LA SECURITE NUMERIQUE

Protection de la vie privée

et

Sécurité des Systèmes d'Information

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.

Août 2023

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

Juill. 2023

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

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

Sept. 2023

Les incidents de cybersécurité

90 % des vols d'un compte utilisateur et/ou administrateur viennent d'un acte humain

OCTOBRE 2023

Menaces à la bombe sur les messageries internes de Pronote ou par mail au secretariat de direction

JUILLET 2023

Vol et publication sur Internet de la liste des 630 inscrits aux formations BTS

MAI 2023

Modification de notes et d'appréciations dans le logiciel de vie scolaire d'un lycée

Ce qui ne détruit pas rend plus fort !

« C'est en se protégeant chacun que nous augmenterons notre résilience collective »

Usurper une identité
Action d'une personne opportuniste qui cherche à nuire à une personne, une entité, un service numérique en utilisant des données identifiantes ne le concernant pas

Subir un incident de sécurité
Apprendre et se sécuriser encore plus
Rappeler des recommandations connues

Être victime d'une usurpation d'identité
300000 personnes en France sur une année

Les sanctions

Le communiqué de presse du Recteur sur les alertes à la bombe

Rennes, le 30 novembre 2023

Gestion des alertes à la bombe

Depuis plusieurs semaines, des alertes à la bombe perturbent le fonctionnement d'établissements scolaires, dans l'Académie de Rennes comme dans d'autres régions de France.
Le Recteur de la Région académique Bretagne et le Préfet de la Région Bretagne travaillent en étroite collaboration pour gérer cette situation et accompagner les chefs d'établissements.

Le plan Vigipirate Urgence attentat étant en vigueur, les établissements suivent un protocole précis pour la prise en compte des messages d'alerte à la bombe.

Tous les établissements concernés ont porté plainte et toutes les enquêtes sont en cours pour retrouver les auteurs de ces menaces, qui encourent 2 ans de prison et 30 000 € d'amende.

Le Recteur, le Préfet et l'ensemble de leurs services sont pleinement mobilisés pour faire cesser ces agissements et accompagner les équipes dans le traitement de ces actes et de leurs conséquences.
Ils apportent tout leur soutien aux chefs d'établissements, aux équipes éducatives, ainsi qu'aux élèves et aux familles, impactés par ces perturbations.

1) Dépôt de plainte

2) Recherche de traces pour identifier l'auteur

3) Interpellation de l'auteur et garde à vue / audition de l'auteur et de son entourage

Sanction :
2 ans d'emprisonnement
30 000€ d'amende

Quelques chiffres académiques

+ 7 millions de mails par mois et 91 % des attaques lancées par un courriel de phishing

- Statistiques du 1 septembre au 30 septembre 2023
  - Adresses IP bloquées : 581 000
  - Trafic Total
    5,5 millions de mails reçus
    1,55 millions de mails envoyés
  - Mails légitimes
    3,2 millions reçus
    1,53 millions envoyés

2,3 millions de mails Illégitimes

- Environ 500 comptes compromis par an qui spamment vers l'extérieur
  Environ **1% des agents académiques** sur 53000 agents

Vérifions si mon mot de passe a déjà fuité

Firefox Monitor

We found
Prénom. Nom @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

Adobe

Fuite de données ajoutée :
4 décembre 2013

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

Protégeons nos comptes utilisateurs

Les clés pour un mot de passe robuste : Newsletter #1 (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 (?;.:/!§%µ) 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&1Soleil=été*

