

Zeitschrift: Générations
Herausgeber: Générations, société coopérative, sans but lucratif
Band: - (2016)
Heft: 76

Artikel: Sécuriser son smartphone en cinq étapes
Autor: B.S.
DOI: <https://doi.org/10.5169/seals-830535>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

Download PDF: 15.03.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

Sécuriser son smartphone en cinq étapes

Pas besoin d'être un expert pour protéger le précieux contenu de votre téléphone. Voici quelques précautions de base.

Photos, e-mails, réservations, virements bancaires... Les smartphones mettent tout à portée de main. Sauf que en cas de perte ou de vol, c'est une véritable mine d'informations qui se retrouve à ciel ouvert. Il existe heureusement des solutions faciles et gratuites pour faire la nique aux intrus. B. S.

1 Activer le verrouillage

Le code PIN c'est bien... Mais il ne protégera votre téléphone que lors de l'allumage! Il faut donc activer la fonctionnalité de verrouillage qui s'enclenchera automatiquement après plusieurs secondes ou minutes d'inactivité sur l'appareil. C'est l'option essentielle contre les regards importuns! Votre portable exigera systématiquement un mot de passe, un dessin ou une reconnaissance digitale avant de libérer l'accès au contenu.

2 Non à la facilité!

Avec tous nos mots de passe, on est tenté d'accepter la saisie automatique pour se connecter à nos différents comptes. Problème: si votre téléphone tombe entre de mauvaises mains, un clic suffira pour accéder à vos données personnelles ou faire des transactions. Evitez donc d'enregistrer vos codes pour les applications contenant des données sensibles (e-banking, réservations, etc.) et déconnectez-vous après chaque usage. Certains smartphones permettent d'activer un mot de passe pour restreindre l'accès aux applications d'achats. Pensez aussi à activer cette option!



Pour éviter de recevoir pareil message, mieux vaut appliquer les conseils de sécurité donnés ici.

3 Sortir protégé

Au parc, au restaurant ou dans les gares, les wifi gratuits sont très pratiques. Il faut pourtant s'en méfier, car beaucoup ne sont pas protégés. Pour éviter que des malfaiteurs ne récupèrent vos données personnelles, le mieux serait de s'en passer. Mais si vous devez vraiment vous en servir, évitez impérativement de faire des achats ou des saisies de codes sur ces réseaux libres. Et, pour mieux vous protéger encore, désactivez les récepteurs wifi et Bluetooth lorsqu'ils ne sont pas nécessaires.

4 Surveiller à distance

Maintenant que le contenu est bien protégé, occupez-vous du contenant et installez une application de localisation. En cas de perte ou de vol, celle-ci permettra de tracer votre téléphone sur une carte et, si besoin, de lan-

cer un signal sonore ou de bloquer l'appareil. Seule condition pour que cela fonctionne: il faut avoir installé l'application avant la disparition du smartphone. Parmi les plus couramment téléchargées, *Mobile tracker Samsung Dive* pour les Samsung et *Localiser mon iPhone* pour les iPhone.

5 Tout mettre à l'abri

Perdre un objet de valeur, c'est déjà pénible. Mais perdre tout son contenu, c'est encore pire. Pour éviter ce scénario catastrophe, faites régulièrement une sauvegarde de votre téléphone sur votre ordinateur. Soit avec le logiciel gratuit fourni avec l'appareil, soit sur les services de stockage en ligne. Le site *iCloud.com* fait office de référence pour les iPhone et *OneDrive.com* cible davantage les utilisateurs d'Android. Tous les deux offrent un espace de stockage gratuit.