ACADÉMIE
DE VERSAILLES

Liberté
Égalité
Fraternité

ACADÉMIE
DE VERSAILLES

Liberté
Égalité
Fraternité

Actualités de la sécurité numérique
Usage sécurisé des outils numériques

Olivier Desport
Responsable de la sécurité de SI de l'académie

Sommaire

ACADÉMIE
DE VERSAILLES

Liberté
Égalité
Fraternité

1- DÉFINITION DE LA SSI

Définition

La SSI (Sécurité des systèmes d'Information) constitue l'ensemble des moyens humains et techniques mis en œuvre permettant d'assurer :

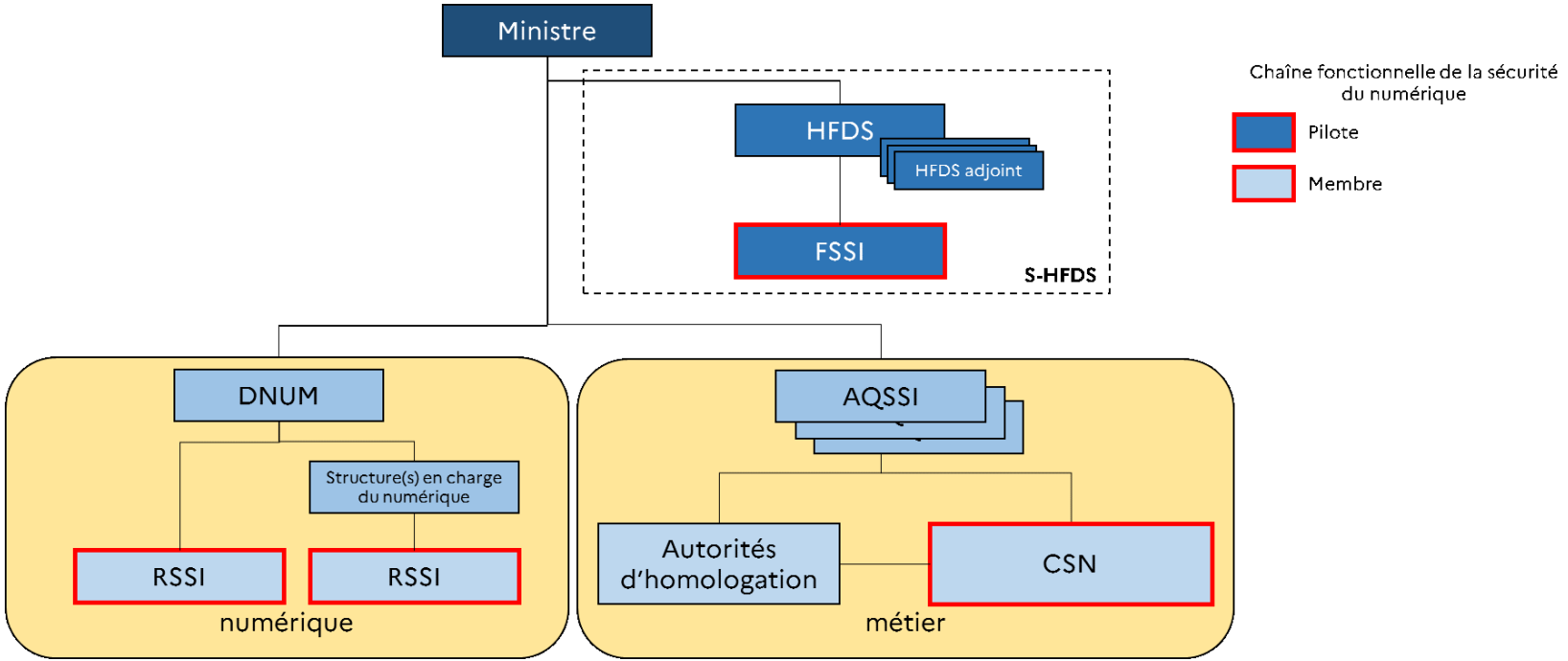
- **la confidentialité des données** (seules les personnes autorisées peuvent accéder à une ressource donnée),
- **l'intégrité** (l'information doit être fiable et ne doit pas avoir été modifiée de manière fortuite ou malveillante)
- **la disponibilité** (le service doit être accessible aux heures définies),
- **la traçabilité** (les accès aux services et aux informations est conservé dans des journaux)
- **la non-répudiation** (les utilisateurs ne doivent pas pouvoir contester les actions qu'ils effectuent)

