RÉGION ACADÉMIQUE
ÎLE-DE-FRANCE

Liberté
Égalité
Fraternité

RÉGION ACADÉMIQUE
ÎLE-DE-FRANCE

Liberté
Égalité
Fraternité

SENSIBILISATION À LA CYBERSÉCURITÉ

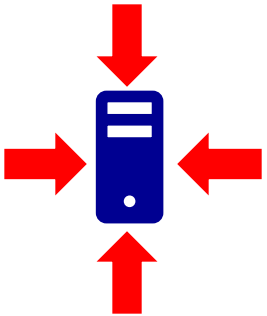
Informations et bonnes pratiques

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 :

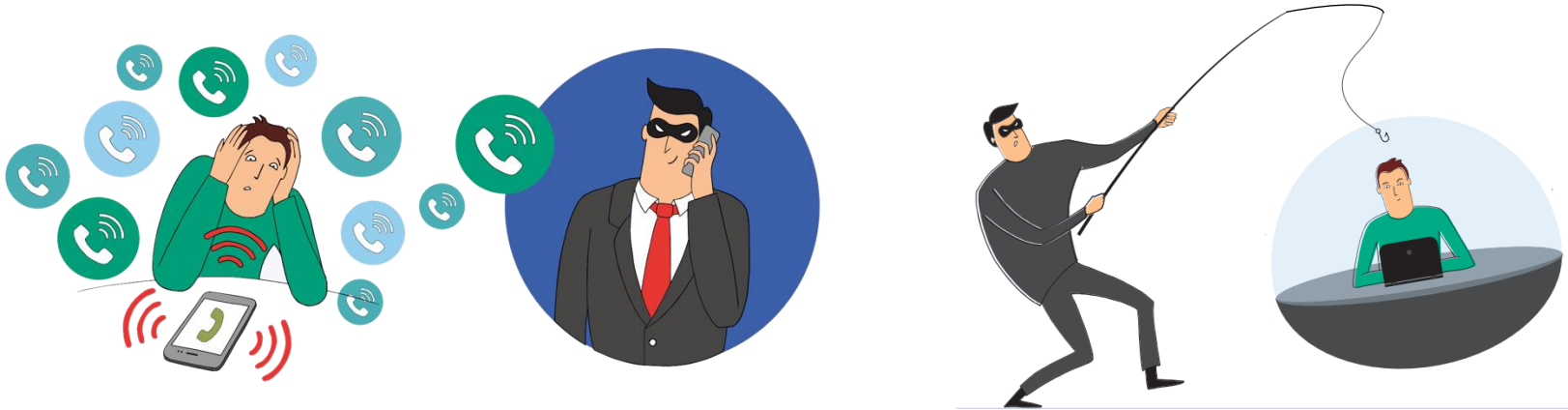
- Le hameçonnage ou *phishing*
- Les pièces-jointes infectées
- Les attaques par déni de service
- L'exploitation de failles de sécurité



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

91 % des attaques sont lancées par un courriel de *phishing*

38 % des pièces jointes malveillantes sont des fichiers Microsoft Office

Les supports amovibles sont responsables de **9 %** des vecteurs d'attaque

En 2022 en France, **19 %** des attaques par rançongiciel ont concerné des ministères et **23 %** des collectivités territoriales

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Les pièces jointes infectées

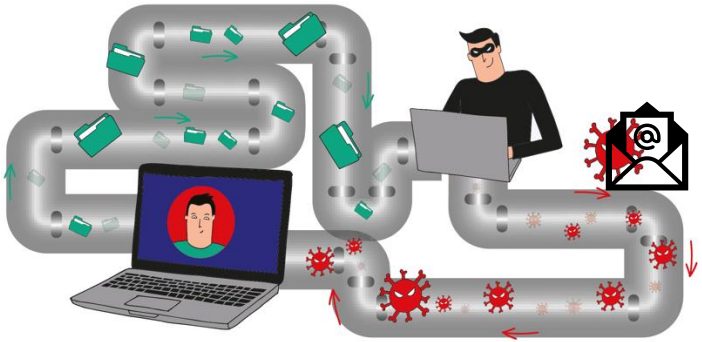
C’est l’envoi depuis la messagerie de fichiers infectés dans un but précis :

- 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 *email* et que vous vous apercevez qu’il est frauduleux,

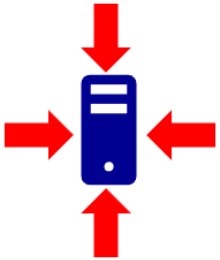
ne cliquez jamais sur la pièce jointe



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 ?

