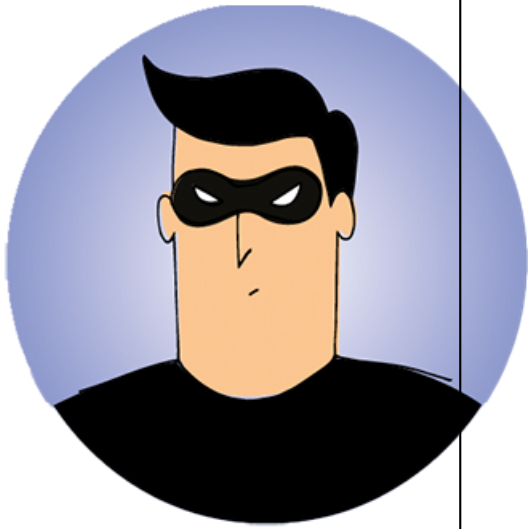
RÉGION ACADÉMIQUE
ÎLE-DE-FRANCE

Liberté
Égalité
Fraternité

SENSIBILISATION À LA SÉCURITÉ NUMÉRIQUE

Informations et bonnes pratiques

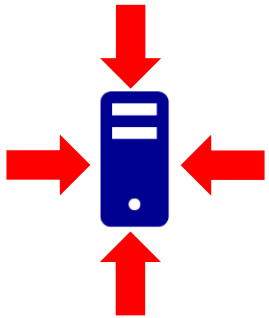
1. Actualité de la menace



Constat

Les Cyber-attaques sont de plus en plus fréquentes et de plus en plus ciblées. Elles se matérialisent par les pratiques suivantes :

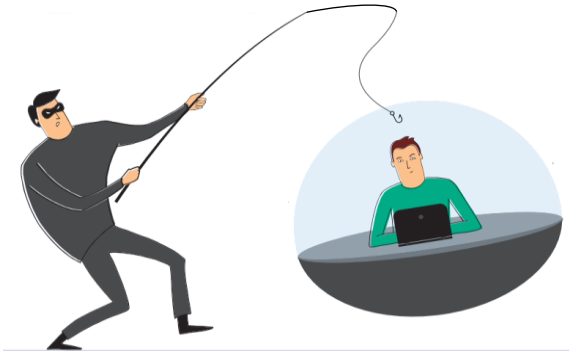
- le hameçonnage ou « phishing » ;
- les pièces-jointes infectées ;
- les attaques par déni de service ;
- l'exploitation de failles de sécurité.



L'hameçonnage ou phishing

Ce sont des 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 à la messagerie.

Les attaquants imitent nos logos et nos sites : Iprof, messagerie, ARENA, etc… pour tromper les utilisateurs.



Quelques chiffres

1500 comptes académiques usurpés sur 2024-2025
Baisse de 50 % par rapport à 2023-2024.

1900 incidents de sécurité pris en charge par l'académie en 2024-2025.

18 % des cyberattaques concernent l'administration publique.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Les pièces jointes infectées

C’est l’envoi depuis la messagerie de fichiers infectés dans un but précis :

- prendre le contrôle du poste ou de serveurs ;
- accéder aux données présentes sur le poste ou sur le réseau de postes ;
- chiffrer les données récupérées (ransomware) et exiger une rançon pour en restituer l’accès.

Ces fichiers peuvent se cacher dans toute pièce jointe.

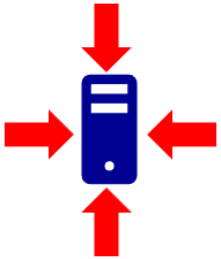
Si vous ouvrez un mail et que vous vous apercevez qu’il est frauduleux,

ne cliquez jamais sur la pièce jointe

Les autres attaques

- **Attaques par déni de service** : des milliers de machines se connectent au système d'Information (SI) afin de le surcharger et de le rendre indisponible.

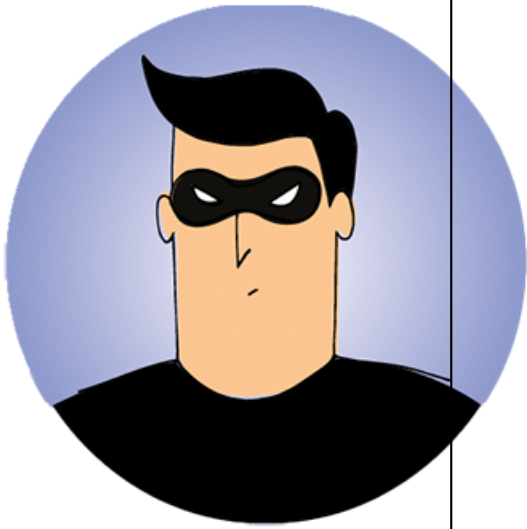
  Des établissements ont déjà subi ce type d'attaque, qui rendent impossible l'accès à internet. Des ENT en ont également été victimes.