ACADÉMIE
DE VERSAILLES

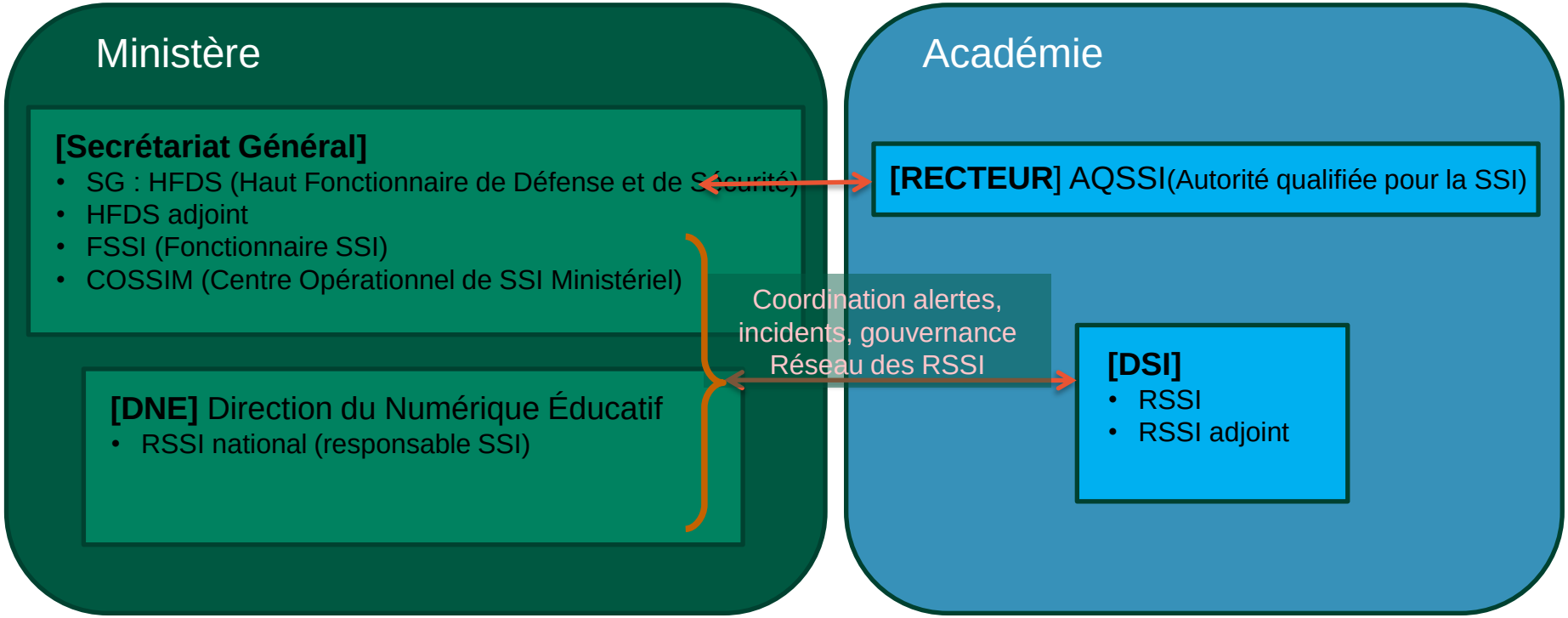
Liberté
Égalité
Fraternité

2- GOUVERNANCE DE LA SSI

Gouvernance nationale



Gouvernance du MENJS



Gouvernance de la région académique : la DRASI

8 fonctions transverses

Gouvernance de la région académique : la DRASI

Comité opérationnel SSI

Pilote : RSSI Versailles

Membres : RSSI et adj. Créteil / Paris / Versailles

- **Gouvernance et actions régionales**
- Politiques de sécurité
- Sensibilisation
- Gestion des incidents
- Gestion de crise
- Protection et résilience des infrastructures
- Audit de sécurité

Gouvernance académique (1)

Le recteur en sa qualité d'AQSSI, est juridiquement responsable de la SSI pour l'académie. Elle exerce :

- la maîtrise d'ouvrage (définition des enjeux de sécurité liés aux systèmes d'information),
- la responsabilité de passer des actes contractuels (marchés publics),
- la responsabilité de mettre en place des organisations (comité de pilotage de la SSI, logistique de crise),
- les arbitrages budgétaires,
- la possibilité, le cas échéant, d'intenter une action en justice.

