie.gouv.fr)
- Site gouvernemental "Cyber malveillance" (https://www.cybermalveillance.gouv.fr/)
- Site de la CNIL (https://www.cnil.fr/fr/cybersecurité)

À venir

- Parcours de formation à la sécurité numérique sur MAGISTERE.
- Des kits d'accompagnement dédiés à la sécurité numérique et adaptés à différents publics.
- Programmation d'événements à l'échelle académique, départementale ou à celle des bassins