



**ACADÉMIE
DE RENNES**

*Liberté
Égalité
Fraternité*

Direction des systèmes d'information et de l'innovation

LA SÉCURITÉ NUMÉRIQUE EN ÉTABLISSEMENT

Entrer dans la fonction de référent sécurité numérique en EPLE
session #1 – 6 décembre 2023

Les actualités de la presse

Cyberattaque de Betton : « Environ 2 % sur l'ensemble des données de la ville ont été exfiltrées »

A Betton, près de Rennes, une cyber attaque dans les ordinateurs de la mairie a permis à des malfaiteurs de faire main basse sur des données personnelles. La ville réagit et un expert donne ses conseils pour se protéger de potentiels hameçonnages.



**Alerte attentat à Cesson.
Un élève du lycée reconnaît
être l'auteur du message de
menaces**



**Pas de piratage de Parcoursup,
mais une intrusion visant les
usagers d'un lycée de l'académie
de Rennes**

C'est une campagne de type "stealer", ces logiciels espions spécialisés dans le vol des données, qui a visé les usagers d'un lycée de l'académie de Rennes et permis un accès frauduleux. Voici la conclusion des experts du ministère de l'enseignement

Ordre du jour

- La protection des données dans l'éducation
 - Le RGPD : définitions et principes
 - L'organisation académique
 - Les rôles et missions : DPD, Responsable de traitement, RSN
 - La mise en conformité d'un traitement de données à caractère personnel
- Cybersécurité
 - Phishing, usurpation de comptes
 - Focus : gestion des mots de passe
- Ressources et outils pour votre mission
- Ateliers de mise en situation :
 - Réagir suite à une usurpation de compte
 - Conseiller l'organisateur d'un voyage scolaire

RGPD : DÉFINITIONS ET PRINCIPES

Le règlement général à la protection des données

RGPD / GDPR : FAQ avec la CNIL

RÈGLEMENT
GÉNÉRAL SUR LA
PROTECTION DES
DONNÉES

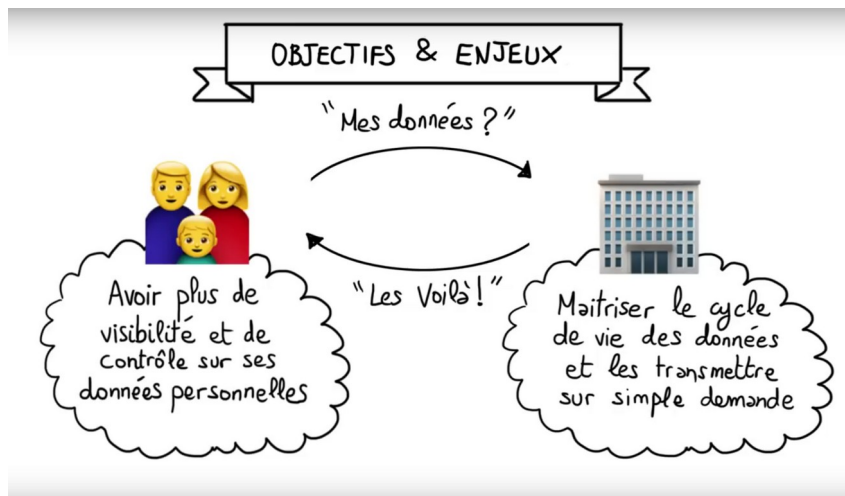


Texte de référence
européen en matière de
protection des données
personnelles pour les
résidents de l'U.E



25 MAI 2018

(ou **GDPR** pour:
General Data Protection Regulation)

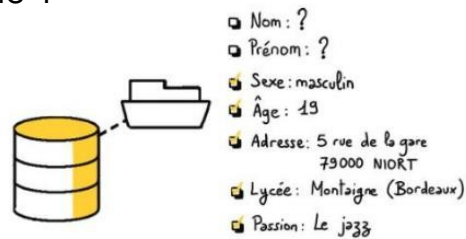


<https://www.cnil.fr/fr/reglement-europeen-protection-donnees>

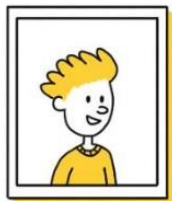
Une donnée à caractère personnel

Papier et numérique

Article 4



=



Marc PELLETIER

Toute information permettant de faire le lien **directement ou indirectement** avec une personne physique

Exemples :

- nom, prénom, date de naissance
- pseudonyme
- numéro de sécurité sociale (NIR)
- numéro de téléphone
- adresse IP
- cookies
- photographie, avatar, voix

Une donnée hautement sensible

Article 9



Données biométriques



Données génétiques



Orientations sexuelles

Les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.