Le responsable de la sécurité des systèmes d'information (RSSI) est nommé et mandaté par l'AQSSI pour mettre en place la politique générale de sécurité des systèmes d'information. Le RSSI est le responsable opérationnel.

Gouvernance académique (2)

- Mise en place d'un système de gouvernance au niveau de l'académie
  - Établir une politique adaptée à l'académie
  - Fixer les objectifs
  - Attribuer les moyens et contrôler leur efficacité afin d'atteindre ces objectifs
- Enjeux de la gouvernance
  - Augmentation de la fiabilité, gestion du risque et minimisation de l'impact des incidents de sécurité
  - Confiance des parties prenantes (autorités, partenaires, personnels, les élèves et leurs parents, le grand public)
  - Adoption de bonnes pratiques appropriées aux besoins
  - Conformité aux exigences nationales et académiques

Le RSSI au sein de la DSI

Le recteur désigne au sein de la DSI un RSSI, qui assure les rôles de conseil, d'assistance, d'information, d'alerte et de préconisation :

- il émet des préconisations, assure la communication et la formation,
- il contrôle régulièrement le niveau de sécurité du système d'information,
- il assure le traitement de crises (liaison COSSIM, réquisitions judiciaires …),
- il est identifié comme le référent par tous (rectorat, DSDEN, EPLE, partenaires …),
- il établit la confiance numérique en améliorant le niveau de sécurité.

Quel lien entre SSI et RGPD ?

- RGPD (Règlement Général sur la Protection des Données) : règlement visant à garantir et protéger l'accès aux données à caractère personnel des citoyens européen
  - Consentement des utilisateurs
  - Minimisation des données recueillies
  - Loyauté : données recueillies selon des procédés clairs et transparents
  - Intégrité : les données doivent être protégées et conservées dans le temps utile à leur traitement
  - Finalité : Les données personnelles ne peuvent être obtenues que pour des « finalités déterminées, explicites et légitimes »
- Le RSSI vérifie que les données personnelles sont traitées et conservées en toute sécurité grâce à des mesures techniques et organisationnelles appropriées et conformes aux exigences SSI académiques et nationales
- La SSI s'applique également aux données ne contenant pas de données à caractère personnel (données financières, stratégiques…)

Politique de confiance numérique

Publication

https://www.ac-versailles.fr/la-politique-de-confiance-numerique-de-l-academie-125689

Référentiels

CODE	TITRE	DESCRIPTION
RES-MAITRISE	Systèmes autorisés sur le réseau	Seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau local d'une entité, à l'exception des équipements personnels des enseignants et de tout autre équipement personnel s'ils sont cloisonnées dans un sous-réseau ne permettant pas d'accéder aux ressources locales.
RES-INTERCO	Interconnexion avec des réseaux externes	Toute interconnexion entre les réseaux locaux d'une entité et un réseau externe (réseau d'un tiers, Internet, etc.) doit être réalisée via les infrastructures nationales.
RES-ENTSOR	Filtrage réseau pour les flux sortants et entrants.	Dans l'optique de réduire les possibilités offertes à un attaquant, les connexions des machines du réseau interne vers l'extérieur doivent être filtrées.
RES-FILTRAGE-WEB	Filtrage des accès au web	Les accès à internet sur les protocoles FTP(S), HTTP(S) sont journalisés et filtrés afin de protéger le SI contre des usages malveillants ou non appropriés. Les utilisateurs peuvent demander au RSSI un avis pour lever une interdiction. Les journaux d'accès sont conservés sur douze mois glissants.
RES-PROT	Protection des informations	Les accès à Internet passent obligatoirement à travers des passerelles maîtrisées de l'entité. Dès lors que des informations sensibles doivent transiter sur des réseaux non maîtrisés, il convient de les protéger spécifiquement par un chiffrement adapté.