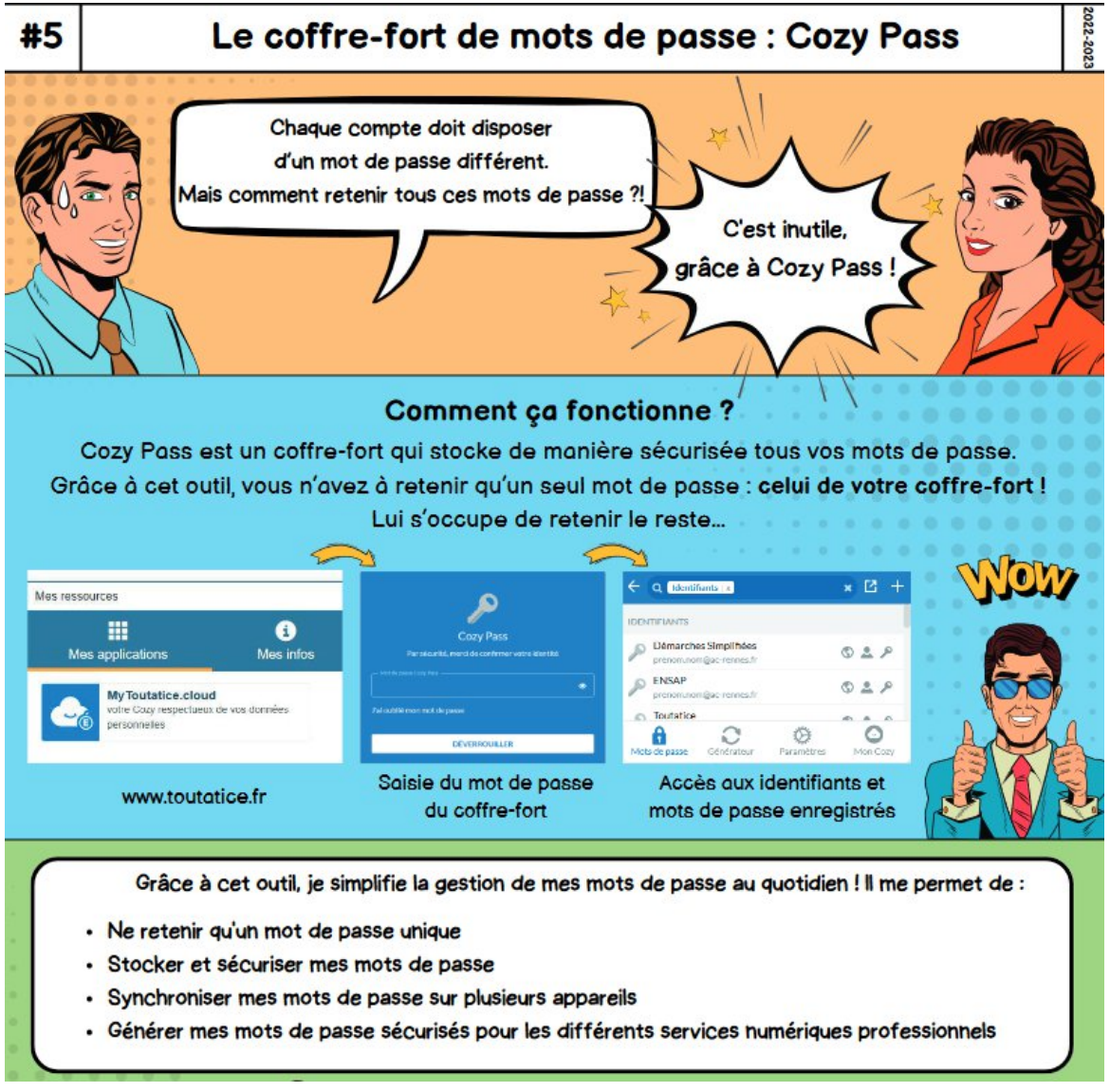
Un outil pour créer et stocker mes mots de passe : le coffre-fort de mot de passe

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 pour créer votre espace et utiliser l'application "Pass".

Utilisons un carnet de mot de passe numérique !



- Un mot de passe maître à retenir (14 caractères et 4 classes minimum)
  La phrase de passe : « j'aime manger 2 bananes dans ma journée pour être en forme !» --> J'am2bdmjpeef!
- Un mot de passe différent pour chaque service utilisé
- Un mot de passe généré aléatoirement
- Une synchronisation avec différents appareils
- Une saisie automatique des mots de passe

Verrouillons notre session

C'est rapide, simple et sécurisant !

