Feuille d'information

«Utilisation d'applications sur des appareils mobiles employés à des fins professionnelles au sein de l'administration fédérale»

Que dois-je savoir?

L'utilisation d'applications informatiques sur les appareils mobiles à la Confédération est réglementée par la directive d'application pour la synchronisation des smartphones et tablettes E021.
E021 - Directive d'application pour la synchronisation des smartphones et tablettes

La présente feuille d'information contient les recommandations de la Confédération concernant l'utilisation d'applications sur les appareils mobiles, privés ou non, employés à des fins professionnelles. Elle s'adresse à l'ensemble du personnel de l'administration fédérale.

04/2023

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Centre national pour la cybersécurité NCSC

Installation parcimonieuse

Toute nouvelle application peut présenter un risque pour la sécurité informatique. C'est pourquoi il vous est conseillé de supprimer les applications dont vous n'avez plus besoin. Moins vous avez d'applications, plus il vous est facile d'en garder la vue d'ensemble et de limiter les risques informatiques. Vérifiez régulièrement les applications installées sur votre appareil.	**Recommandation** • N'installez que les applications dont vous avez réellement besoin. • Supprimez les applications que vous n'utilisez plus.

Mises à jour

Les applications qui ne sont pas à jour peuvent présenter un risque pour la sécurité informatique. Vérifiez régulièrement si des mises à jour sont disponibles et installez-les immédiatement.	**Recommandation** • Mettez à jour vos applications dès qu'une nouvelle version est disponible ou, idéalement, configurez-les de manière à automatiser les mises à jour.

Gestion des autorisations

Lorsque vous utilisez une application pour la première fois ou après une mise à jour, il vous est demandé de sélectionner les autorisations que vous souhaitez lui accorder. En configurant correctement votre appareil, vous pouvez empêcher que l'application n'accède à vos données personnelles.	**Recommandation** • N'accordez une autorisation (par ex. l'accès au carnet d'adresses) que si vous avez impérativement besoin de cette fonction. En cas d'incertitude, refusez l'autorisation. Il vous sera toujours possible de l'accorder plus tard dans le menu «Réglages». • Vérifiez les accès accordés à chaque application.

Réseaux sociaux

Vous pouvez installer les applications de réseaux sociaux (Instagram, TikTok, etc.) sur les appareils mobiles qui ont été mis à votre disposition à des fins de service. Sachez toutefois que ces applications peuvent obtenir des autorisations très étendues et sont connues pour collecter un nombre particulièrement élevé de données, comme les informations relatives à vos contacts.	**Recommandation** • Vérifiez que vous avez vraiment besoin des applications sur les appareils mobiles qui ont été mis à votre disposition à des fins de service. • Accordez-leur le moins d'autorisations possibles. • Consultez le guide de l'OFPER sur l'usage des médias sociaux.

Localisation

La localisation a le double inconvénient d'empiéter sur votre vie privée et de consommer de la batterie. Activez ce service manuellement quand vous utilisez une application qui le requiert. Vous trouverez la liste des applications qui demandent l'accès à votre localisation sous «Service de localisation».	**Recommandation** • Si vous n'avez pas besoin du service de localisation pour une application, désactivez-le dans le menu «Réglages», sous «Confidentialité».  • Souvent, il vous suffit de sélectionner l'option «Lorsque l'app est active» au lieu de «Toujours». 

Communications confidentielles

Si vous disposez du système MDM sur vos appareils mobiles, vous pouvez utiliser l'application «Threema Work» pour les communications qui doivent rester confidentielles (conversations téléphoniques, messages vocaux et écrits).	**Recommandation** • Utilisez les applications «Threema Work» ou «Skype for Business» pour les conversations sensibles, que vous les meniez par oral ou par écrit. • Pour les conversations qui doivent rester confidentielles, utilisez uniquement l'application «Threema Work». • Hormis les deux applications mentionnées ci-dessus, n'utilisez pas de services de messagerie fournis par un tiers pour vos conversations professionnelles. **Directive** E027 - Directive d'application Communication vocale chiffrée (CVC)

Symboles de la barre d’état

<table>
<tr><td rowspan="8">Regardez les symboles qui s’affichent dans la barre d’état, sur l’écran de votre appareil. Ils vous indiquent si une application collecte des données de localisation ou utilise des fonctions de partage. Si des tâches se déroulent sans que vous ne vous souvenez les avoir lancées, cherchez-en la cause en vérifiant quelles applications sont actives en arrière-plan.</td><td>

Recommandation

Faites attention aux symboles qui s’affichent dans la barre d’état de votre appareil mobile.

</td></tr>
<tr><td>Une application ou un site web utilise votre localisation.</td></tr>
<tr><td>L’appareil est connecté au réseau (par ex. une application échange des données sur le réseau).</td></tr>
<tr><td>Le transfert d’appels est activé.</td></tr>
<tr><td>Une application utilise le micro de l’appareil.</td></tr>
<tr><td>Une application utilise la caméra et peut-être le micro de l’appareil.</td></tr>
<tr><td>09:41 L’appareil est en train d’effectuer une prise de son ou une capture d’écran.</td></tr>
<tr><td>En cas d’activité suspecte, prenez contact avec le service d’assistance de votre fournisseur.</td></tr>
</table>

Utilisation à l'étranger

La plus haute prudence s'impose lors de voyages à l'étranger. Dans certains pays, les autorités douanières ont le droit d'examiner vos applications. Pour éviter tout désagrément, désinstallez les applications Secure MDM (Secure Mail, Secure Notes, Secure Tasks) avant d'entrer sur le territoire du pays en question. Si vous avez absolument besoin de certaines applications (par ex. en raison des directives du pays), utilisez un autre appareil mobile.	**Recommandation** • Lors de vos voyages à l'étranger, n'emportez que les appareils dont vous avez réellement besoin. • Des dispositions particulières s'appliquent aux personnes exposées qui voyagent sous le statut diplomatique, en particulier pour ce qui concerne la publication d'informations. Renseignez-vous auprès de votre office ou de votre assistance VIP sur les directives et les possibilités en la matière. • Conseils du Département fédéral des affaires étrangères pour les voyages à l'étranger: Conseils pour les voyages en bref • Conseils du NCSC pour les voyages à l'étranger: Voyages à l'étranger: redoublez de prudence

Changement d'appareil mobile

Après un changement d'appareil mobile, l'ancien contient toujours un grand nombre de données.	**Recommandation** • Supprimez vos données sur vos anciens appareils mobiles.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Centre national pour la cybersécurité NCSC