Politique de confiance numérique

Annexe 4 - Charte des personnels

Devoir de réserve dans ses communications effectuées avec son identité numérique professionnelle

- À destination d'acteurs externes à l'institution
- Outils : messagerie, réseaux sociaux…

▼ Protection de l'institution

▼ Protection du personnel (limitation de son exposition)

Assurer la continuité de service

- En cas d'absence d'un personnel
- Favoriser l'usage des outils collaboratifs et de partage (lecteurs réseaux, ENT…)
- Définir les droits et devoirs de l'institution pour l'accès aux données de l'agent

▼ Assurer la continuité des missions

▼ Protection du personnel (accès à des données privées)

Politique de confiance numérique

Annexe 4 - Charte des personnels

Recommandations d'usage sécurisé de la messagerie

- Ne pas utiliser sa messagerie personnelle à usage professionnel
- Ne pas rediriger sa boite académique vers une boite personnelle

▼ Protéger la confidentialité des données

▼ Limiter les fuites de données et l'impact des usurpations de comptes

▼ Respect du RGPD (transfert de données hors UE)

Utilisation d'internet

Vérifier

- La localisation des données (RGPD)
- Le types de données traitées (personnelles, confidentielles, santé…)
- Le chiffrement des transferts de données (ex : HTTPS)

▼ Respect du droit européen

▼ Protection des données des personnels et des élèves

GT sécurité numérique

- GT inter-catégoriel : DAASEN, DSI, DANE, IPR/IEN 2D, IEN numérique 1D, Chefs d'EPLE
- Améliorer la maturité cyber de l'académie par la sensibilisation des publics
- Sensibiliser, former, éduquer, informer toute la communauté éducative
- Promouvoir la filière cyber et améliorer l'accès du public féminin
- Actions

Mise à disposition de ressources (portail SSI ARIANE)
https://ariane.ac-versailles.fr/pia/jcms/s1_8458810/fr/portail-de-la-securite-des-systemes-d-information-ssi

- Évènements : intervenants en établissement, webinaires, hackathons, jeux sérieux...

ACADÉMIE
DE VERSAILLES

Liberté
Égalité
Fraternité

3- ACTUALITÉ DE LA MENACE SSI

Typologies de cyber-attaques

Constat : les cyber-attaques sont de plus en plus fréquentes et de plus en plus ciblées.

Elles se matérialisent par les méthodes suivantes :

- **Hameçonnage (phishing)** : messages frauduleux invitant les utilisateurs à fournir leurs identifiants, réutilisés par la suite pour se connecter de manière usurpée aux services en ligne et en particulier la messagerie. Les attaquants imitent nos logos et nos sites (Iprof, messagerie, ARENA…) pour tromper les utilisateurs
- **Pièces jointes infectées** : envoi par messagerie de fichiers infectés dans le but
  - de prendre le contrôle du poste ou de serveurs
  - d'accéder aux données présentes sur le poste ou sur le réseau
  - Chiffrer les données (ransomware) et exiger une rançon pour en restituer l'accès
- **Attaques par déni de service** : des milliers de machines se connectent au SI afin de le surcharger et le rendre indisponible
- **Exploitations de failles de sécurité** non corrigées

Actualité de la menace

Fuites de données mises en ligne par des pirates sur le darkweb (août – sept. 2023)

- 13 000 identifiants de comptes SFR, avec email et mot de passe
- 63 500 identifiants de comptes Pandora, bijouterie, avec email et mot de passe
- 400 millions d’informations de comptes LinkedIn, avec prénom, nom, email, ID, ville, pays, numéro de téléphone, fonction, entreprise, url LinkedIn
- 137 millions d'informations de comptes Canva, outil de design en ligne, avec prénom, nom, pseudo, email et mot de passe hashé

ACADÉMIE
DE VERSAILLES

Liberté
Égalité
Fraternité

4- INCIDENTS DE SÉCURITÉ

Incidents de sécurité : définition et exemples

Un incident de sécurité est caractérisé lorsqu'est constatée une atteinte aux principes de la SSI (voir définition en diapo 5).