Appui simultané sur ces 2 touches

Je quitte le bureau pour une courte durée
Je discute avec un élève
Je discute avec un enseignant
Je pars en réunion

Au retour :

- Je m'identifie pour ouvrir la session
- Je retrouve mon travail à l'identique

Adaptons notre poste de travail

Newsletter #3 (2023-2024)

#3

2023-2024

ATTENTION AUX REGARDS INDISCRETS !

UN PIRATE N'EST PAS NÉCESSAIREMENT UN GÉNIE DE L'INFORMATIQUE.

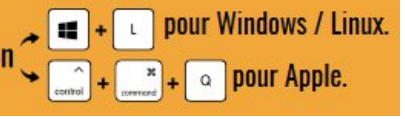
Il est facile de voler des mots de passe en observant discrètement les saisies au clavier et l'écran d'un ordinateur.

Pour vous protéger, vous pouvez adapter votre position de travail :

- En orientant votre bureau de façon à ce que votre clavier et votre écran ne soient pas exposés aux regards.
- En collant des films occultants sur les fenêtres dans les bureaux visibles du public.
- En posant des filtres de confidentialité sur vos écrans pour bloquer les regards indiscrets.

Au quotidien, adoptez ces gestes simples :

- Saisissez votre identifiant et votre mot de passe à l'abri des regards.
- Verrouillez votre session quand vous quittez votre poste de travail avec la combinaison
- Fermez votre porte de bureau à clé en cas d'absence lorsque cela est possible.



Séparons les usages personnels des usages professionnels

Newsletter #3 (2021-2022)

1

J'utilise des mots de passe différents pour mes usages professionnels et personnels

2

Je distingue ma messagerie professionnelle de ma messagerie personnelle

3

Je ne fais pas suivre mes mails professionnels sur des services de messagerie utilisés à des fins personnelles

#3 DISTINGUER LES USAGES PROFESSIONNELS ET PERSONNELS

4

Afin d'éviter le piratage de données, j'évite de connecter un équipement professionnel à un réseau Wi-Fi public ou inconnu

5

J'éteins mon poste afin de garantir l'application des mises à jour à son redémarrage

6

Je m'abstiens, dans la mesure du possible, d'enregistrer des données professionnelles à caractère personnel ou secret sur mes équipements personnels (clé USB, disque dur, téléphone, etc.) ou sur des moyens personnels de stockage en ligne