Etat de santé



Origine raciale
ou ethnique



Infractions pénales
aux condamnations



Opinions politiques,
philosophiques,
religieuses

Droits des personnes renforcés

Articles 15 à 22 et 77 à 80



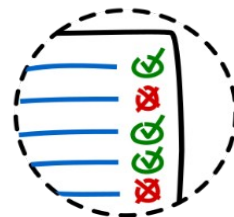
Accès



Rectification



Effacement



Limitation



Opposition



Portabilité



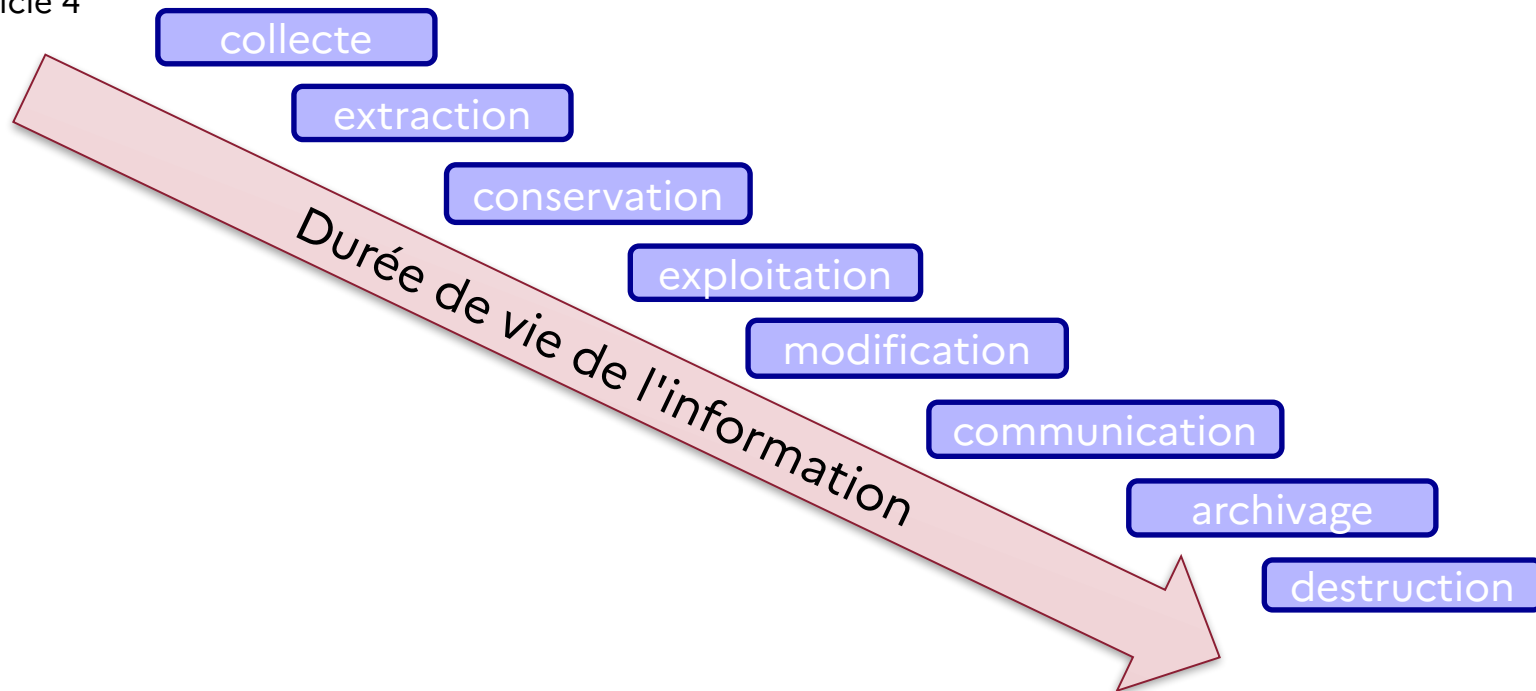
Réclamation



Actions

Traitement de données à caractère personnel

Article 4



Principes relatifs aux traitement de données à caractère personnel

Article 5



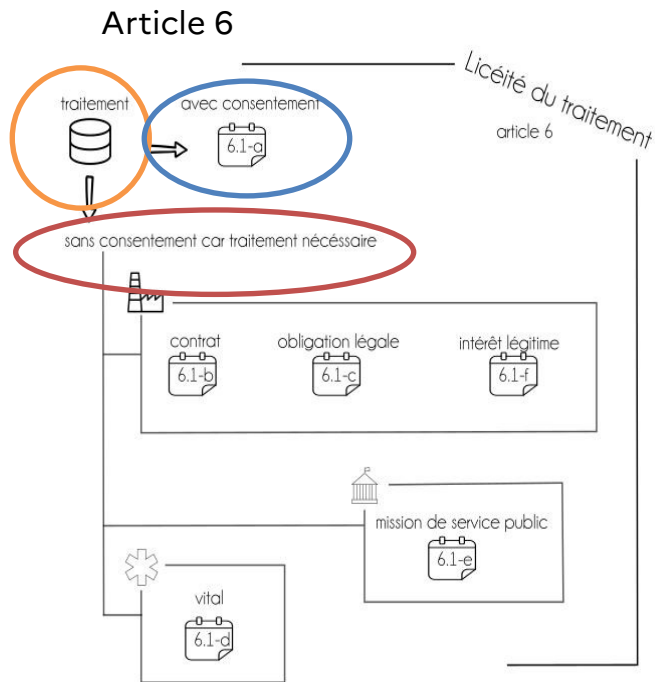
Licéité, loyauté, transparence

Minimisation, exactitude,
limitation de la conservation

Intégrité et confidentialité

Responsabilité

La licéité d'un traitement de données à caractère personnel



- ✓ **Le respect d'une obligation légale incombant au responsable du traitement** (ex : *traitements métiers*)
- ✓ La sauvegarde de la vie de la personne concernée
- ✓ **L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement**
- ✓ **L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci**
- ✓ La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée (ex : *informations internes*)
- ✓ **Consentement de la personne**

La licéité d'un traitement de données à caractère personnel

Le consentement : doit être libre, spécifique, éclairé et univoque



Nécessaire recueil de consentement positif

Formulaire

Mail d'acceptation, ...

Exemples « fichier des anciens élèves »,
« recueil date anniversaire personnel »....

! Pour les moins de 15 ans, ce sont les
représentants légaux qui consentent (art. 8)

→ Privilégier, dans la mesure du possible, et lorsque c'est pertinent,
la nécessité d'exercice d'une mission d'intérêt public

Le RGPD dans le domaine de l'éducation

10 principes clés pour protéger les données de vos élèves

De nombreux usages pédagogiques s'appuient aujourd'hui sur l'utilisation de données personnelles des élèves, c'est-à-dire sur des informations qui permettent de les identifier (nom, prénom, coordonnées, données biométriques, etc.). Le Règlement général sur la protection des données (RGPD) renforce les droits des personnes dans ce domaine. **Voici les réflexes à adopter pour enseigner avec le numérique tout en respectant le RGPD.**

BIEN CHOISIR SES OUTILS

<p>PRIVILÉGIER l'usage de logiciels libres ou développés par le ministère</p> <p>UTILISER de préférence des logiciels ou applications hébergés dans l'Union européenne</p> <p>INFORMER le chef d'établissement ou le directeur d'école de l'utilisation en classe d'une ressource collectant des données personnelles</p>	<p>1 </p> <p>2 </p> <p>3 </p> <p>4 </p> <p>5 </p>	<p>LIRE attentivement les informations disponibles sur les sites pour savoir si des données personnelles sont collectées, à quelles fins, et être vigilant à ce qu'aucune réutilisation commerciale ne soit envisagée</p> <p>VÉRIFIER que les parents et les élèves sont informés du traitement de leurs données personnelles et de la possibilité d'exercer leurs droits (d'accès, de rectification, etc.)</p>
--	---	---

PROTÉGER LES DONNÉES DES ÉLÈVES DANS TOUTE ACTIVITÉ PÉDAGOGIQUE

<p>LIMITER toute collecte de données personnelles aux informations indispensables au bon déroulement de l'activité puis veiller à ce qu'elles soient supprimées ou archivées selon la réglementation</p> <p>RESPECTER le droit à l'image des élèves</p> <p>SENSIBILISER les élèves aux enjeux de la protection des données personnelles</p>	<p>6 </p> <p>7 </p> <p>8 </p> <p>9 </p> <p>10 </p>	<p>CRÉER des pseudos lors des activités pédagogiques en ligne si l'utilisation de l'identité de l'élève n'est pas nécessaire</p> <p>S'ASSURER de la sécurité des données collectées notamment grâce à des mots de passe et à un antivirus</p>
--	--	---

Où s'informer ?

Pour prendre conseil auprès d'un délégué académique à la protection des données :

<https://education.gouv.fr/RGPD>



<https://www.education.gouv.fr/RGPD>

L'ORGANISATION ACADÉMIQUE

Périmètre de la sécurité numérique



Périmètre SSI

Le RSSI est garant de la sécurité de plusieurs domaines de SI de l'Éducation

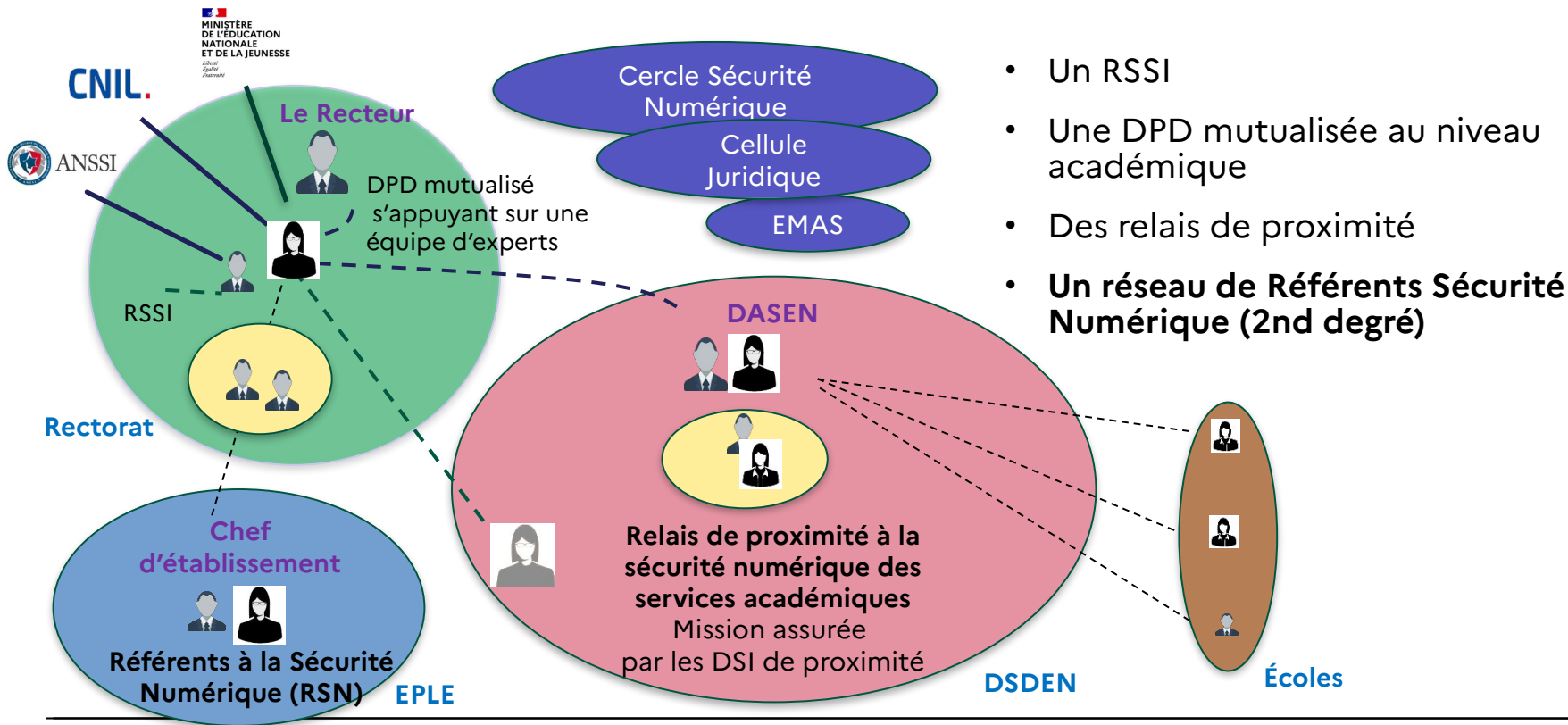
- Académie : Rectorat, DSDEN, EPLE, École
- National : Examens et concours & Forge