Quelques exemples :

- Vol d'identifiants et usurpation du compte
- Poste infecté par un virus ou un malware
- Ransomware
- Service indisponible (saturation ou perturbation)
- Perte de données
- Intrusion dans le système d'information
- Fuite de données confidentielles
- accès non autorisé à une ressource
- Menaces via un outil numérique

Déclarer un incident de sécurité

Les incidents de sécurité doivent être déclarés sur la plate-forme CARIINA

Ou écrire à

alerte-ssi@ac-versailles.fr

ACADÉMIE
DE VERSAILLES

Liberté
Égalité
Fraternité

5- HYGIÈNE NUMÉRIQUE

Bonnes pratiques générales

- Sauvegardez régulièrement vos données professionnelles
- Séparez vos usages personnels et professionnels
- Utilisez les services fournis ou recommandés par l'académie avant d'envisager de partager et de stocker vos documents professionnels sur un espace de stockage public (demande d'avis nécessaire auprès du RSSI)
- Utilisez des mots de passe complexes et changez-les régulièrement
- Maintenez vos systèmes à jour
- Limitez les échanges d'informations confidentielles ou sensibles lorsque vous êtes connectés à des réseaux non maitrisés (lieux publics, à l'étranger)
- Évitez l'utilisation de supports amovibles non maîtrisés (disques externes, clés USB), qui peuvent contenir des virus.
- En cas d'infection par un rançongiciel (ransomware), déconnectez immédiatement le poste de travail du réseau (Wifi ou filaire) puis contactez le service d'assistance

Bonnes pratiques d'utilisation de la messagerie

Séparez vos usages professionnels de vos usages personnels :

- utilisez la messagerie académique pour tous vos usages professionnels,
- ne transférez pas les messages professionnels vers une messagerie personnelle

Lorsque vous recevez des courriels, prenez les précautions suivantes avant de les ouvrir :

- l'identité d'un expéditeur n'est en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message,
- n'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts,
- si un lien ou plusieurs figurent dans un courriel, vérifiez l'adresse du site en passant votre souris sur chaque lien avant de cliquer. L'adresse complète du site s'affichera alors dans la barre d'état en bas de la page ouverte. Si vous avez un doute sur l'adresse affichée, abstenez-vous de cliquer,
- ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire),

ACADÉMIE
DE VERSAILLES

Liberté
Égalité
Fraternité

6- RESSOURCES

Ressources

- BD de sensibilisation
  - Spam, phishing : https://edu-html.ac-versailles.fr/phishing/
  - Travail à distance : https://edu-html.ac-versailles.fr/phishing2/
  - Confidentialité des mots de passe : https://edu-html.ac-versailles.fr/phishing3/
- Espace ARIANE SSI : https://ariane.ac-versailles.fr/pia/jcms/djv_79815/fr/securite-systeme-d-information
- Site du MENJS : https://www.education.gouv.fr/securite-des-systemes-d-information-6149

Comment se former et s'évaluer sur le thème de la cybersécurité ?

MOOC de l'ANSSI : https://secnumacademie.gouv.fr/

Parcours M@GISTERE Agir pour contribuer à ma sécurité numérique et à celle de mon organisation

Evaluation PIX : https://pix.fr/

- Site de la CNIL : https://www.cnil.fr/fr/10-conseils-pour-la-securite-de-votre-systeme-dinformation
- Guide d'hygiène de l'ANSSI : https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

