ACADÉMIE
DE RENNES
*Liberté*
*Égalité*
*Fraternité*

Le quart
d'heure DSII

ACADÉMIE
DE RENNES
*Liberté*
*Égalité*
*Fraternité*

Direction
des systèmes d'information
et de l'innovation

# CYBERSÉCURITÉ
# ATTENTION AUX REGARDS INDISCRETS

# 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

# Les attaques informatiques contre les ENT continuent dans le Nord

***Technologie :*** *La semaine dernière, des menaces d'attentats ont été envoyés aux élèves, aux personnels et aux familles suite au piratage de l'environnement numérique de travail de la région Ile de France. Cette fois, c'est l'académie de Lille qui est touchée, et ce dans un contexte sécuritaire inquiétant.*

Par Guillaume Serries | Lundi 25 Mars 2024

Réaction 1 Tweet plus +

ÉDUCATION ET ENSEIGNEMENT SUPÉRIEUR

## Piratages et menaces d'attentats déstabilisent l'Éducation nationale

**Des menaces d'attaques contre des collèges et des lycées ont lieu depuis jeudi par le biais des espaces numériques de travail, notamment des messageries scolaires. Outre la prise en charge et la communication aux familles comme aux agents, la question de la vulnérabilité de ces outils se pose.**

# 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

# Créons un mot de passe robuste


Un mot de passe équivaut à la clé de votre habitation

- Choisir un mot de passe robuste avec une phrase de passe

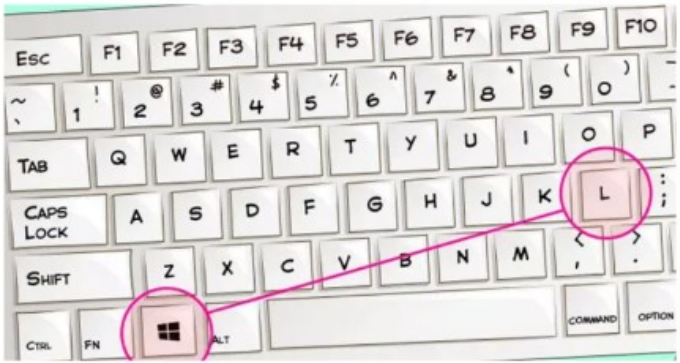
- Différencier les mots de passe qui servent dans votre domaine pro et votre domaine perso

- Ne pas partager son mot de passe

- Les enregistrer dans un coffre-fort de mot 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


**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 + L pour Windows / Linux. / control + command + Q pour Apple.
- Fermez votre porte de bureau à clé en cas d'absence lorsque cela est possible.

# 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 …

# 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*

Merci pour votre attention.