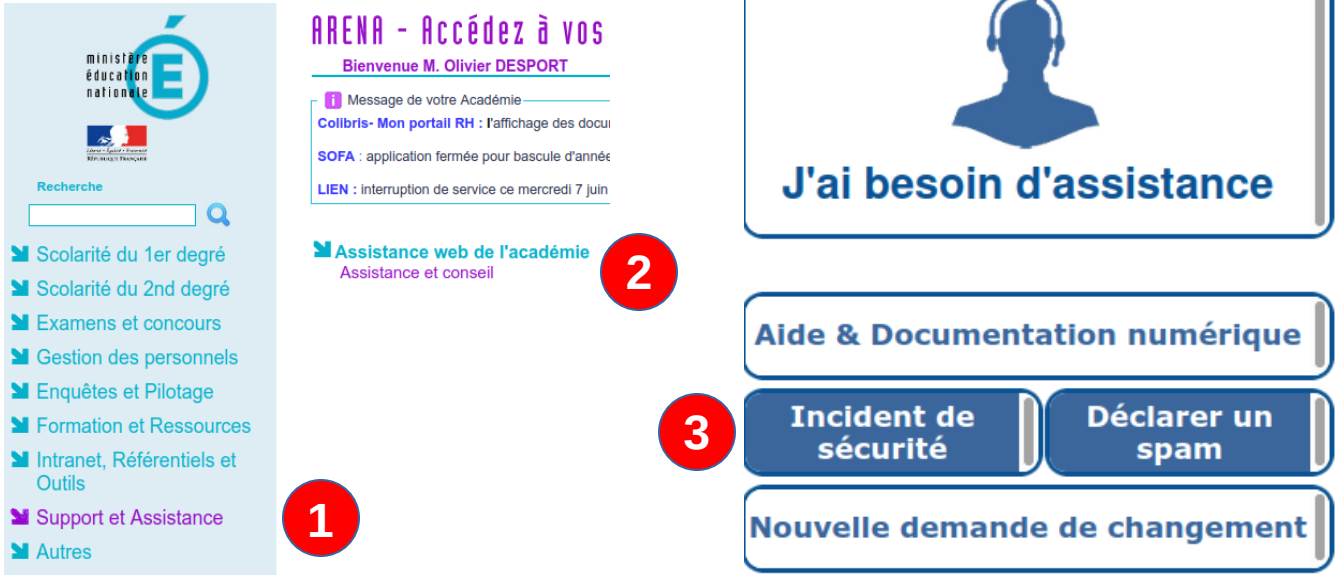
- Vol d'identifiants et usurpation du compte
- Poste infecté par un virus ou un malware
- *Ransomware* (rançongiciel)
- Service indisponible (saturation ou perturbation)
- Perte de données
- Intrusion dans le système d'information
- Fuite de données confidentielles
- Accès non autorisé à une ressource

Quelles conséquences possibles ?

- Accès à internet indisponible
- Chiffrement des données et demande de rançon
- Modification frauduleuse des données
- Service indisponible (saturation ou perturbation)
- Perte de données
- Fuite de données confidentielles
- Accès non autorisé à une ressource

Comment déclarer un incident de sécurité ?

Les incidents de sécurité doivent être déclarés par tout personnel sur la **plate-forme CARIINA** (https://id.ac-versailles.fr)



Le Responsable de la sécurité des SI et la DSI vous apporteront l'assistance nécessaire.

Informez votre chef d'établissement de l'incident

3. Les bonnes pratiques

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

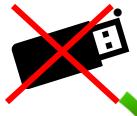
- **Utilisez les services fournis** ou recommandés par l'académie (ex : https://portail.apps.education.fr) avant d'envisager de partager et de stocker vos documents professionnels sur un espace de stockage public, qui serait non conforme au RGPD

✔ Protégez la confidentialité de vos données

- **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

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 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 :

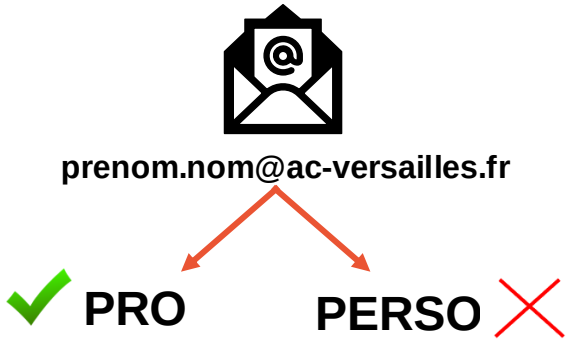
& " ' (- _) = $ * , ; : ! + % ? . / # { [| \ @] } < >

- Tous les autres caractères (notamment accentués) sont interdits.

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

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

Ressources pour aller plus loin

Ressources académiques

- 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 DANE : https://www.dane.ac-versailles.fr/spip.php?article242
  Les cookies, le RGPD, le mot de passe : https://www.dane.ac-versailles.fr/spip.php?article510
- 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/

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

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