Périmètre Protection des données

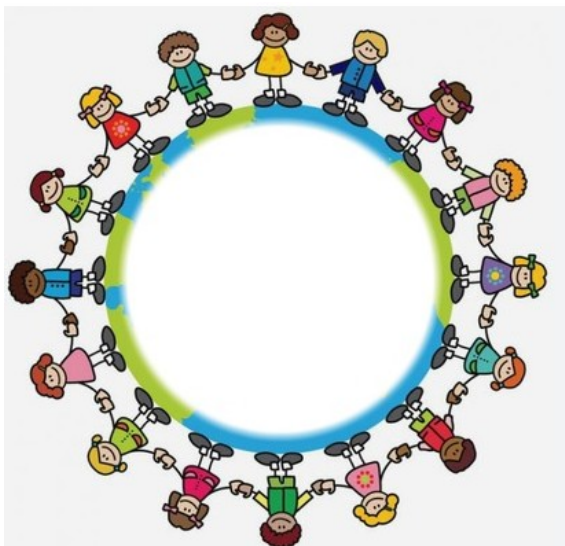
Le DPD conseille les responsables de traitement des organismes public de l'éducation

- Académie : Recteur, DASEN
- EPLE : Personnel de direction

L'organisation académique autour de la sécurité numérique



Le Cercle de Sécurité Numérique (CSN)



RSSI - Responsable Sécurité des Systèmes d'Information

DPD – Délégué à la protection des données

CAD - Cellule d'appui à la direction

Officiers SSI dans chaque pôle de la DSII

Pôle **Amigo** – Assistance Mutualisée Informatique Grand Ouest

Pôle **Applications et utilisateurs**

Pôle **DSI proximité**

Pôle **ENAE** – Equipement Numérique de l'Agent et de l'élève

Pôle **Fabrique numérique**

Pôle **Hébergement et Infrastructures**

RGPD : LES RÔLES ET MISSIONS

Le rôle du responsable de traitement

Le responsable de traitement doit :



- Être sensibilisé sur la protection des données et la SSI
- Avoir connaissance des traitements de données à caractère personnel dans son département
- Valider les traitements et tenir le registre des activités de traitements de l'établissement
- Informer la DPD et RSSI en cas d'incidents de sécurité

Article 4 : « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement »

Article 24 : « le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. »

Le rôle du délégué à la protection des données (DPD)

Les lignes directrices de sa lettre de mission :



- Donne un avis sans interdire
- Informe, accompagne, conseille les responsables de traitement
- Contrôle le respect du RGPD
- Travaille avec l'équipe DPD/DAJ du MENJS
- Correspond avec la CNIL
- Collabore avec EMAS

Article 37 : « Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.»

Article 39 : « Les missions du délégué à la protection des données sont au moins les suivantes : informer et conseiller le responsable de traitement ou le sous-traitant, [...] contrôler le respect du présent règlement, [...] dispenser des conseils, [...], coopérer avec l'autorité de contrôle »

Rôles et missions : DPD, Responsable de traitement

Quels rôles pour quels traitements ?

Responsable de traitement	Pour	Délégué à la protection des données
Ministre générale du MENJS	Traitements nationaux	DPD du MENJS
Recteur	Traitements académiques	DPD académique mutualisé
Chef d'établissement (EPLÉ)	Traitements locaux	DPD académique mutualisé
Directeur/trice des Services départementaux de l'Éducation nationale (DASEN)	Traitements propres aux écoles publiques	DPD académique mutualisé

Le rôle du Référent Sécurité Numérique

Les lignes directrices de sa lettre de mission :

- Informer et sensibiliser la communauté scolaire aux questions de sécurité numérique
- Assister et conseiller le chef d'établissement :
 - sur la protection des données et la SSI
 - sur la tenue du registre des activités de traitements
- Alerter le chef d'établissement et le DPD / RSSI en cas d'incidents



Conditions d'exercice de la mission



- Indemnité : 1/2 IMP
- Formations et rendez-vous réguliers (convocations EAFC)
- Appui sur le DPD, le CSN et la communauté des RSN

RGPD : MISE EN CONFORMITÉ

Mise en conformité : ce dont vous n'avez plus à vous occuper ;-)



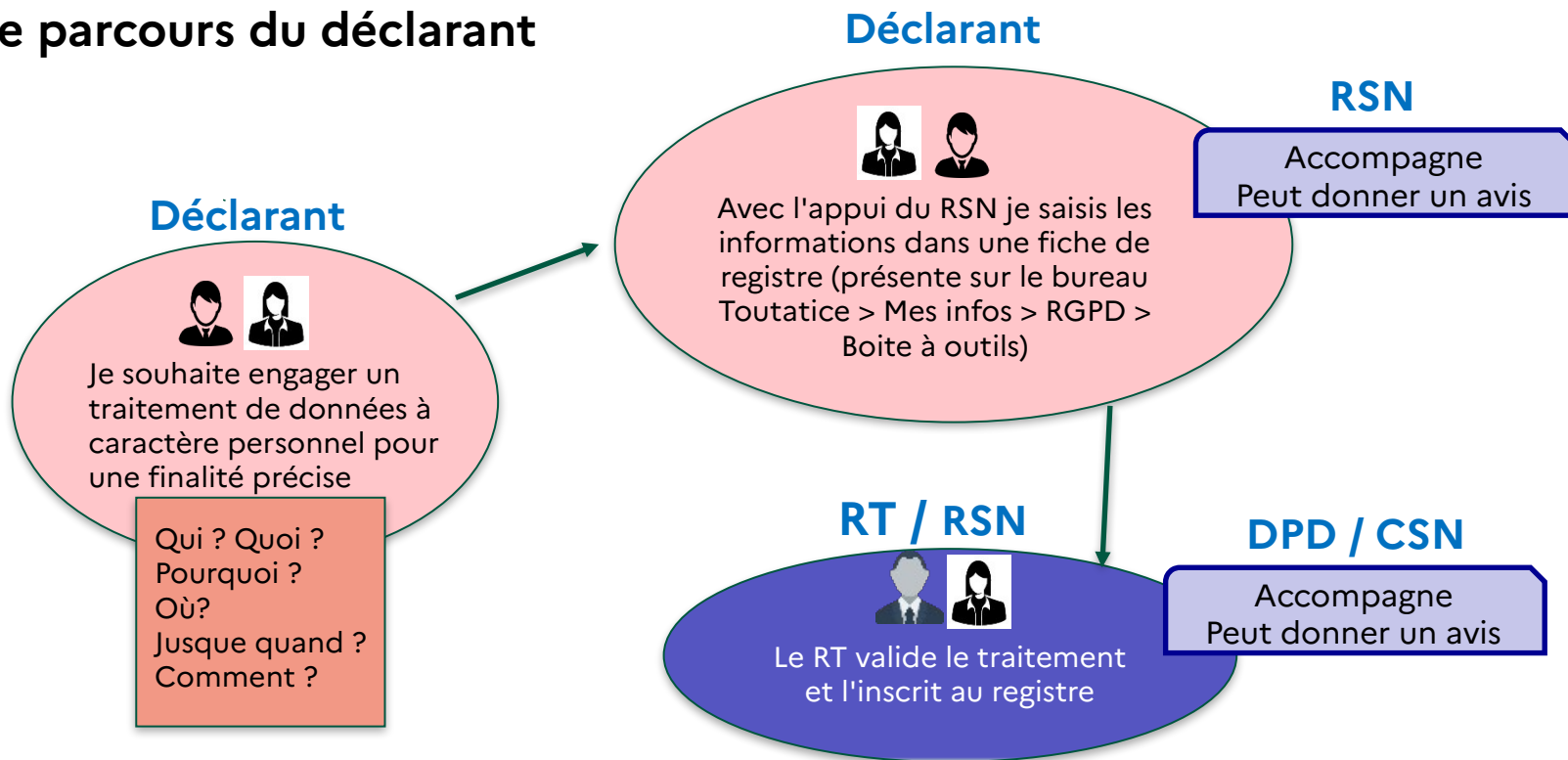
Pour les traitements de données sur le périmètre académique (ou national), le responsable de traitement est le recteur (resp. le ministre), et les démarches de mise en conformité sont déjà réalisées pour toutes les applications du cadre de confiance (pédagogie, gestion, communication, collaboration...)

Restent les traitements « locaux » à l'EPL...

Mise en conformité : évaluer et décrire un traitement de données "local"

- **Qui ?**
 - Responsable de Traitement
 - Services opérationnels
 - Sous-traitant
- **Quoi ?**
 - Catégories de données
 - Données sensibles
- **Pourquoi ?**
 - Finalité(s)
 - Base légale
- **Où ?**
 - Hébergement des données
 - Transfert possible hors UE
- **Jusqu'à quand ?**
 - Conservation données
- **Comment ?**
 - Mesures de sécurité

Le parcours du déclarant



Le registre des activités de traitement



Cybersécurité

La sécurité numérique, c'est protéger sa vie privée et celle des autres !

