Hes·so
Master

Bonnes pratiques relatives à la gestion du mot de passe et de l'ordinateur

Gestion du mot de passe

- Utilisez un mot de passe suffisamment long et complexe
- Utilisez un mot de passe impossible à deviner

  Comment créer un mot de passe solide ? Voici 2 exemples :

  - La méthode des premières lettres :
    Un tiens vaut mieux que deux tu l'auras > 1tvmQ2tl'A
  - La méthode phonétique :
    J'ai acheté huit CD pour cent euros cet après-midi > ght8CD%E7am
- **Pour votre compte de messagerie Outlook fourni par HES-SO Master**, choisissez un mot de passe particulièrement robuste

  Votre adresse de messagerie est généralement associée à beaucoup de vos comptes en ligne. Cela permet notamment de recevoir les liens de réinitialisation des mots de passe de vos autres comptes. Un cybercriminel qui réussirait à pirater votre messagerie pourrait facilement utiliser la fonction « mot de passe oublié » des différents services auxquels vous pouvez accéder, comme votre compte bancaire, pour en prendre le contrôle.

  Votre mot de passe de messagerie est donc l'un des plus importants à protéger.

- Utilisez un gestionnaire de mots de passe

  KeePass, un gestionnaire de mots de passe sécurisé et gratuit : ce petit logiciel libre et en français, certifié par l'OFIT et par l'ANSSI et permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications. KeePass dispose aussi d'une fonction permettant de générer des mots de passe complexes aléatoires.
- Changez votre mot de passe au moindre soupçon
- Ne communiquez jamais vos mots de passe à un tiers
- N'utilisez pas vos mots de passe sur un ordinateur partagé par plusieurs personnes

  En principe, l'utilisation d'un ordinateur partagé est à proscrire pour vous connecter aux ressources de HES-SO Master. Si toutefois les circonstances vous y obligent, n'y stockez aucune information relative à votre compte et votre mot de passe HES-SO.
- Activez la « double authentification » lorsque c'est possible (exemple suivant avec SWITCH edu-ID)

  SWITCH edu-ID : comment activer l'authentification en 2 étapes

Gestion de votre ordinateur

Vous utilisez votre ordinateur privé et/ou votre smartphone pour accéder à certaines ressources mises à votre disposition par HES-SO Master.

1. D'une façon générale, ayez une utilisation responsable et vigilante de vos équipements. Ayez conscience que vos activités personnelles peuvent faire prendre un risque aussi à HES-SO Master, redoublez donc d'attention et de prudence.

2. **Appliquez les mises à jour de sécurité sur tous vos équipements connectés** (PC, tablettes, téléphones…), et ce dès qu'elles vous sont proposées, afin de corriger les failles de sécurité qui pourraient être utilisées par des cybercriminels pour s'y introduire et les utiliser pour attaquer le réseau de HES-SO Master au travers de vos accès.

3. Vérifiez que vous utilisez bien un **antivirus** et scannez vos équipements : vérifiez que tous vos équipements connectés (PC, téléphones, tablettes…) sont bien protégés par un antivirus, qu'il est bien à jour, et effectuez une analyse complète (scan) de vos matériels. Si un matériel ne peut avoir d'antivirus, évitez le plus possible de l'utiliser pour accéder aux services de HES-SO Master.

4. À la maison, **sécurisez votre connexion WiFi personnelle**. Il est donc primordial de bien la sécuriser pour éviter toute intrusion sur votre réseau qui pourrait être utilisée pour attaquer le réseau de HES-SO Master. Utilisez un mot de passe suffisamment long et complexe (voir plus haut) et assurez-vous que vous utilisez bien le chiffrement de votre connexion en WPA2. Pensez également à mettre à jour régulièrement votre « box Internet » en la redémarrant ou depuis son interface d'administration.

5. **Sauvegardez régulièrement votre travail** : la sauvegarde est le seul moyen permettant de retrouver ses données en cas de cyberattaques, mais également en cas de panne ou de perte de son équipement. Sauvegardez régulièrement votre travail sur un support externe à votre équipement (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée.

6. **Méfiez-vous des messages inattendus** : que ce soit par messagerie (email, SMS, chat…), en cas de message inattendu ou alarmiste, demandez toujours confirmation à l'émetteur par un autre moyen. Il peut s'agir d'une attaque par hameçonnage (phishing) visant à vous dérober des informations confidentielles (mots de passe), de l'envoi d'un virus par pièce jointe ou d'un lien qui vous attirerait sur un site piégé, ou encore d'une tentative d'arnaque aux faux ordres de virement (voir menaces supra).

7. **N'installez vos applications que dans un cadre « officiel »** et évitez les sites suspects. Sur vos équipements personnels utilisés pour accéder aux ressources de HES-SO Master, n'installez des applications que depuis les sites ou magasins officiels des éditeurs (exemple : Apple App Store, Google Play Store) pour limiter les risques d'installation d'une application piégée pour pirater votre équipement. De même, évitez les sites Internet suspects ou frauduleux (téléchargement, vidéo, streaming illégaux) qui pourraient également piéger vos équipements.