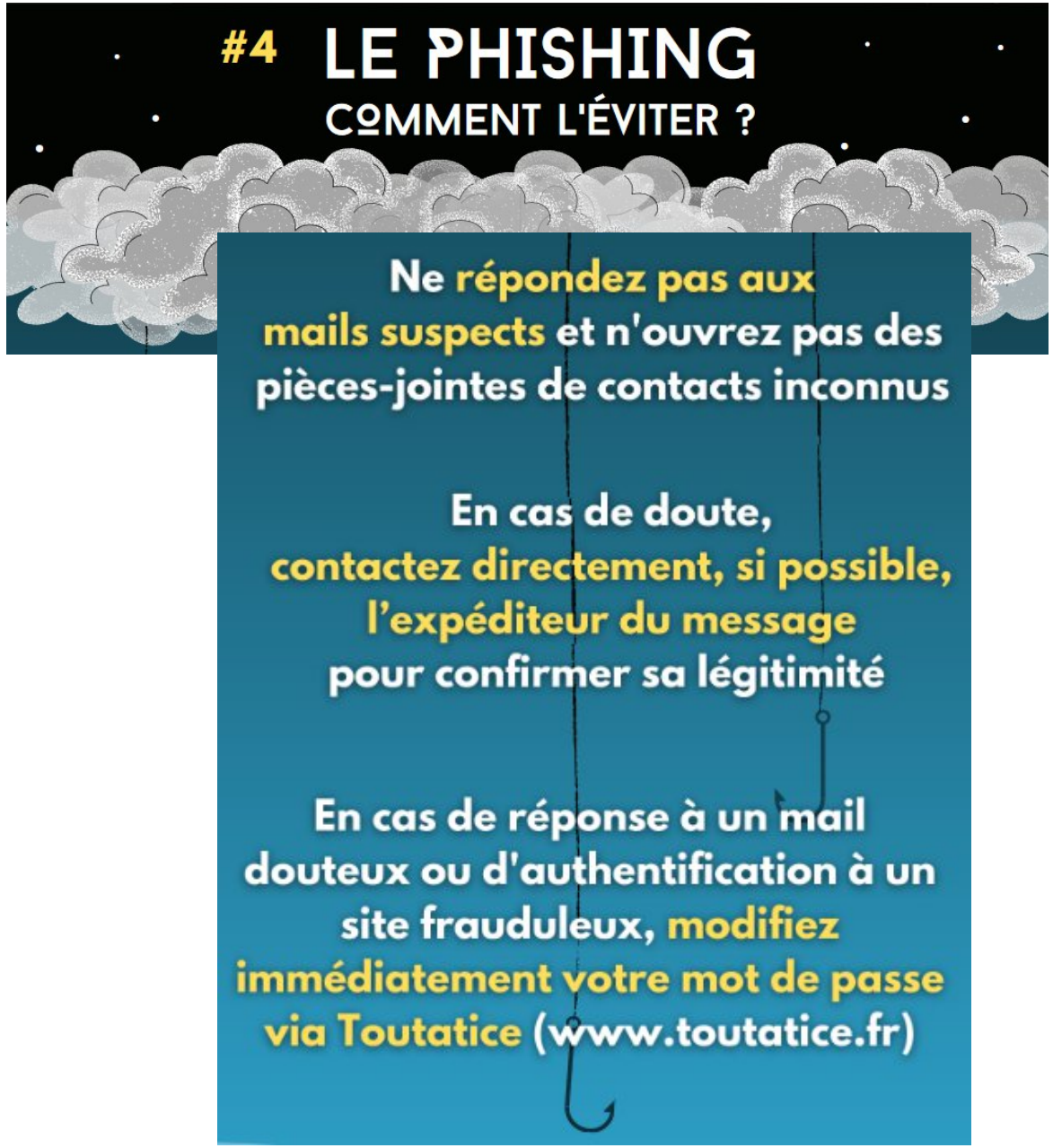
7

J'ai une utilisation raisonnable d'Internet au travail (sécurisée, adaptée à mes activités professionnelles et respectueuse du cadre légal)

La non application de ces bonnes pratiques entraine le risque que des personnes malveillantes volent des données académiques

Soyons vigilant face au phishing !

Newsletter #3 (2021-2022)



Communiquons des informations sensibles par un outil sécurisé

Newsletter #6 (2019-2020)

#6 FILESENDER

TRANSFERT SECURISE DE FICHIERS

Accessible depuis votre **bureau Toutatice**, FileSender vous permet de transférer sur Internet de manière sécurisée des fichiers volumineux (jusqu'à 100 Go) ou comportant **des informations à protéger**. Cet outil de confiance, mis à disposition par le GIP Education-Recherche RENATER, permet également les échanges avec des élèves, des familles et des personnels extérieurs à l'académie.

FILESENDER par RENATER

Trois fonctions principales :

Le dépôt vous permet de simplement transférer vos fichiers via un lien à partager avec vos destinataires ou directement via un mail. De plus, il permet le chiffrement de ce partage via un mot de passe.

La création d'invitation vous permet de donner la possibilité à une ou plusieurs personnes d'utiliser votre espace de dépôt. Ils recevront une notification les invitant à déposer leurs fichiers.