Alertes Politiques Communication Ressources F.A.Q. L'Équipe

SSI RGPD Chartes

Textes juridiques Cadres de référence

Boîte à outils

- Exemple de fiche de registre
- Registre de traitement
- Autorisation de captation de l'image d'un mineur
- Autorisation de captation de l'image d'un majeur
- Modèle des conditions générales d'utilisation (CGU) site-service
- Annexe au Règlement Général sur la Protection des Données pour le Cahier des Clauses Administratives Générales (CCAG)
- Modèle des mentions légales pour un site internet
- Modèle de convention sur la confidentialité en prise en main à distance
- Modèle de registre des violations de données à caractère personnel (DCP)

Fiche de registre

Description du traitement					
Nom / sigle					
N° / REF					
Date de création					
Mise à jour					
Responsable du traitement		Nom	Adresse	CP	Ville
Délégué à la protection des données					
Finalité(s) du traitement effectué					
Finalité principale					
Sous-finalité 1					
Mesures de sécurité					
Contrôle d'accès des utilisateurs					
Mesures de traçabilité					
Mesures de protection des logiciels					
Sauvegarde des données					
Chiffrement des données					
Contrôle des sous-traitants					
Autres mesures					
Hébergement qui protège les accès à PRONOTE.net.					
Lieu où les données sont hébergées					
Informations hébergées sur si externe					
Catégories de données personnelles concernées		Description	Durée de conservation		
Etat civil, identité, données d'identification, images					
Vie personnelle (habitudes de vie, situation familiale, etc.)					
Vie professionnelle (CV, situation professionnelle, scolarité, formation, diplômes, etc.)					
Informations d'ordre économique et financier (revenus, situation financière, situation)					
Données de connexion (adress IP, logs, etc.)					
Données de localisation (déplacements, données GPS, GSM, etc.)					
Données sensibles					
Données révélant l'origine raciale ou ethnique		Description	Durée de conservation		
Données révélant les opinions politiques					
Données révélant les convictions religieuses ou philosophiques					

Le registre des activités de traitement

Fiche de registre

Description du traitement
Nom / sigle : Le nom du service qui souhaite produire une enquête
N° / REF : Combien de fiche de déclaration ont été créées ?
Date de création : Date du début de recueil des données
Mise à jour : Dernière date de modification de la fiche

Responsable du traitement
Nom :
Adresse :
Services administratifs - Recteur
Etablissement du 2nd degré - Chef d'établissement
Etablissement du 1er degré - DASEN 1er degré
96 rue d'Artrain

Délégué à la protection des données DPD

Finalité(s) du traitement effectué
Finalité principale : Pourquoi les données sont collectées ?
Sous-finalité 1 : Est-ce que les données vont servir à autre chose après récolte ? (Facultatif)
Sous-finalité 2 : Les sous-finalités sont facultatives
Sous-finalité 3 :
Sous-finalité 4 :
Sous-finalité 5 :
Sous-finalité 6 :
Sous-finalité 7 :
Base légale : Mission de service public / Intérêt légitime / obligation légale / Consentement

Mesures de sécurité
Contrôle d'accès des utilisateurs : Ce sont les habilitations d'accès aux données collectées, qui a accès aux données de l'enquête et comment (moyens) ?

Mesures de traçabilité
Est-ce que des données de logs sont collectées ? Logs traçage, géolocalisation, ...

Mesures de protection des logiciels
Non concernés
Sauvegarde des données : Si elles sont sauvegardées, où sont-elles sauvegardées ? Combien de copies ?

Article 30 : « Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. »

Le registre des activités de traitement est obligatoire pour tous les organismes dès qu'on traite des données à caractère personnel (et donc dans chaque EPLE)

En cas de contrôle de la CNIL, c'est un des documents demandé :

<https://www.cnil.fr/fr/RGDP-le-registre-des-activites-d-e-traitement>

Participation au comité métier pour la mise à disposition d'un outil OURANOS : Outil de Registre Académique et National et de l'Organisation Scolaire (2025)

La durée de conservation

XXVI

B.O.
 N°24
 16 JUIN
 2005

FRI ET CONSERVATION
 DES ARCHIVES CONCERNANT
 L'ÉDUCATION NATIONALE

Type de documents	DUA	Sort final	Observations	Échelon concerné
2.4 Dispositifs particuliers de formation				
2.4.1 Scolarisation hors établissement (cours à domicile, par correspondance, ...) : déclarations des parents, listes, contrôles des IA.	10 ans	C		IA Communes Organismes de formation à distance
2.4.2 Formation continue				
2.4.2.1 Groupements d'établissements (GRETA)				
Conseils inter-établissements : comptes rendus de réunions	10 ans	C		GRETA
Réunions du bureau du GRETA	10 ans	C		GRETA
Bilans d'activité et documents préparatoires au budget	10 ans	C	Les GRETA n'ont pas de budgets propres. Leurs budgets sont intégrés dans ceux de l'EPL support.	GRETA
Dossiers par formation organisée : offres de prestation, conventions de formation, fiches financières, copies de factures, feuilles de présence des stagiaires, copies des attestations de stage délivrées, documents pédagogiques, ...	1 an après apurement des comptes	T	Il convient de conserver les copies des attestations de stage pendant 50 ans pour les formations concernant la sécurité ou les métiers à risques. Ces attestations peuvent n'être conservées que 10 ans s'il existe une liste récapitulative des stagiaires stage par stage. Conserver les années scolaires se terminant en 0 et 5.	GRETA
2.4.2.2 Services de formation continue de l'enseignement supérieur	5 ans	T	Conservation sélective de documents	Collectivités territoriales FFC

Déterminer une durée de conservation :

- Obligation légale
Ex : Conservation du dossier administratif d'un fonctionnaire jusqu'aux 80 ans de la personne
- Selon les données / le contexte
Ex : fiche de rentrée

CYBERSÉCURITÉ PHISHING, USURPATION

Compromission de comptes / Phishing



- Statistiques mensuelles (échantillon du 10 avril au 11 mai)
 - Adresses IP bloquées : 974 351
 - Trafic Total : 3.7 millions de mails reçus et 895 000 mails envoyés
 - Emails légitimes : 2.1 millions reçus 868 000 envoyés
- Environ 500 comptes compromis par an
 - Servent essentiellement à spammer vers l'extérieur (notamment vers les autres académies, les particuliers...)
- Signalements à l'adresse spam@ac-rennes.fr
 - Analyse et adaptation des règles d'antispam
 - Blocage des URLs incriminées dans les EPLE et services académiques
 - Faux positifs

Agissons pour limiter les risques de vol de compte



#1 LES CLÉS POUR UN MOT DE PASSE ROBUSTE

Année 2022-2023

Pourquoi dois-je avoir un mot de passe robuste ou fort ?

Objectif : vous protéger d'un piratage de votre mot de passe académique et d'une usurpation de votre identité.

La robustesse d'un mot de passe dépend :

- de la longueur du mot de passe
- de sa complexité, c'est-à-dire du nombre de symboles différents utilisés
- du caractère aléatoire du mot de passe
- de l'unicité du mot de passe (il doit être unique pour chaque site ou service web)



Quels sont les critères d'un mot de passe robuste ?

La création de votre mot de passe académique doit répondre à plusieurs critères :

- Il doit comporter au minimum douze caractères
- Il ne doit contenir aucun nom d'utilisateur, nom, prénom ou date de naissance
- Il ne faut utiliser aucune suite de lettres ou nombres séquentiels (azerty, 123456, abcd)
- Il est fortement recommandé qu'il combine des lettres minuscules, majuscules, des chiffres, des caractères spéciaux (?;./!\$%&) et/ou des lettres accentuées



Une méthode pour créer mon mot de passe : la "phrase de passe"

Une phrase de passe est une association de mots simples respectant les critères d'un mot de passe robuste :

ex : J'ai mangé 4 pommes peut devenir J'aiMangé4pom



Vous pouvez avoir recours à des techniques d'association avec des éléments visuels :

ex : mer, palmier, été et soleil peut devenir Mer-Palmier&ISoleil-été

Un outil pour créer et stocker mes mots de passe : le coffre-fort de mot de passe

Un coffre-fort de mot de passe permet de :

- générer des mots de passe aléatoires
- stocker des mots de passe de manière sécurisée
- synchroniser ces derniers sur plusieurs appareils



Rendez-vous sur www.toutatice.fr et cliquez sur [MyToutatice.cloud](https://mytoutatice.cloud) pour créer votre espace et utiliser l'application "Pass".