- **Exploitations de failles de sécurité** non corrigées qui permettent des intrusions.

  Maintenez à jour les logiciels et utilisez des systèmes d'exploitation maintenus sur tous vos appareils (ex : Windows 7 n'est plus maintenu et est exposé à des failles non corrigées).

2. Les incidents de sécurité



Quels sont les incidents de sécurité les plus courants ?

- Vol d’identifiants et usurpation du compte.
- Poste infecté par un virus ou un malware.
- Ransomware (rançongiciel).
- Service indisponible (saturation ou perturbation).
- Perte de données.
- Intrusion dans le système d’information.
- Fuite de données confidentielles.
- Accès non autorisé à une ressource.

La chaîne d'alerte SSI de l'académie de Versailles

Pour tout incident de sécurité qui concerne votre environnement de travail

Poste de travail

Le réseau interne de l'école ou l'établissement

La messagerie académique

L'ENT

Une application en ligne du ministère (iProf, ONDE, SIECLE, Nuage, TRIBU, Filesender...)

Saisir la chaîne d'alerte en déclarant un incident de sécurité

Comment déclarer un incident de sécurité ?

1. Depuis le guichet Cariina et moi

2. Ou par courriel

Envoyer un courriel à

alerte-ssi@ac-versailles.fr

3. Les bonnes pratiques

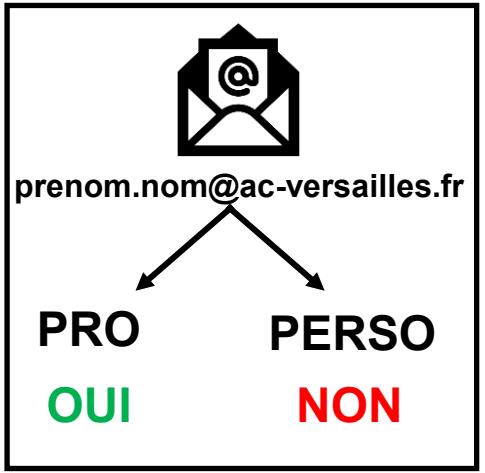
L’utilisation de la messagerie académique

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, qui peut être non conforme au RGPD.
- N'utilisez pas la messagerie professionnelle pour un usage personnel.
- **Différenciez vos mots de passe (professionnels, personnels) :**

  ☑ **Protégez la confidentialité de vos données professionnelles et de l'institution**

  ☑ **Cloisonnez votre vie professionnelle et votre vie personnelle en cas d'incident**



Quelles sont les bonnes pratiques dans le cadre professionnel ?

Limitez l'utilisation de supports amovibles non maîtrisés (disques externes, clés USB), qui peuvent contenir et propager des virus.

☑**Protégez vos données et celles des autres utilisateurs**

En cas d'infection par un rançongiciel (ransomware), déconnectez immédiatement le poste de travail du réseau (Wifi ou filaire) puis ouvrez immédiatement un ticket d'incident de sécurité.

☑**Protégez les données des autres utilisateurs**

Utilisez des mots de passe complexes et différents
et changez-les régulièrement en respectant
les critères de complexité académiques

☑**Protégez-vous contre une usurpation d'identité**

Votre nouveau mot de passe doit respecter les règles suivantes :

- Longueur comprise entre ***12 et 32 caractères***.
- Au moins une lettre ***minuscule*** (de a à z).
- Au moins une lettre ***majuscule*** (de A à Z).
- Au moins un ***chiffre*** (de 0 à 9).
- Au moins un ***caractère spécial*** parmi les suivants :

  & " ' (- _) = $ * , ; : ! + % ? . / # { [| \ @] } < >
- Tous les autres caractères (notamment accentués) sont interdits.

Sécurité des mots de passe

Combien de temps faut-il à un pirate pour trouver votre mot de passe 2025

12 x RTX 5090 | bcrypt (10)

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minescules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Instantané	Instantané	Instantané	Instantané	Instantané
5	Instantané	Instantané	57 minutes	2 heures	4 heures
6	Instantané	46 minutes	2 jours	6 jours	2 semaines
7	Instantané	20 heures	4 mois	1 an	2 ans
8	Instantané	3 semaines	15 ans	62 ans	164 ans
9	2 heures	2 ans	791 ans	3k ans	11k ans
10	1 jour	40 ans	41k ans	238k ans	803k ans
11	1 semaine	1k ans	2M ans	14M ans	56M ans
12	3 mois	27k ans	111M ans	917M ans	3Md ans
13	3 ans	705k ans	5Md ans	56Md ans	275Md ans
14	28 ans	18M ans	300Md ans	3Bn ans	19Bn ans
15	284 ans	477M ans	15Bn ans	218Bn ans	1Bd ans
16	2k ans	12Md ans	812Bn ans	13Bd ans	94Bd ans
17	28k ans	322Md ans	42Bd ans	840Bd ans	6Tn ans
18	284k ans	8Bn ans	2Tn ans	52Tn ans	463Tn ans

Hive Systems › hivesystems.com/password

☑Utilisez le coffre-fort de mots de passe Keepass XC pour générer des mots de passe complexes et uniques

KEEPASS XC
Documentation d'utilisation

Quelles sont les bonnes pratiques dans le cadre professionnel ?

