FEDIL

Member News

ECOLE À DISTANCE : LES BONNES PRATIQUES DE CYBERSÉCURITÉ

Avec la fermeture des écoles, le travail à domicile est devenu la règle pour l'ensemble des élèves au
Grand-Duché de Luxembourg. Chacun doit s'adapter à de nouveaux outils et de nouvelles méthodes
de travail. Dans ce contexte, la cybersécurité ne doit pas être oubliée, afin que l'expérience pédagogique ne tourne pas au cauchemar.

Il y a principalement 3 points qui doivent être surveillés :
a. Le matériel (ordinateur, tablettes…)
b. Les applications
c. La connexion

Le matériel

1. Effectuez régulièrement les mises à jour sur le matériel utilisé pour les cours en ligne.
2. Utilisez de préférence un ordinateur dédié au travail scolaire. Si ce n'est pas possible, mettez
en place des comptes séparés pour les membres de la famille.
3. Eviter d'y connecter des interfaces (clés usb, cartes mémoire ou autre) dont l'origine est
incertaine.
4. Installez un logiciel antivirus et mettez-le à jour régulièrement.
5. Assurez-vous que votre ordinateur est verrouillé et stocké avec soin lorsqu'il n'est pas
utilisé.

Les applications

1. Utilisez uniquement les logiciels et plateformes mis à disposition par le Ministère de
l'Education pour le travail scolaire.
2. Veillez à mettre à jour tous les logiciels et applications installés sur votre ordinateur.
3. Professeurs : assurez-vous que vos élèves utilisent bien leur accès personnel.
4. Elèves et Parents : utilisez votre accès personnel en veillant à changer le mot de passe initial
qui vous a été fourni.

5. Modifiez le mot de passe par défaut que vous avez reçu pour accéder à ce compte. Utilisez
un mot de passe solide composé de lettres minuscules, de capitales, de chiffres et de
caractères spéciaux.
6. Transfert de données : utilisez uniquement les fonctions de partage des applications mises à
disposition par le Ministère de l'Education et non des services de transfert sur le cloud
public.
7. Utilisez uniquement votre adresse mail scolaire pour échanger des messages.

La connexion

• Ne vous connectez à aucun réseau public, inconnu ou non sécurisé
• Veillez à sécuriser correctement votre accès Wi-Fi à la maison (le réseau doit être crypté et
accessible uniquement avec un mot de passe).
• Connectez-vous aux réseaux 3G ou 4G si vous n'avez pas accès à une connexion Wi-Fi
sécurisée

Right Box

Soyez vigilants en consultant vos mails et les réseaux sociaux. De nombreux messages trompeurs
relatifs au Covid-19 circulent. Il s'agit notamment :
– de fake news. Pour rester informés sur l'actualité liée au Covid-19, optez plutôt pour les sites
officiels du gouvernement ou des médias reconnus ;
– de mails de phishing qui contiennent des liens vers de faux sites qui vous demandent vos
codes d'accès ;
– de messages d'arnaque qui vous proposent par exemple d'acheter des masques de
protection ou des remèdes contre le Coronavirus ;

Un seul conseil : réfléchissez avant de cliquer.

Communiqué par SECURITYMADEIN.LU