- choisir un mot de passe robuste
- 1 compte administrateur = 1 personne
- les utiliser exclusivement sur des équipements professionnels
- les enregistrer dans un coffre-fort de mot de passe

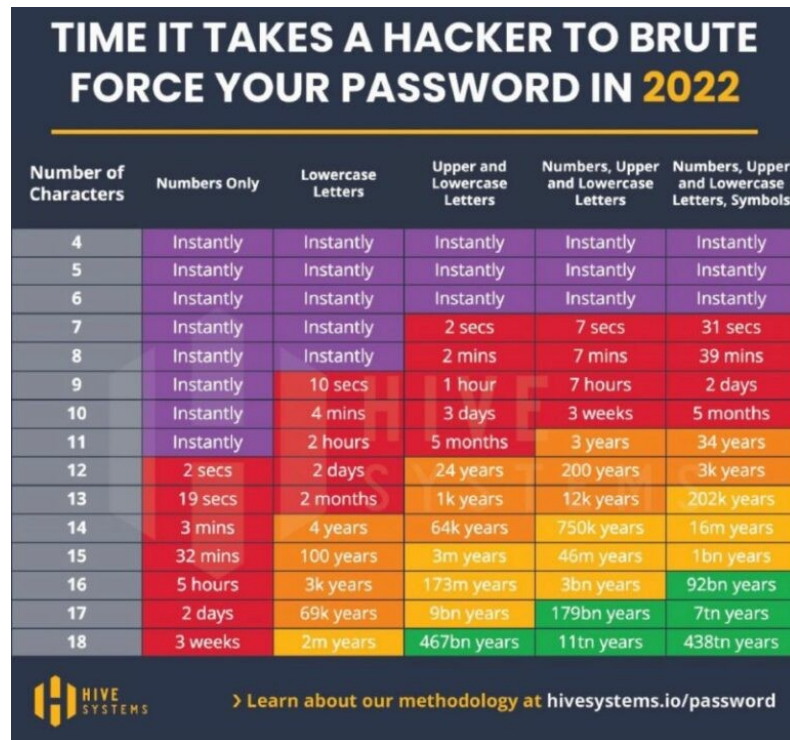
Focus : comment choisir un ~~mot~~ de une phrase de passe robuste et facile à retenir

Testons-nous

Que pensez-vous de ces exemples de mots de passe ?
Sécurisés ou pas ? Faciles à deviner, à retenir ?

- MyP4\$\$w0rd!
- Thierry56
- J0ffr€do*1972
- K?5oU2
- C'estPasSiComplicé:-)
- 250x4=1000
- 65yrreihT
- 99887766554433221100

Testons-nous



Les 25 mots de passe les plus communs en France (projet Richelieu)

Rang	2019
1	123456
2	123456789
3	azerty
4	1234561
5	qwerty
6	marseille
7	000000
8	1234567891
9	doudou
10	12345
11	loulou
12	123

13	password
14	azertyuiop
15	12345678
16	soleil
17	chouchou
18	1234
19	1234567
20	123123
21	123451
22	bonjour
23	111111
24	nicolas
25	jetaime

Mon mot de passe a-t-il déjà fuité ?



We found
thierry.joffredo@ac-rennes.fr
exposed in **3** data breaches.

Connectez-vous pour obtenir des étapes claires sur la façon de résoudre ces fuites de données, afficher toutes les fuites de données et surveiller en permanence toute nouvelle fuite de données connue.

Connectez-vous pour résoudre les fuites de données



V Verifications.io

Fuite de données ajoutée :
9 mars 2019

Données ayant fuité :
**Dates of birth, Email addresses,
Employers, Genders, Geographic
locations, IP addresses, Job titles,
Names, Phone numbers et
Physical addresses**

E Edmodo

Fuite de données ajoutée :
1 juin 2017

Données ayant fuité :
**Email addresses, Passwords et
Usernames**

A Adobe

Fuite de données ajoutée :
4 décembre 2013

Données ayant fuité :
**Email addresses, Password hints,
Passwords et Usernames**

Comment faire ?

- La robustesse d'un mot de passe dépend essentiellement :
 - de sa **longueur**
 - et de sa **complexité**
- Il doit comporter au minimum :
 - **12 caractères** comprenant des **majuscules, des minuscules, des chiffres et des caractères spéciaux**,
 - ou **14 caractères** comprenant des **majuscules, des minuscules et des chiffres**, sans caractère spécial obligatoire.
- Il ne doit comporter **aucune information « devinable »** (prénom, date de naissance, nom de ville, suite séquentielle de lettres ou de chiffre...)

Comment faire ?

- Association (plus ou moins aléatoire) de mots :
 - **voilà_Paris_17_hirondelles** (à vous d'imaginer une histoire ou une représentation mentale pour le retenir)
- Choisir une **phrase de passe** :
 - *J'ai mangé quatre pommes, je suis content* → **J'aiMangé4Pommes:-)**
 - En ne gardant que les premières lettres, et en remplaçant des petits mots par des chiffres ou des symboles (de=2, si=6, un(e)=1, et=&...)
La vie, c'est comme une boîte de chocolats ! On ne sait jamais sur quoi on va tomber. →
Lv,cec1b2c!Onsjsqovt.


Mais surtout...


utiliser un coffre-fort de mots de passe qui inclue un générateur de mots de passe aléatoires !

MyToutatice, mon Espace Numérique Personnel (ENP)


Drive 
Stocker et partager les fichiers de l'utilisateur


Bureautique en ligne 
Créer, partager et modifier des documents bureautiques en ligne

Notes collaboratives 
Créer et partager facilement des notes collaboratives et légères

Photos 
Stocker et partager les photos de l'utilisateur et créer des albums

 **MyToutatice.cloud**
votre Cozy respectueux de vos données personnelles

Carnet de mots de passe 
Gérer, Stocker et synchroniser vos mots de passe

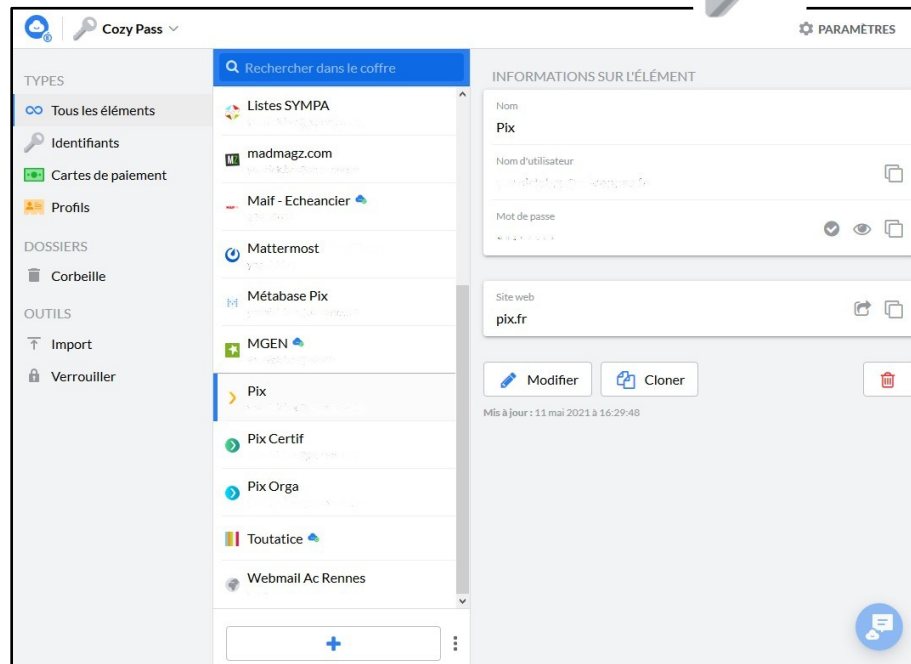
Contacts 
Regrouper l'ensemble des contacts de l'utilisateur

Qu'est-ce qu'un carnet numérique de mots de passe ?



- Un espace sécurisé permettant de **gérer** et **stocker** des mots de passe
- Un espace permettant de **générer** des mots de passe forts, sécurisés et aléatoires en fonction de paramètres (nombre de caractère, minuscule, majuscule, caractères spéciaux, ...)
- **Partager** ses mots de passe sur plusieurs appareils (fixes ou mobiles)

Vous disposez d'un carnet numérique de mots de passe dans votre cloud personnel MyToutatice :



MyToutatic / Cozy Pass

Comment ajouter un identifiant dans mon carnet ?

L'application « Pass » est présente sur la page d'accueil de l'espace **MyToutatic**



Pour ajouter un nouvel identifiant dans son coffre-fort, il suffit de cliquer sur le « + »




Le bouton  permet d'accéder au **générateur de mot de passe**



AJOUTER UN ÉLÉMENT


Type
Identifiants

Nom
Mon exemple

Nom d'utilisateur
prenom.nom@jac-rennes.fr


Mot de passe
.....   

