Sécurité numérique : Protéger au mieux vos données

1. Gestion des accès et des identifiants

Signalement de violations :
Signaler toute violation de son compte à l'administrateur EcoleDirecte, dès que possible, pour une réaction rapide et efficace.

Sécurité des mots de passe :
Choisir un mot de passe complexe en utilisant une combinaison de majuscules, minuscules, chiffres et caractères spéciaux pour renforcer la sécurité.

Renouvellement des mots de passe :
Changer régulièrement vos mots de passe, surtout en cas de doute sur leur confidentialité, pour prévenir les accès non autorisés.

Confidentialité lors de la saisie :
Saisir ses identifiants et mots de passe en privé, à l'abri des regards, pour protéger ses informations.

Gestion des mots de passe :
Gérer vos mots de passe via des logiciels dédiés et éviter l'enregistrement des mots de passe dans les navigateurs web pour une meilleure sécurité.

Déconnexion des sessions :
Déconnecter vos sessions EcoleDirecte sur PC après chaque utilisation, même brève, pour empêcher les accès non autorisés.

2. Précautions en ligne et avec les logiciels

Préférence pour les plateformes officielles :
Utiliser uniquement les sites et applications mobiles officiels Aplim pour éviter le vol de données personnelles via des plateformes non sécurisées.

Protection Antivirus :
Utiliser et mettre à jour une suite de sécurité antivirus pour se prémunir contre les logiciels malveillants et les virus.

Vigilance avec les pièces jointes :
Ne jamais ouvrir une pièce jointe aux extensions douteuses (.pif, .bat, .com, .lnk, etc…) pour éviter les infections par des malwares.

Méfiance envers les liens suspects :
Ne jamais cliquer sur un lien suspect, surtout s'il demande des identifiants, pour prévenir le « phishing ».

3. Maintenance et mises à jour

Mises à jour régulières :
Mettre à jour l'application mobile EcoleDirecte sur votre smartphone dès la disponibilité d'une nouvelle version pour bénéficier des dernières protections.

4. Sécurité réseau et matérielle

Sécurité des réseaux :
Se connecter à des réseaux privés pour éviter les risques liés à l'utilisation de réseaux publics non sécurisés (ex : restaurant, cinéma, bar, hôtel, …).

Prudence avec les supports amovibles :
Se méfier des clés USB et disques durs externes inconnus qui peuvent contenir des virus ou logiciels malveillants.

5. Sensibilisation et formation

Sensibilisation des utilisateurs :
Sensibiliser vos utilisateurs à la cybersécurité pour qu'ils adoptent une attitude vigilante et responsable en ligne.



Aplim

EcoleDirecte