ACADÉMIE D'ORLÉANS-TOURS
Liberté Égalité Fraternité

Pratiques et recommandations autour de la sécurité du numérique

Suite à la propagation de messages malveillants sur les ENT et à l'augmentation des menaces cyber, il est de notre devoir à tous d'adopter les bonnes pratiques pour se protéger et protéger les autres.
Ces recommandations vous aideront.

Pour protéger ses mots de passe (messagerie électronique, ENT etc.)

Choisir un mot de passe sécurisé

- ☑ L'ANSSI recommande d'utiliser un mot de passe de 12 caractères qui comprend des minuscules et **au moins 1 majuscule, 1 chiffre, 1 caractère spécial.**
- ☑ Le mot de passe académique doit être modifié 2 fois par an. Il doit s'agir d'un véritable changement : **changer un seul caractère ne peut pas suffire**.

Protéger ses mots de passe

- ☑ Pour se souvenir de son mot de passe, on peut utiliser une **phrase de passe** : il suffit de mémoriser une phrase personnelle et d'utiliser les premières lettres de chaque mot de la phrase pour constituer un mot de passe personnel.
- ☑ Un mot de passe ne doit pas être réutilisé sur plusieurs sites.
- ☑ Pour retenir plusieurs mots de passe, **il ne faut pas les enregistrer dans votre navigateur**.

Utiliser un coffre-fort de mots de passe

- ☑ Vous pouvez utiliser Keepass, un coffre-fort de mots de passe **gratuit et certifié ANSSI**. Vous pouvez le télécharger ici.
- ☑ Attention cependant : il ne faut pas enregistrer la base de données sur les PC des établissements, mais sur **votre ordinateur personnel ou un support amovible** (disque dur, clé USB, à condition d'en avoir une copie à un autre endroit).
- ☑ Keepass existe également sur Android (exemple : Keepassdroid) et sur i-Phone (exemple : MiniKeePass).
- ☑ Vous trouverez ici des tutoriels pour vous aider.

Pour protéger son ordinateur

Ne pas se connecter au wifi public

- ☑ Vous ne devez jamais connecter votre PC à un wifi public, sauf s'il est muni d'un VPN.

Utiliser un antivirus

- ☑ Depuis plusieurs années, les personnels de l'EN bénéficiaient d'une licence gratuite de l'antivirus Trend pour un usage personnel. Le marché n'ayant pas été reconduit avec les mêmes modalités, cet usage n'est plus possible à compter de la rentrée. En remplacement, vous pouvez utiliser l'antivirus Windows Defender, proposé gratuitement sur Windows, ou une solution de votre choix.

Savoir reconnaître un mail frauduleux

- ☑ Pour savoir repérer un mail frauduleux, vous pouvez vous aider des conseils donnés sur le PIA.

Vérifier la sécurité d'un document téléchargé

- ☑ En cas de doute sur la sécurité d'un document, vous pouvez utiliser Jecliqueoupas, l'outil d'analyse en ligne proposé par le gouvernement. Il est nécessaire d'avoir une adresse académique.

Signaler un site illicite

- ☑ Vous pouvez signaler les sites illicites à la plateforme Pharos.

Que faire en cas de doute ?

Nettoyer son ordinateur en cas de virus

- ☑ Si vous soupçonnez la présence d'un virus sur votre ordinateur, vous pouvez le nettoyer grâce à **Rescue disk**. Vous pouvez le télécharger ici.
- ☑ Attention : ce nettoyage nécessite un accès internet et un certain nombre de manipulations.

Diagnostiquer si l'ordinateur a été un victime d'un incident

- ☑ Si vous pensez être victime d'un incident, le site Cybermalveillance vous propose un outil de diagnostic qui vous donne des **recommandations** (en cas de fraude à la CB, il vous orientera par exemple vers la plateforme Perceval).
- ☑ Le cas échéant, il vous orientera vers des professionnels qui vous aideront.
- ☑ Ce site est consultable ici.

Document créé par Michaël Carpentier (RSSI-DPD de l'Académie Orléans-Tours) en collaboration avec Mathilde Dénoyer (DRANE) - Mai 2024