URI 1
 https://www.exemple.fr 


 [Nouvel URI](#)

DESCRIPTION

CHAMPS PERSONNALISÉS

 [Nouveau champ personnalisé](#)

Texte

 Annuler

MyToutatice / Cozy Pass

Une extension à installer sur son navigateur, une application à utiliser en mobilité

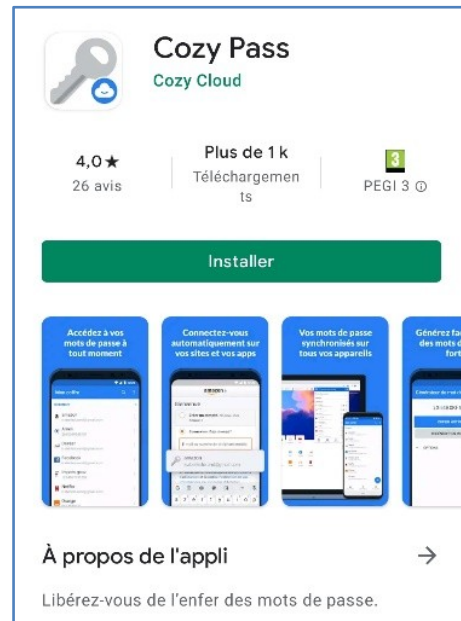
Pour faciliter l'usage du carnet (auto-complétion, synchronisation sur mobile)

Plutôt réservé à un usage privé ou personnel.

À éviter sur les postes partagés.



Ajout de l'extension dans Firefox



Installation d'une application mobile

RESSOURCES ET OUTILS POUR VOTRE MISSION

Le site de cybersécurité

ACADÉMIE DE RENNES
Cybersécurité
La sécurité numérique, c'est protéger sa vie privée et celle des autres !

Alertes Politiques Communication Ressources F.A.Q. L'Équipe

Fermeture des accès Pronote depuis l'étranger suite au vol d'un mot de passe administrateur (SPR)

BIENVENUE SUR L'ESPACE CYBERSÉCURITÉ

L'espace Cybersécurité de l'Académie de Rennes regroupe les bonnes pratiques sur la Sécurité des Systèmes d'Information (SSI) et les informations liées au Règlement Général à la Protection des Données (RGPD).

Cet espace, proposé par la Direction des Services de l'Information et de l'Innovation (DSII), vous informera des actualités et des alertes concernant le domaine de la Sécurité Numérique.

Actualités

- 22-23 | FLASH INFOS N°140 : Fermeture des accès Pronote depuis l'étranger
- 22-23 | FLASH INFOS N°139 : Ouverture du site Cybersécurité
- NIR ou "numéro INSEE" : nouveau décret pour son usage
Le décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire est paru : <https://www.legifrance.gouv.fr/affichTexte.do?cidText...>
- 22-23 | FLASH INFOS N°126 : Sites web écoles-établissements indisponibles

Mentions légales - Cybersécurité 2023 - Dernière mise à jour du site : il y a 22 heures

- **Accessible** depuis le bureau Toutaticice > Mes infos > Cybersécurité
<https://cybersecurite.toutaticice.fr>
- **Alertes** : Alerte SSI, chaînes d'alertes
- **Politiques – cadres de référence** au regard des enjeux de sécurité et de souveraineté : visio-conférence, services en ligne, filtrage web, ...
- **Communication** : Newsletter, Flashes infos
- **Ressources** : Services pour collaborer, sites utiles ...

La Newsletter mensuelle

#4 LES VIRUS « STEALER »

LA SÉCURITÉ NUMÉRIQUE, C'EST PROTÉGER SA VIE PRIVÉE ET CELLE DES AUTRES ! DSII

Des comptes élèves, dont les identifiants ont été volés, ont été utilisés pour envoyer des messages de menace terroriste, notamment sur promoteo. Des virus « Stealer » implantés dans des logiciels malveillants ont été retrouvés sur leurs ordinateurs personnels.

1 Quel rôle jouent-ils ?
Les virus informatiques de type « Stealer » (« dérobeurs » en français) sont spécialisés dans le vol d'identifiants (note de passe, ...) et autres données stockées, notamment dans les navigateurs web (Firefox, Edge, Safari, ...)

Comment se propagent-ils ?
Le virus peut être introduit intentionnellement par des personnes malveillantes dans des logiciels contractés ou via des liens frauduleux postés sur différentes plateformes grand public comme les réseaux sociaux.

01 L'utilisateur clique sur un lien internet trompeur, télécharge un logiciel et installe un programme contenant le virus.

02 Le virus récupère les mots de passe présents dans les navigateurs web du poste utilisé. Le pirate est en possession de ces identifiants et peut usurper vos différents comptes.

Comment éviter ce type d'attaque ?

- Téléchargez des logiciels ou des programmes à partir du site officiel de l'éditeur.
- Ne désactivez jamais votre antivirus à la demande d'un logiciel.
- N'ouvrez pas les pièces jointes et ne cliquez pas sur les liens d'un e-mail suspect (mattand, a1erastie, aguicheur, ...).
- Utilisez des mots de passe forts, impersonnels et différents pour chaque accès.
- Ne stockez pas vos mots de passe de manière non sécurisée : notes sur papier, fichiers textes, notes sur votre smartphone.
- Utilisez le gestionnaire de mots de passe Cozy Pass pour stocker vos mots de passe.

Une question ? Contactez la plateforme d'assistance AMIGO
<https://assistance.ac-rennes.fr>

LA SÉCURITÉ NUMÉRIQUE, C'EST PROTÉGER SA VIE PRIVÉE ET CELLE DES AUTRES ! DSII

#3 Réagir face à l'usurpation d'identité

2022-2023

1 Qu'est-ce qu'une usurpation d'identité numérique et comment la reconnaître ?
Un tiers utilise vos données personnelles à votre insu. Il peut s'agir :

Nom, Prénom NUMEN	Photo d'identité	Adresse de messagerie	Date de naissance	Identifiant et mot de passe
Utiliser votre identifiant et mot de passe pour accéder à des données sensibles	Mes collègues m'indiquent qu'ils reçoivent des messages douteux envoyés depuis mon compte.	Je n'ai plus accès à la rubrique "Messagerie" sur Convergence.	Je constate l'utilisation de mes données personnelles sur internet sans mon accord.	

2 Que faire si vous êtes victime d'une usurpation d'identité numérique ?

- Modifiez votre mot de passe académique depuis Toutatice
- Prévenez la DSII à l'adresse dédiée : alerte.ssi@ac-rennes.fr
- Avertissez vos collègues et vos contacts
- Rendez-vous sur Cybermveillance.gouv.fr pour effectuer un dialogue en ligne

3 Comment se prémunir contre l'usurpation d'identité numérique ?

- Méliez vous des courriels invitant à saisir des données ou à cliquer sur un lien non reconnu
- Assurez vous, lorsque vous saisissez des informations confidentielles, que les données du site sont chiffrées (Mention HTTPS dans l'adresse)

Utilisez des mots de passe robustes et différents pour chaque compte

Azerly2023 ❌
aLSiBvill4nt ✔️

Ne laissez pas vos mots de passe à la vue de tout le monde

Amigo

Une question ? Contactez la plateforme <https://assistance.ac-rennes.fr>

LA SÉCURITÉ NUMÉRIQUE, C'EST PROTÉGER SA VIE PRIVÉE ET CELLE DES AUTRES !

#5 Le coffre-fort de mots de passe : Cozy Pass

Chaque compte doit disposer d'un mot de passe différent. Mais comment retenir tous ces mots de passe ?

C'est inutile, grâce à Cozy Pass !

Cozy Pass est un coffre-fort qui stocke de manière sécurisée tous vos mots de passe. Grâce à cet outil, vous n'avez à retenir qu'un seul mot de passe : celui de votre coffre-fort ! Lui s'occupe de retenir le reste...

Comment ça fonctionne ?

Grâce à cet outil, je simplifie la gestion de mes mots de passe au quotidien ! Me permet de :

- Ne retenir qu'un mot de passe unique
- Stockier et sécuriser mes mots de passe
- Synchroniser mes mots de passe sur plusieurs appareils
- Gérer mes mots de passe sécurisés pour les différents services numériques professionnels

Accès aux identifiants et mots de passe enregistrés

Pour obtenir des informations et accéder à ces services, scannez le QR code ou rendez vous sur le lien : <https://www.toutatice.fr/portal/share/L7858X>

Pour plus d'informations, contactez la plateforme d'assistance <https://assistance.ac-rennes.fr>

Amigo

Le cadre de référence des services en ligne

Classification des services en ligne

Le tableau suivant permet de présenter les services numériques académiques en regard des services numériques grand public.