Portail SSI

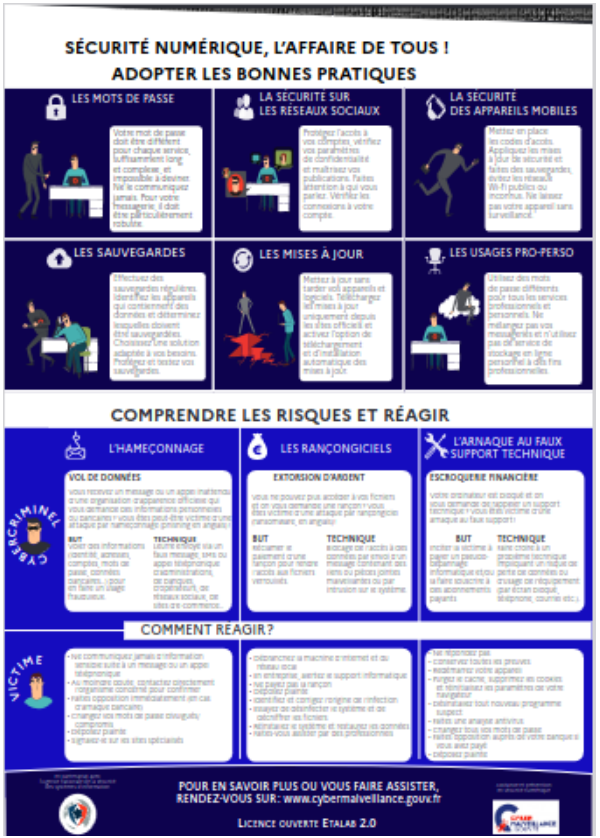

Portail de la Sécurité des systèmes d'information (SSI)
!! ALERTE EN COURS
Derniers messages destinés à hameçonner les utilisateurs.
En savoir plus
ACCÈS RAPIDE
ORGANISATION DE LA SSI
ÉTAT DE LA MENACE
DÉCLARER UN INCIDENT
POLITIQUE DE SÉCURITÉ
SENSIBILISATION FORMATION
Bienvenue sur l'espace ARIANE dédié à l'actualité de la cybersécurité dans notre académie.
L'accroissement exponentiel en cours des usages numériques en lien avec le travail à distance, le numérique éducatif et la dématérialisation de l'offre de services renforce l'exposition de l'institution aux attaques et décuple les dommages potentiels. La sécurité numérique est devenue un objectif stratégique central.
Longtemps considérée comme un frein aux usages, elle est désormais perçue par tous les acteurs comme une condition nécessaire à la pratique professionnelle, permettant d'assurer la confidentialité, l'intégrité, la disponibilité des données et plus largement celle des services numériques.
Notre objectif commun consiste à améliorer notre niveau de maturité sur les différents aspects de la cybersécurité.
La stratégie repose sur trois axes :
mise en place d'une gouvernance (instances académiques en charge de la cybersécurité, chaînes d'alerte),
sensibilisation des acteurs,
surveillance et protection du système d'information.
Vous trouverez sur cet espace une actualité sur les différentes actions mises en oeuvre dans l'académie, des documentations, des ressources de sensibilisation ainsi qu'un état de la menace cyber.
Les règles d'hygiène à retenir et à diffuser
SÉCURITÉ NUMÉRIQUE L'AFFAIRE DE TOUS !
Livret d'accompagnement
Affiche
ACTUALITÉS
MALLETTE CYBERSÉCURITÉ
NOUVEAUTÉ
Une mallette mise à disposition de tous les personnels pour une meilleure sensibilisation à la cybersécurité (actualités, informations et bonnes pratiques).
Télécharger la mallette
Télécharger la lettre d'accompagnement envoyée aux chefs d'établissement à l'occasion de la pré-rentrée.
ÉDUSCOL
Découvrez les nouvelles ressources pédagogiques dédiées à la cybersécurité du portail Eduscol sur notre page "Sensibilisation formation"
Ressources à disposition
Parcours cybercitoyen
CNIL
Les stealers
Recommandations en cas de menace d'attentat relayée par des outils numériques


2. Ressources
BANDES DESSINÉES DE SENSIBILISATION
JE RÉFLÉCHIS AVANT DE CLIQUER
Spam, phishing et virus
Travail à distance
Mot de passe
HYGIÈNE NUMÉRIQUE
Livret "Règles d'hygiène numérique"
Affiche "Bonnes pratiques et compréhension des risques"
MESSAGERIE
Sécuriser l'accès à votre messagerie académique
Modèle de transfert de courriel suspicieux
WEBINAIRES SÉCURITÉ
Webinaire services académique
RESSOURCES ÉLÈVES TER DEGRÉ
Parcours cybercitoyen 2021-2022
Descriptif parcours
Réalisations
Parcours cybercitoyen 2022-2023
Infographie parcours cybercitoyen 2023
Chartes
Support enseignants
Support élèves
Piratage de comptes ENT : les stealers

BD de sensibilisation

Hygiène numérique

- À intégrer dans chaque formation au numérique



QUESTIONS

ACADÉMIE
DE VERSAILLES

Liberté
Égalité
Fraternité

Merci à tous pour votre attention