10 règles d'or pour la cybersécurité

Protégez vos comptes avec une authentification forte !

- Utilisez l'**authentification multifactorielle (MFA)** quand c'est possible!
- Utilisez des **mots de passe longs (15 caractères au moins)**, contenant des majuscules, des minuscules, des caractères numériques et des caractères spéciaux (&,$,%, !,=,+...).
- Ne les **partagez PAS**
- Utilisez un **gestionnaire de mots de passe** (A ne pas confondre avec l'enregistrement de mots de passe dans votre navigateur, à éviter !)

Créez des comptes distincts

- Utilisez des **mots de passe distincts pour vos comptes professionnels et personnels**.
- **Protégez votre e-mail scolaire** : ne l'utilisez pas pour vous inscrire sur des sites ou plateformes non liés à l'école !
- Vérifiez régulièrement les applications et services **ayant accès à vos comptes.** Supprimez ceux que vous n'utilisez plus ou auxquels vous ne faites pas confiance.

Créez des sauvegardes

- Stockez toutes vos données dans un système où des sauvegardes sont effectuées régulièrement et de manière centralisée.
- Le personnel est tenu de sauvegarder les documents relatifs à son travail dans son compte scolaire 0365.

Mises à jour de sécurité

- **Mettez régulièrement à jour tous vos logiciels et applications** afin de corriger les éventuelles failles de sécurité.
- Prenez l'habitude de **redémarrer régulièrement vos appareils**, car certaines mises à jour nécessitent un redémarrage pour être prises en compte.
- **Soyez attentif aux notifications concernant les mises à jour** et agissez rapidement pour maintenir la sécurité de votre appareil.

Sécurisez votre espace de travail

- Ne laissez **jamais** de documents physiques (i.e., des papiers) ou d'appareils **sans surveillance** sur votre bureau.
- **Verrouillez votre ordinateur** si vous le laissez sans surveillance.
- Veillez à **récupérer rapidement tous les documents imprimés** à l'imprimante.

SCHOLA EUROPAEA
Brussels III

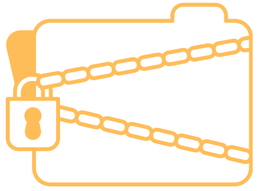
10 règles d'or pour la cybersécurité

Éviter les réseaux Wi-Fi publics - Utiliser un VPN

- **Évitez** le Wi-Fi public.
- Utilisez de préférence **le réseau Wi-Fi de l'école** et uniquement à des fins pédagogiques.
- Le personnel est invité à toujours se connecter au **réseau privé virtuel (VPN)** lorsqu'il travaille à distance.

Attention à l'hameçonnage

- **Lisez** attentivement les recommandations de l'école concernant le phishing.
- **Ne répondez jamais** et ne fournissez jamais vos informations personnelles ou celles d'autres personnes.
- **Exercez-vous** à la détection des tentatives d'hameçonnage.
- **Signalez** les tentatives d'hameçonnage à IXL-ICT@eursc.eu et supprimez l'e-mail/le texte ensuite.



Traitement des informations sensibles

- **Ne jetez jamais** d'informations sensibles (dossiers médicaux, données financières ou copies de documents d'identité) dans les poubelles jaunes ordinaires.
- **Broyez** tous les documents confidentiels ou sensibles.
- Eviter de discuter d'informations confidentielles dans des lieux publics de l'école. Essayez toujours de vous isoler pour éviter que quelqu'un n'entende votre conversation.

Attention au téléchargement

- N'utilisez que les **sites web et les plateformes officiels** pour télécharger des applications et des logiciels.
- Méfiez-vous des **types de fichiers inconnus** ; évitez de télécharger des fichiers exécutables (.exe) si vous n'êtes pas sûr de leur sécurité.
- Lancez toujours des **analyses antivirus** sur les fichiers téléchargés avant de les ouvrir.
- Sur les appareils de l'école, le téléchargement de logiciels doit être évité. Les logiciels sont installés par l'équipe informatique.

Signalement à l'équipe IT

Signalez tous les problèmes de sécurité à l'équipe IT de l'école lorsque vous remarquez :

- Un manquement au présent document;
- un incident de sécurité, suspecté ou confirmé, se produit (par ex. haque l'hameçonnage).

Contact : IXL-ICT@eursc.eu

SCHOLA EUROPAEA
Brussels III