La gestion des dépôts vous permettra de suivre l'évolution de vos différents transferts (supprimer un dépôt, visualiser le nombre de téléchargements, retrouver les fichiers déposés à votre intention, renvoyer une invitation…)

Utilisons des services en ligne de confiance

Politiques > Cadres de référence

Classification des services en ligne

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

Service disponible dans le cadre de confiance ENT + GAR Service accessible depuis Toutatice ne nécessitant pas d'inscription au registre des activités de traitement ou de conventionnement avec l'éditeur
Service de confiance autorisé sous conditions Service autorisé sous les conditions mentionnées en bas de tableau
Service hors cadre de confiance 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.

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

Classification des services en ligne

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

Responsabilité du Responsable de traitement

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

Organisation de la Sécurité Numérique académique (CSN)

Le Recteur
*AQSSI

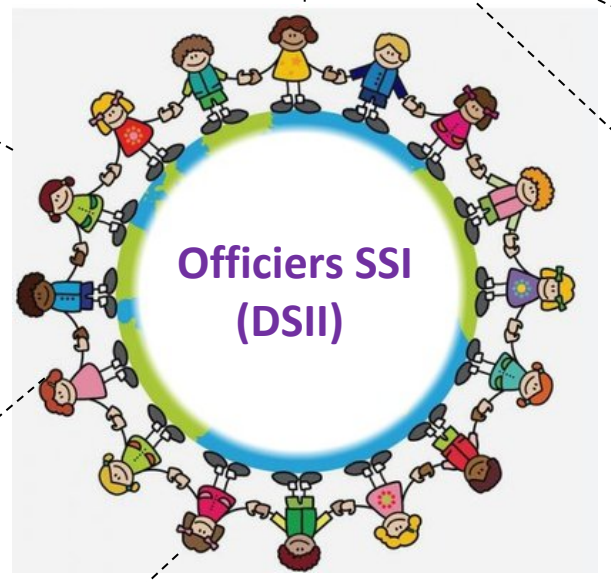
Équipe *RSSI acad.
*DPD

Cabinet du Recteur

Communauté nationale RSSI et DPD

Équipe Mobile Académique de Sécurité

Cellule juridique académique



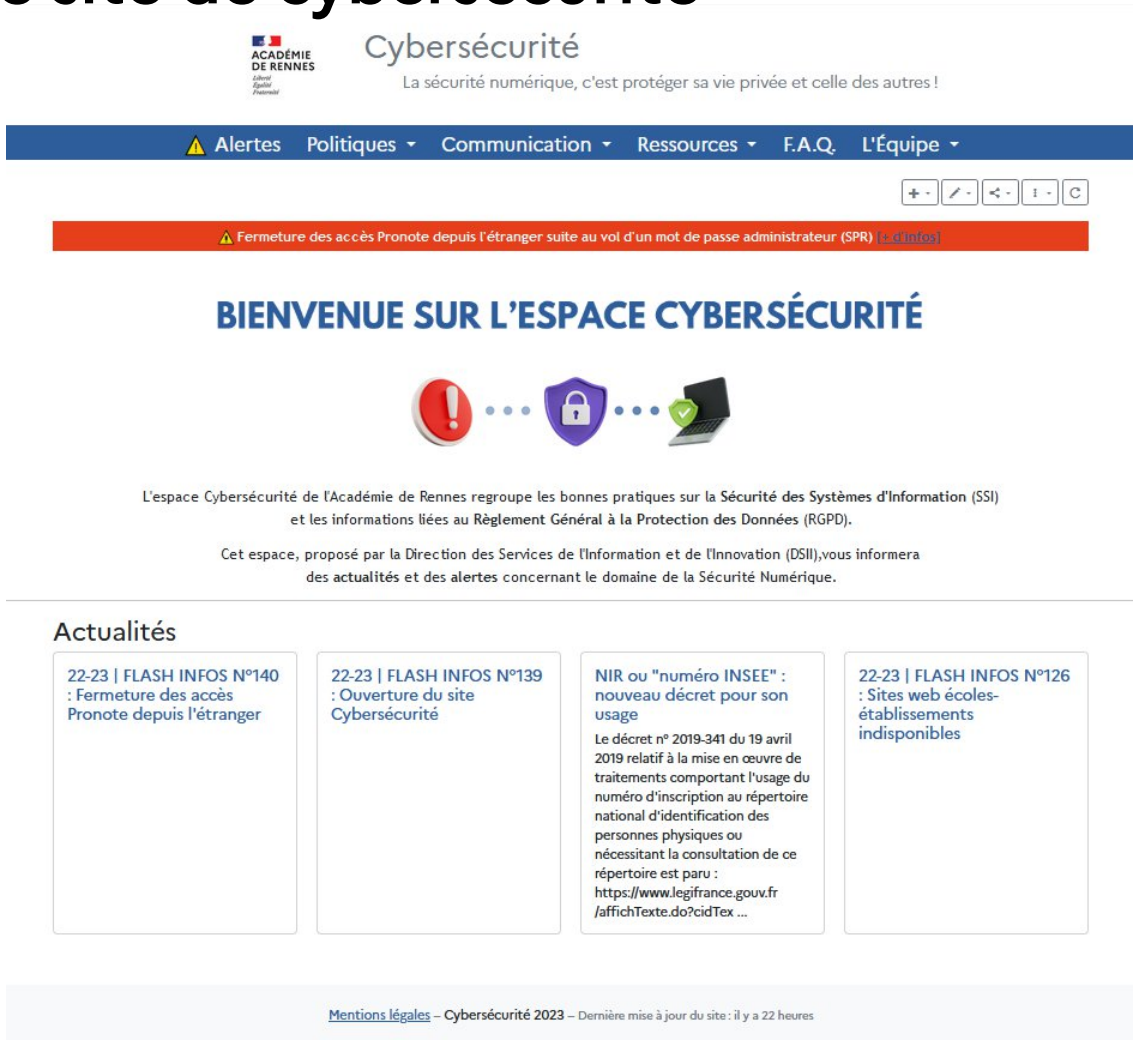
Responsables de traitement

Chef établissement Recteur

Référent Sécurité Numérique

*AQSSI = autorité qualifiée pour la sécurité des systèmes d'information
*RSSI = responsable sécurité des systèmes d'information
*DPD = délégué à la protection des données

Le site de cybersécurité



- **Accessible** depuis le bureau Toutatice > Mes infos > Cybersécurité https://cybersecurite.toutatice.fr

