ACADÉMIE
DE POITIERS

Liberté
Égalité
Fraternité

SENSIBILISATION À LA CYBERSÉCURITÉ

Sensibilisation aux enjeux de la cybersécurité

CYBER CONFIANCE
Tous acteurs de la sécurité au quotidien

SENSIBILISATION À LA CYBERSÉCURITÉ

Sensibilisation aux enjeux de la cybersécurité

Ordre du jour

1. Actualités de la menace cyber

2. Les bonnes pratiques en matière d'hygiène numérique

3. Quelques attaques connues

1. Actualités de la menace cyber

L'état de la menace en quelques mots

Les principales cyber-attaques :

- **Le hameçonnage ou phishing**
- **Les pièces jointes infectées**
- **Les attaques par déni de service (DDoS)**
- **Exploitation de failles de sécurité**

Quelques chiffres clés :

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

38 % des pièces jointes malveillantes sont des **fichiers Microsoft Office**

9% des vecteurs d'attaque dont les **supports amovibles** sont responsables

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

Quels sont les conséquences et les impacts de ces attaques ?

Accès à internet indisponible
Interruption des services en ligne

Chiffrement, et demande de rançon
Violation de donnée et risque de ne jamais la retrouver

Accès non autorisé à une ressource
Violation de la confidentialité, risque de fuite d'informations sensibles, atteinte à la sécurité

Modification frauduleuse des données
Altération de données, perte de confiance, atteinte à la réputation

Fuite de données confidentielles
Violation de la confidentialité, perte de confiance, risques juridiques

Service indisponible (saturation ou perturbation)
Interruption des services en ligne, perturbation de l'apprentissage, mécontentement des utilisateurs

SENSIBILISATION À LA CYBERSÉCURITÉ

Sensibilisation aux enjeux de la cybersécurité

2. Les bonnes pratiques en matière d'hygiène numérique

Quelles sont les bonnes pratiques dans le cadre professionnel ?

Faites des sauvegardes régulières
Sauvegardez régulièrement vos données professionnelles, sur plusieurs destinations (disque externe, solutions internes DSI…)

Utilisez les services fournis ou recommandés avant de partager ou stocker vos documents professionnels
Utilisez les services fournis ou recommandés avant d'envisager de partager et de stocker vos documents professionnels sur un espace de stockage public

Limitez les échanges d'informations confidentielles
Limitez les échanges d'informations confidentielles ou sensibles lorsque vous êtes connectés à des réseaux non maîtrisés en raison du risque important de capture des données par un tiers

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

En cas d'infection par un rançongiciel déconnectez le poste du réseau (WIFI ou filaire)
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.

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

Focus messagerie professionnelle – Séparez vos usages professionnels de vos usages personnels

Utilisez la messagerie académique pour tous vos usages professionnels

N'utilisez pas la messagerie professionnelle pour un usage personnel

Ne transférez pas les messages professionnels vers une messagerie personnelle

Différenciez vos mots de passe (professionnels, personnels)

Focus messagerie professionnelle – Lorsque vous recevez des courriels, prenez les précautions suivantes avant de les ouvrir :

Vérifiez la cohérence entre l'expéditeur présumé et le contenu du message

Si un lien figure dans un courriel, vérifiez l'adresse du site en passant votre souris dessus avant de cliquer

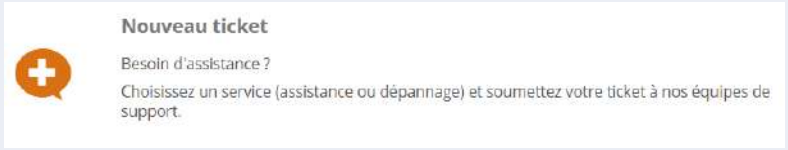
N'ouvrez pas les pièces jointes provenant de destinataires inconnus

Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles

Focus - Comment déclarer un incident de sécurité ou simplement poser une question sur la cybersécurité?

- Par le portail d'assistance académique : https://sumitnaq.phm.education.gouv.fr/

1



2

- Par email : cybersecurite@ac-poitiers.fr

Les ressources essentielles à connaître

Les ressources Académiques

- Parcours **PIX** traitant de la cybersécurité: https://integration.pix.fr/cybersecurite
- Site gouvernemental « **Cyber malveillance** » : https://www.cybermalveillance.gouv.fr/
- Site de la **CNIL** : https://www.cnil.fr/fr/cybersecurite
- **CLEMI** : https://www.clemi.fr/familles/outils-de-sensibilisation-et-mediation/campagne-de-sensibilisation/les-ecrans-apprendre-sen-servir-pour-ne-pas-les-subir

Pour vous former

- N'hésitez pas à suivre le parcours de sensibilisation en ligne produit par Cybermalveillance.gouv.fr ***"Agir pour contribuer à ma sécurité numérique et à celle de mon organisation".***
- 3 modules de 20 minutes pour découvrir les bases de l'hygiène numérique !

SENSIBILISATION À LA CYBERSÉCURITÉ

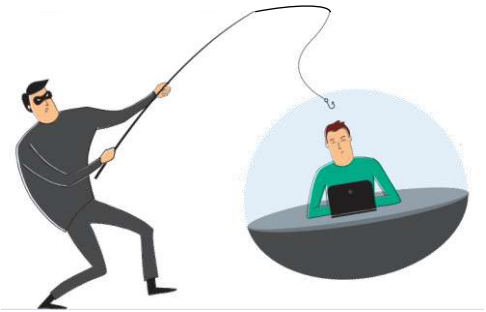
Sensibilisation aux enjeux de la cybersécurité

3. Quelques attaques connues

3. Quelques attaques connues

Hameçonnage (phishing)

- Concernant le phishing, les attaquants créent des messages trompeurs en se faisant passer pour des entités légitimes. **Ils imitent nos logos et nos sites** : Iprof, messagerie, ARENA, etc… pour tromper les utilisateurs.
- Ce sont des techniques de manipulation psychologique pour **inciter les utilisateurs à se connecter** et accéder à leurs informations confidentielles.
- Ces informations sont ensuite exploitées pour des **activités malveillantes** telles que l'**usurpation d'identité** et le **vol de données sensibles**, mettant ainsi en danger la **sécurité** et la **confidentialité** des utilisateurs visés.



3. Quelques attaques connues

Pièces jointes infectées

- C'est l'envoi depuis la messagerie de **fichiers infectés** dans un but précis, ces fichiers se cachent dans une **pièce jointe**.
- Si vous ouvrez un mail et que vous vous apercevez qu'il est **frauduleux, ne cliquez jamais sur la pièce jointe**.
- Le but final de cette attaque est de :
  - ❑ **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 (rançongiciel) et exiger une rançon pour en restituer l'accès

3. Quelques attaques connues

Quelques autres attaques

- **Attaques par déni de service (DDOS)** : des milliers de machines se connectent au système d'Information (SI) afin de le **surcharger** le **rendre indisponible**. Des établissements et des ENT ont déjà subi ce type d'attaque, qui rendent impossible l'accès à internet.

- **Attaque par exploitation de faille de sécurité Windows** : les attaquants exploitent une **vulnérabilité** qui cause des dommages potentiels comme le contrôle total du système ou le vol de données sensibles. Il est donc important de régulièrement **mettre à jour** les postes informatiques.