Sauvegardez régulièrement vos données professionnelles, sur plusieurs destinations (disque externe, stockage en ligne...)
☑**Protégez-vous contre les pertes ou les altérations de vos données**

Limitez les échanges d'informations confidentielles ou sensibles lorsque vous êtes connectés à des réseaux non maîtrisés (lieux publics, à l'étranger), en raison du risque important de capture des données par un tiers.
☑**Protégez la confidentialité de vos données**

Utilisez les services fournis ou recommandés par l'académie (ex : https://portail.apps.education.fr) avant d'envisager de partager et de stocker vos documents professionnels sur un espace de stockage public, qui serait non conforme au RGPD.
☑**Protégez la confidentialité de vos données**

NUAGE : synchroniser des fichiers et des dossiers entre vos terminaux

PAD avancé : rédaction collaborative

Portail Tubes : publier des vidéos

TRIBU : espace collaboratif

Visio-Agents : Visioconférence

Pod Educ : podcasts

apps.education.fr

FILESENDER : partage temporaire de fichiers volumineux

TCHAP : messagerie instantanée

EVENTO : planifier vos événements

DOCS : écriture collaborative

apps.education.fr

FRANCE TRANSFERT : permet aux personnes externes de vous envoyer des fichiers

GRIST : tableur et des base de données

QUESTIONNAIRE : réaliser des enquêtes ou des questionnaires

Les services numériques académiques

ARENA **Accès à vos applications RH ou métiers (Colibris, iProf…)**

ARIANE **Intranet académique : l'actualité de l'académie en direct**

Webmail Agenda **Messagerie académique**
La messagerie académique est votre messagerie professionnelle pour tous vos échanges liés à vos missions et au suivi de votre carrière. Relevez régulièrement vos messages pour rester informé(e).

MACA DAM **Utilisez MACADAM pour configurer votre mot de passe**

Héberger le site web de son établissement ou de son école sous SPIP ou Wordpress

Spip

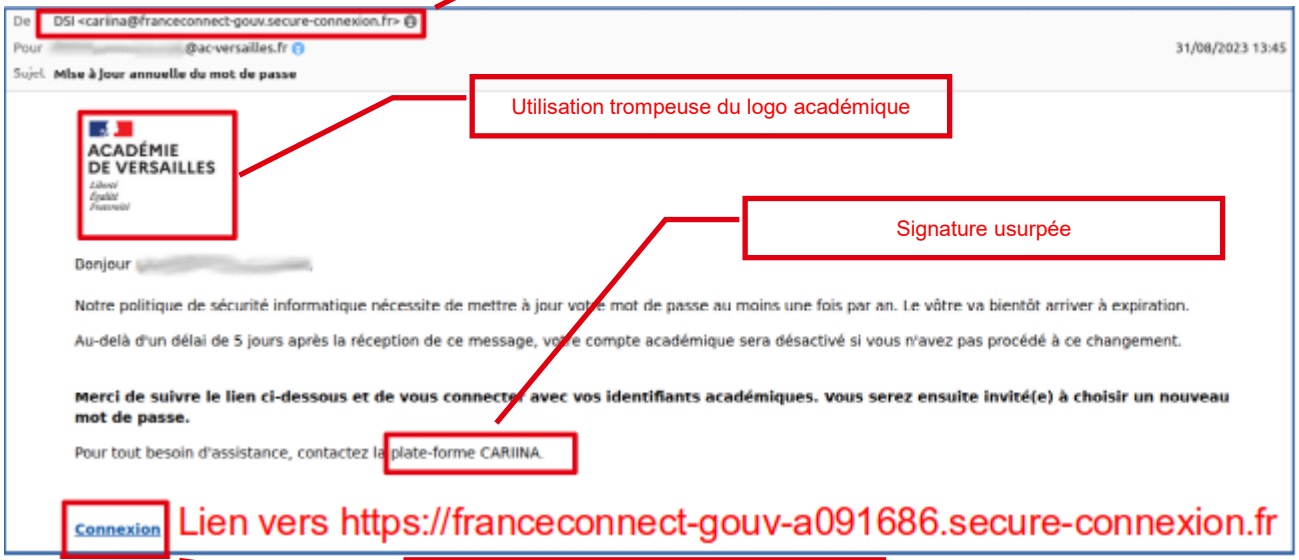
L’utilisation de la messagerie académique