<p>Service disponible dans le cadre de confiance ENT + GAR</p> <p>Service accessible depuis Toutatice ne nécessitant pas d'inscription au registre des activités de traitement ou de conventionnement avec l'éditeur</p>
<p>Service de confiance autorisé sous conditions</p> <p>Service autorisé sous les conditions mentionnées en bas de tableau</p>
<p>Service hors cadre de confiance</p> <p>Service ne respectant pas les principes de souveraineté, à savoir l'hébergement des données personnelles sur le territoire européen par une société soumise au droit européen.</p>

	Collaboration		
Partages et espaces collaboratifs	<p>toutatice.fr MyToutatice</p> <p>Triskell Tribu</p>	X	<p>Edmodo Google Drive</p> <p>Dropbox OneDrive</p>
Bureautique en ligne	<p>toutatice.fr Toutapad</p> <p>Triskell MyToutatice</p>	<p>DigiDocs (3) CryptPad (1)</p> <p>Framapad, Framacalc (1)</p>	<p>Office365</p> <p>Google Workspace</p>
Espace numérique de classe	<p>toutatice.fr Moodle Modulo</p>	<p>Beneylu School (3)</p> <p>One 1D (3)</p>	
Communication élèves / famille 2D	<p>Pronote</p> <p>(hébergé par l'Académie)</p>	<p>Pronote (3)</p> <p>(hébergé chez IndexEducation)</p> <p>Educhorus (3)</p> <p>La-vie-scolaire (3)</p> <p>Eoole directe (3)</p>	<p>Class Dojo</p>
	Communication		
Communication élèves / famille 1D	<p>ENT conventionnés :</p> <p>Espace école Modulo</p> <p>One 1D Beneylu School</p>	<p>Offres gratuites :</p> <p>One 1D (3) Klassly (3)</p> <p>Beneylu School (3)</p> <p>Educartable (3)</p> <p>TouteMonAnnee.com (3)</p>	X

Classification des services en ligne

- Services disponibles dans le cadre de confiance ENT + GAR
- Les services de confiance autorisés sous conditions
- Les services hors cadre de confiance

Le Responsable de traitement s'engage dans les deux derniers cas, avec l'éclairage du DPD

Besoins non listés => demande par la plateforme d'assistance **AMIGO**

Le cadre de référence du filtrage web

Catégorie	Collégiens	Lycéens	Etudiants & Personnels	Description
gambling	Bloquée	Bloquée		Sites de jeux en ligne, casino...
games	Bloquée	Bloquée		Sites de jeux (en ligne ou de téléchargement)
lingerie	Bloquée	Bloquée		Sites de lingerie
remote-control	Bloquée	Bloquée		Sites de prise de contrôle à distance
reaffected	Bloquée	Bloquée		Sites ayant changé de propriétaire et contenu
audio-video	Bloquée sauf : les médias publics youtube.com dailymotion.com vimeo.com lumni.fr litteratureaudio.com			Sites orientés vers l'audio et la vidéo
social_networks	Bloquée sauf : twitter.com			Sites de réseaux sociaux
shopping	Bloquée			Sites de vente et achat en ligne

Les listes de l'Université de Toulouse

- **La liste « games »**
Liste **bloquée** pour les collégiens et les lycéens
Par défaut, liste **autorisée** pour les étudiants et les personnels
- **La liste « audio-vidéo »**
Liste **bloquée** pour les collégiens et les lycéens exceptés certains sites listés dans le tableau
Liste **autorisée** pour les étudiants et les personnels

Les listes académiques

- blacklist-CLG-LYC-PERS : liste des URL **interdites** à tout le monde
- blacklist-CLG-LYC: liste des URL **interdites** aux collégiens et lycéens, **autorisées** aux personnels
- blacklist-CLG: liste des URL **interdites** aux collégiens, **autorisées** et lycéens et aux personnels
- whitelist-PERS-LYC-CLG : liste des URL **autorisées** à tout le monde
- whitelist-PERS-LYC : liste des URL **autorisées** uniquement aux lycéens et aux personnels
- whitelist-PERS: liste des URL **autorisées** uniquement aux personnels

Les quarts d'heure DSII / sécurité numérique

- Conseils pour élaborer un bon mot de passe
- Sécurisation de la messagerie académique
- Paramétrer son navigateur pour protéger sa vie privée
- Utiliser ses mots de passe dans un carnet de mots de passe numérique

À venir :

- Reconnaître un mail frauduleux (phishing)
- ... et bien d'autres (à vos idées!)

Le quart d'heure DSII

Des présentations courtes et régulières en visio afin de partager des solutions pour améliorer ou faciliter votre travail au quotidien

Rendez-vous en ligne les **vendredis à 13h40** sur Visio-agentes en suivant ce lien : Visio
Au programme de novembre et décembre 2023 :

- vendredi 24 novembre : Tout savoir sur le compte académique de l'agent.
- vendredi 1er décembre : Les bonnes pratiques de messagerie.
- vendredi 8 décembre : Comment reconnaître un mail frauduleux (phishing) ?
- vendredi 15 décembre : Comment créer et aménager un espace collaboratif Triskell ?

Accès libre et sans inscription



Offre de services numériques de l'éducation



Offre de services numériques de l'éducation

A propos Mes services numériques ▲ Météo du numérique Ressources ▼ Flash Info

Les accès

- Mon compte académique
- L'ENT Toutatice
- Le portail ARENA
- ÉduConnect

Mon équipement informatique

- Les clés OTP
- Le VPN
- L'ordinateur et ses périphériques
- Restauration de documents

Mes applications

- Scolarité du 2nd degré
- Scolarité du 1er degré
- Gestion des personnels
- Démarches et enquêtes
- Organisation de l'établissement
- Evaluations nationales

Mes outils de collaboration

- Communication
- Partage
- Collaboration et visio

Cybersécurité ↗

Pour connaître et faire connaître l'offre institutionnelle !

Autres ressources



<https://www.cnil.fr/fr/thematique/services-publics/education>

<https://www.cnil.fr/fr/education-numerique-decouvrez-les-conseils-et-ressources-de-la-cnil>



<https://www.cybermalveillance.gouv.fr/>



<https://eduscol.education.fr/3679/education-et-cybersecurite>

ATELIERS DE MISE EN SITUATION

Situation n°1 : Réagir suite à une usurpation d'identité dans l'établissement

Suite à la fuite du mot de passe de son compte académique, un(e) de vos collègues a été victime d'une usurpation d'identité : des mails de phishing ont été envoyés à partir de son adresse, des notes ou des appréciations ont été modifiées dans Pronote, un message injurieux a été envoyé en leur nom à plusieurs personnes dans l'établissement via la messagerie interne, etc.

Que menez-vous comme actions en tant que RSN ?

Comment pouvez-vous accompagner l'ensemble de vos collègues sur une action de sensibilisation ?

Quels ressources et outils pouvez-vous leur proposer ?

Situation n°1 : Réagir suite à une usurpation d'identité dans l'établissement

Tout incident de sécurité pouvant conduire à une fuite ou une utilisation malveillante de données doit être signalé au chef d'établissement, au RSSI et au délégué à la protection des données dans les meilleurs délais. Les mesures à prendre seront décidées en commun, selon la gravité de l'incident, la nature des données, etc.

Le ou la collègue doit le plus rapidement possible reprendre le contrôle de son compte académique et, avec l'aide de la plateforme AMIGO, choisir un nouveau mot de passe répondant aux critères actuels de sécurité.

Vous pouvez, en tant que RSN, agir en amont de ces incidents en menant des actions de sensibilisation auprès de vos collègues ou des élèves de l'établissement :

- Animer une séance de sensibilisation d'une demi-heure sur le thème « comment choisir un bon mot de passe ou une bonne phrase de passe » (en appui : newsletter, quart d'heure DSII...)
- Monter un atelier à destination des collègues pour leur apprendre à utiliser un carnet numérique de mots de passe (MyToutatice / CozyPass)
- Concevoir, avec les élèves, des affiches rappelant les principes de confection d'une phrase de passe robuste et facile à retenir / saisir
- Proposer une campagne Pix autour de la sécurité numérique (avec le RRUPN / l'administrateur Pix de l'établissement)

Situation n°2 : conseiller les organisateurs d'un voyage scolaire

M. LORRAND organise un voyage scolaire en Espagne, pour mai 2024. Il part avec 2 classes de 4ème et pour l'organisation de ce voyage (saisie, collecte des informations, échanges une fois sur place, publication des photos pour les familles) il souhaite utiliser plusieurs services numériques.

- Pour collecter et stocker toutes les informations (liste d'élèves, allergies, médicaments, horaires, contacts...), il pense à Google Drive : c'est pratique, il a un compte Google, et peut partager un dossier avec ses collègues.
- Pour échanger avec l'équipe pédagogique ou entre encadrants, une fois sur place, Whatsapp permettra de communiquer simplement et efficacement
- Pour publier les photos du voyage, et entretenir le lien avec les parents d'élèves, il pense à ouvrir un blog sur wordpress.com et/ou utiliser le compte Instagram de l'établissement (« c'est bon, tout le monde à un compte Instagram aujourd'hui »).

Quels sont les points de vigilance et d'attention ? Que pouvez-vous lui conseiller ?