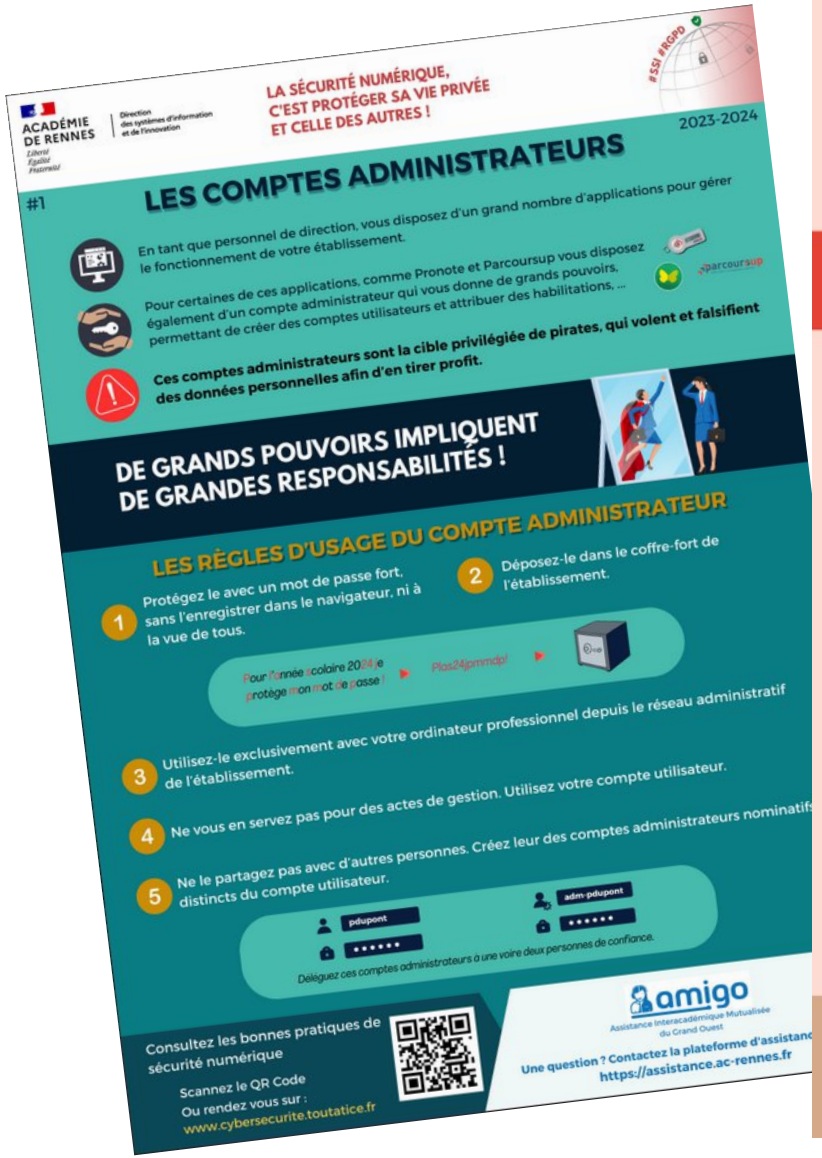
- **Alertes** : Alerte SSI, chaînes d'alertes

- **Politiques – cadre de** référence au regard des enjeux de sécurité et de souveraineté : visio-conférence, services en ligne, filtrage web, …

- **Communication** : Newsletter, Flashs infos

- **Ressources** : Services pour collaborer, sites utiles …

La Newsletter sur la sécurité numérique



En cas d'incident, suivez la chaîne d'alerte

2022-2023
Newsletter #6

EN CAS DE RÉCEPTION DE SPAMS / PHISHING

Vous recevez des méls publicitaires ou frauduleux sur votre adresse mail académique

1. Ne répondez pas au mél, ne cliquez pas sur les liens ou pièces jointes
2. Transférez ce message à l'adresse mél suivante : spam@ac-rennes.fr

EN CAS D'ACTIONS SUR UN MÉL DE PHISHING

- *Vous avez répondu à un mél de phishing*
- *Vous avez cliqué sur un lien*
- *Vous avez ouvert une pièce jointe*

1. Modifiez immédiatement votre mot de passe académique sur : www.toutatice.fr/mon-compte/
2. Contactez la plateforme AMIGO : https://assistance.ac-rennes.fr

EN CAS DE VOL DE MATÉRIEL, D'USURPATION D'IDENTITÉ

- *Vous avez subi un vol de matériel informatique (clé OTP, PC portable, ...)*
- *Vous êtes victime d'une usurpation d'identité*
- *Vous avez subi une violation de données*

1. Modifiez immédiatement votre mot de passe académique sur : www.toutatice.fr/mon-compte/
2. Prévenez la DSII à l'adresse mél dédiée : alerte.ssi@ac-rennes.fr

EN CAS DE BLOCAGE DE COMPTE DE MESSAGERIE

(ABSENCE DE L'ONGLET « MESSAGERIE » SUR LE WEBMAIL)

L'accès à votre messagerie a été bloqué suite à de nombreux méls frauduleux qui ont été envoyés depuis votre compte académique

1. Modifiez immédiatement votre mot de passe académique sur : www.toutatice.fr/mon-compte/
2. Contactez la plateforme AMIGO avec la mention « Compte désactivé » en objet : https://assistance.ac-rennes.fr

ACADÉMIE DE RENNES

Liberté
Égalité
Fraternité

Si vous avez des questions...

https://cybersecurite.toutatice.fr