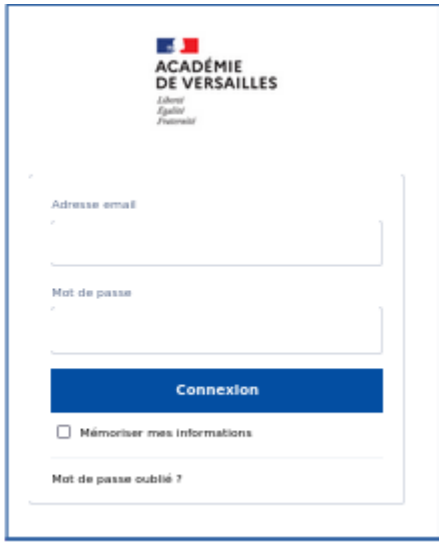
Lorsque vous recevez des courriels, prenez les précautions suivantes avant de les ouvrir :

- Si 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.
- Si un lien ou plusieurs figurent dans un courriel, vérifiez l’adresse du site en passant votre souris sur chaque lien avant de cliquer.
- Ne répondez jamais par courriel à une demande d’informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire).

☑ **Protégez-vous contre le phishing et l'usurpation d'identité !**

Analyse d'un message de phishing





Journalisation et filtrage

La <u>politique de sécurité académique</u> pose les exigences suivantes :

- Toute activité vers l'internet depuis un terminal fourni par la collectivité ou l'académie doit être tracée. Ces traces doivent être accessibles aux chefs d'établissements, aux directeurs d'écoles et au RSSI académique. Elles sont conservées durant un an.

- Un contrôle des navigations internet initiées par les élèves est effectué, en interdisant l'accès à un ensemble de sites reconnus comme inappropriés au sens de la circulaire 2004-035 du 18 février 2004 par l'intermédiaire de mécanismes adaptés réputés efficaces tels que listes noires, listes blanches […].

Ces exigences permettent par exemple de :

- protéger les mineurs contre l'accès à des contenus inappropriés ;

- protéger les réseaux et les terminaux contre les virus en bloquant les requêtes vers internet frauduleuses ;

- établir l'origine d'une usurpation de compte ayant entraîné la profération d'insultes ou de menaces.

Ressources pour aller plus loin

Des posters à afficher dans les lieux de passage

7 conseils pour lutter contre le piratage

La chaîne d'alerte académique

Ressources

- Le portail SSI académique : https://ariane.ac-versailles.fr/pia/jcms/s1_8458810/fr/portail-de-la-securite-des-systemes-d-information-ssi

- Le site de la DRANE : https://drane-versailles.region-academique-idf.fr/
- Culture cyber : https://drane-versailles.region-academique-idf.fr/spip.php?rubrique204
- BD de sensibilisation
  - Spam, phishing : https://edu-html.ac-versailles.fr/phishing/
  - Travail à https://edu-html.ac-versailles.fr/phishing2/distance :
  - Confidentialité des mots de passe : https://edu-html.ac-versailles.fr/phishing3/
  - Rançongiciel : https://edu-html.ac-versailles.fr/phishing4/

Ressources

Plateforme TOP

Initiez-vous à la recherche en source ouverte (OSINT)

THE OSINT PROJECT

https://the-osint-project.fr

Mon empreinte numérique

Comment est exposée votre identité académique ?

Ressources

- **Plateforme Moodle ELEA**

Dans le cadre de l'éducation à la citoyenneté numérique, la Drane d'Ile-de-France a produit des parcours Eléa permettant d'acculturer les élèves aux problématiques de la sécurité numérique et à la maîtrise de leur empreinte numérique. Ces parcours, disponibles dans le réseau des concepteurs, peuvent être consultés puis dupliquer pour être partagés, auprès des élèves, sur les plateformes Eléa, intégrées au sein des ENT.

Sur les traces de mon identité numérique

Choisir un mot de passe robuste

Réagir face au phishing

Plongée au cœur de la cryptographie

OSINT : la conquête des données publiques

Eléa

Réseau des concepteurs

https://concepteurs.apps.education.fr/login/index.php

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
- **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/
- **Ressources du site CYBERMALVEILLANCE.GOUV.FR :** https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/liste-des-ressources-mises-a-disposition
- **PIX :** https://pix.fr
- **EDUCATION ET CYBERSECURITE :** https://eduscol.education.fr/3679/education-et-cybersecurite

Une question sur la cybersécurité ?

Contactez le Responsable de la Sécurité des systèmes d'Information (**RSSI**) : rssi@ac-versailles.fr

1er degré : contactez votre ERUN/CPC numérique

2nd degré : contactez votre **conseiller de bassin pour le numérique** : https://www.dane.ac-versailles.fr/spip.php?rubrique19