Situation n°2 : conseiller les organisateurs d'un voyage scolaire

Le voyage doit être déclaré sur Toutatice, dans l'application « Sorties scolaires ».

La collecte et le traitement (partage) de données personnelles en amont du voyage scolaire peuvent être réalisés dans un Triskell/MyToutatice, avec un accès limité aux personnes organisant le voyage.

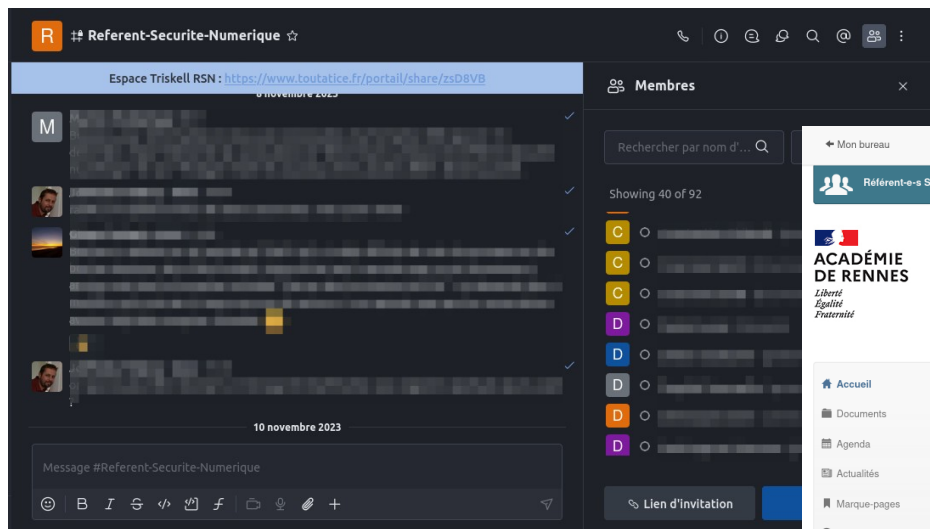
Le dossier / l'espace et les données qu'il contient pourront être supprimés à l'issue du voyage.

Les différentes informations doivent être collectées et traitées de manière organisée et conforme :

- Les données des élèves et des parents (noms, prénoms, numéros de téléphone, adresses...) peuvent être collectées depuis SIECLE Base Elèves avec le secrétariat ;
- Les données de santé (allergies, médicament) sont des données sensibles qui doivent être collectées le temps du voyage, doivent être conservées sur un support sécurisé, avec le consentement des personnes, et être supprimées ensuite.
- Le stockage des horaires, contacts, transporteurs sont déjà collectés dans l'application « Sorties scolaires »
- Les échanges entre encadrants doivent passer par une messagerie instantanée institutionnelle (Le Chat)
- Le lien avec les familles peut être maintenu au travers du site internet (SPIP) de l'établissement, à condition d'avoir le consentement explicite et libre des élèves ou de leurs représentants légaux pour publier des photos, des vidéos, de la voix... sur une durée limitée. Il est sans doute possible d'utiliser un réseau social, mais il faut penser aux parents qui n'ont pas accès à ce réseau social : « forcer » le consentement imposé par le fournisseur du compte en demandant l'inscription n'est pas autorisé.

ET MAINTENANT ?

Des espaces numériques pour la communauté des RSN



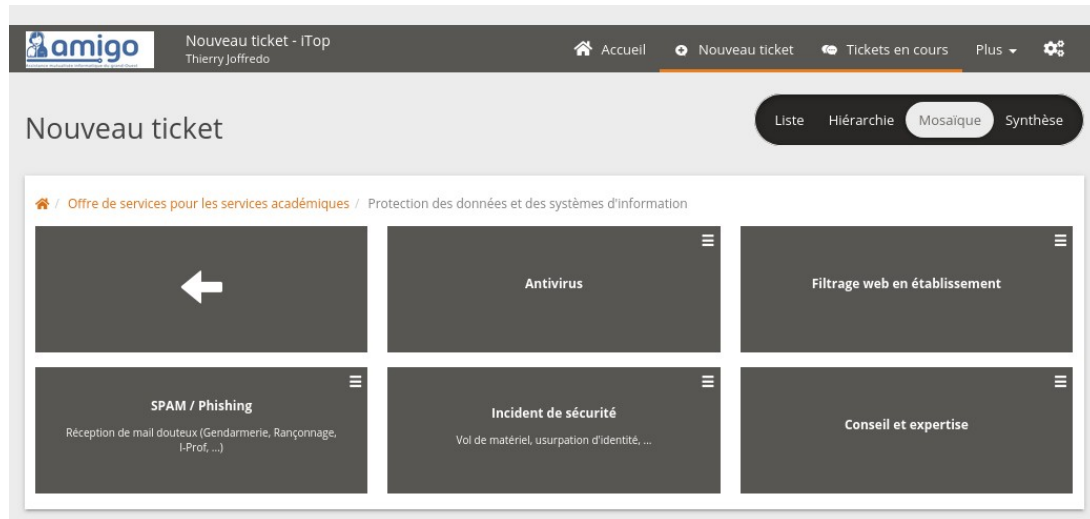
Un espace ressources Triskell :
<https://www.toutatice.fr/portail/share/zsD8VB>



Un canal sur Le Chat :

<https://go.rocket.chat/invite?host=lechat.toutatice.fr&path=invite%2FWRuc9D>

Nous contacter (incidents de sécurité, spam/phishing, conseil et expertise, filtrage web, antivirus...)



The screenshot shows the AMIGO ticketing system interface. At the top, there is a navigation bar with the AMIGO logo, the user's name 'Thierry Joffredo', and navigation links for 'Accueil', 'Nouveau ticket', 'Tickets en cours', and 'Plus'. Below the navigation bar, the main heading is 'Nouveau ticket', followed by a filter menu with options: 'Liste', 'Hiérarchie', 'Mosaïque' (selected), and 'Synthèse'. The main content area displays a breadcrumb trail: 'Offre de services pour les services académiques / Protection des données et des systèmes d'information'. Below this, there is a grid of six service categories, each with a menu icon in the top right corner: 1. A button with a left-pointing arrow. 2. 'Antivirus'. 3. 'Filtrage web en établissement'. 4. 'SPAM / Phishing' with a sub-description: 'Réception de mail douteux (Gendarmerie, Rançonnage, I-Prof, ...)'. 5. 'Incident de sécurité' with a sub-description: 'Vol de matériel, usurpation d'identité, ...'. 6. 'Conseil et expertise'.

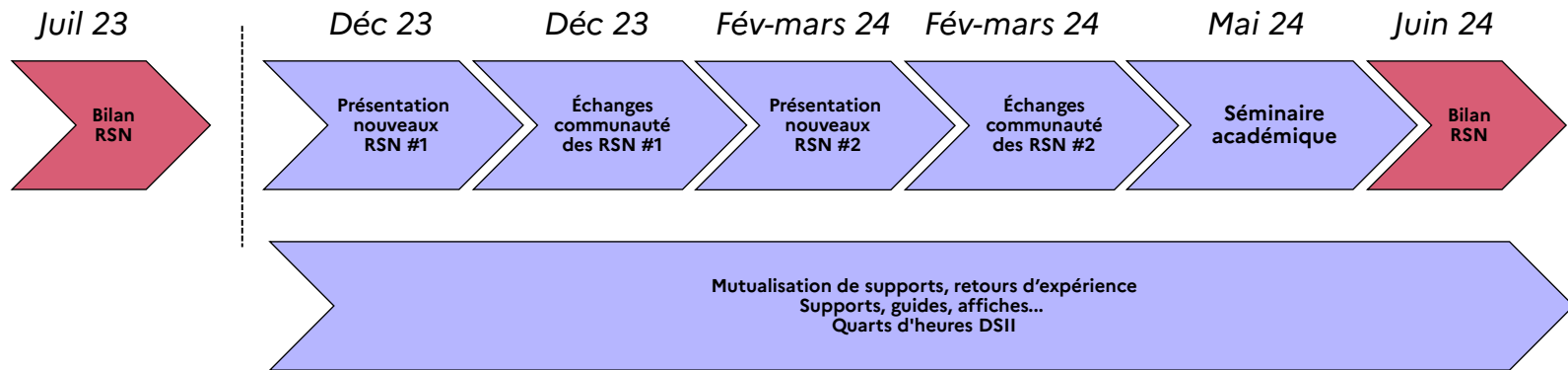
Bien différencier un incident de sécurité d'un spam :

- Incidents de sécurité : usurpation d'identité, vol de matériel...
- Spams : Phishing mail ou téléphone, rançongiciel, arnaque

Animation de la communauté des RSN sur l'année scolaire

2022-23

2023-24





ACADÉMIE DE RENNES

*Liberté
Égalité
Fraternité*

Si vous avez
des questions...



Direction des systèmes d'information et de l'innovation
