www.makeuseof.com /things-you-shouldnt-store-in-smartphone/

10 choses que vous ne devriez jamais stocker dans votre cellulaire

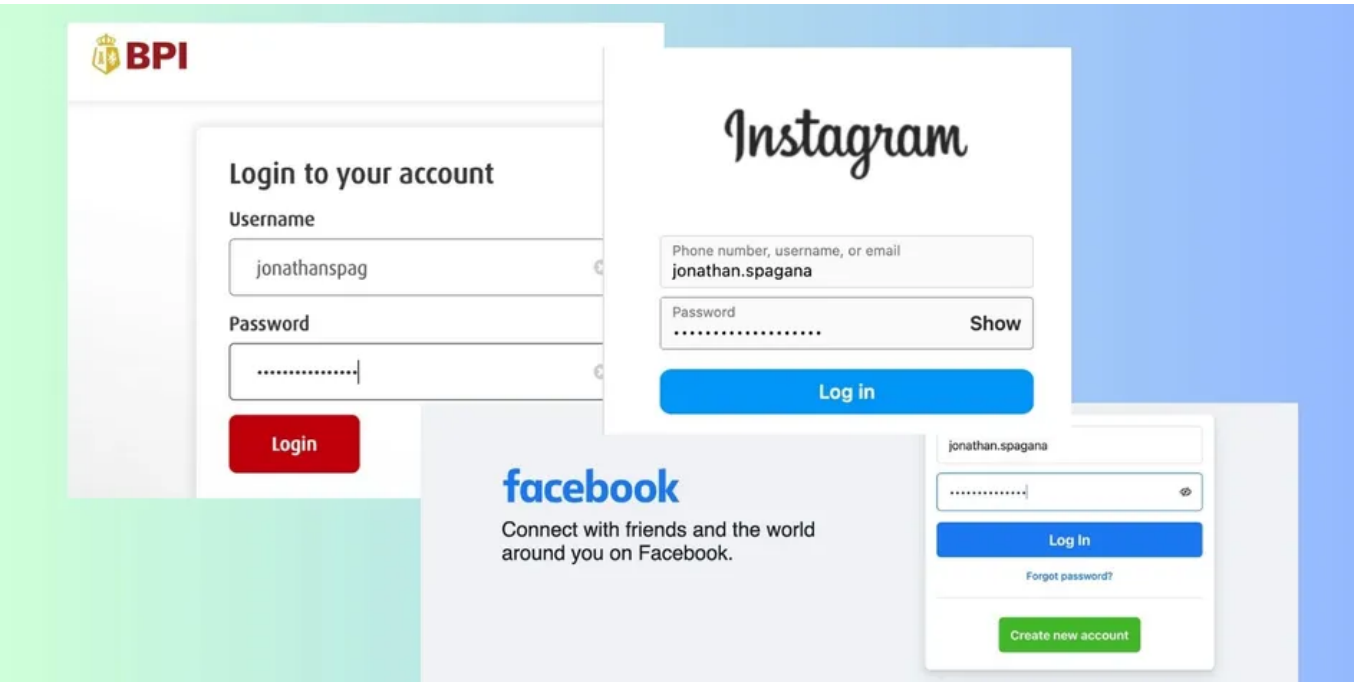
Nos cellulaires transportent une énorme quantité de données sur nous.
Et cela représente une grande opportunité pour les criminels...

Jose Luansing Jr. ⁝

La plupart des gens traitent leurs cellulaires comme des portefeuilles.
Ils stockent des copies numériques de leurs cartes de débit et de crédit, de leurs cartes de membre, de leurs pièces d'identité gouvernementales et de leurs billets de transport, entre autres éléments essentiels.
C'est plus facile que de transporter plusieurs cartes en plastique et en papier dans un portefeuille volumineux.

Bien que pratique, le stockage d'informations personnelles sur votre smartphone est risqué.
Les escrocs pourraient les faire glisser à travers diverses cyberattaques, du piratage NFC aux liens de phishing.
Vous vous exposerez à la fraude et au vol d'identité si vous ne supprimez pas ces éléments de votre appareil.

1. Listes maîtresses de mots de passe



La tenue d'une liste maîtresse de vos mots de passe crée un point de défaillance unique dans votre système de cybersécurité.
La perte de l'accès pourrait entraîner une chaîne de failles de sécurité.
Si votre téléphone est piraté ou volé, l'auteur aura également accès à vos comptes de messagerie, à vos profils de médias sociaux et à vos applications bancaires.

Mais cela ne veut pas dire que vous devriez remplacer les mots de passe complexes par des mots de dictionnaire courts et faciles à retenir.
Des identifiants de connexion solides constituent votre première ligne de défense contre les pirates.
Recycler les mêmes combinaisons faibles pour que vous vous en souveniez est aussi mauvais que de garder des listes maîtresses de mots de passe sur votre téléphone.

Si vous oubliez toujours vos identifiants de connexion, investissez dans un gestionnaire de mots de passe sécurisé.
Ils stockent toutes vos combinaisons nom d'utilisateur-mot de passe derrière un coffre-fort chiffré - vous n'avez besoin de vous souvenir que d'un seul mot de passe principal.

2. Votre adresse personnelle

Débarrassez-vous des fichiers qui affichent votre adresse personnelle.
Les escrocs pourraient utiliser votre carnet d'adresses, vos relevés de facturation et vos factures de services publics pour vous suivre.
C'est une erreur coûteuse qui met en danger votre famille.
Ils peuvent vous envoyer des menaces écrites, vous traquer ou même s'introduire dans votre espace de vie.

Désactivez également les services de localisation de votre téléphone.
Plusieurs applications de médias sociaux publient votre emplacement en direct lorsque vous téléchargez des messages, partagez des histoires ou allez simplement en ligne. Prenez la fonctionnalité Personnes à proximité de Telegram, par exemple.
Il alerte les comptes Telegram en utilisant la même fonctionnalité si vous êtes à moins de deux kilomètres de leur emplacement actuel.

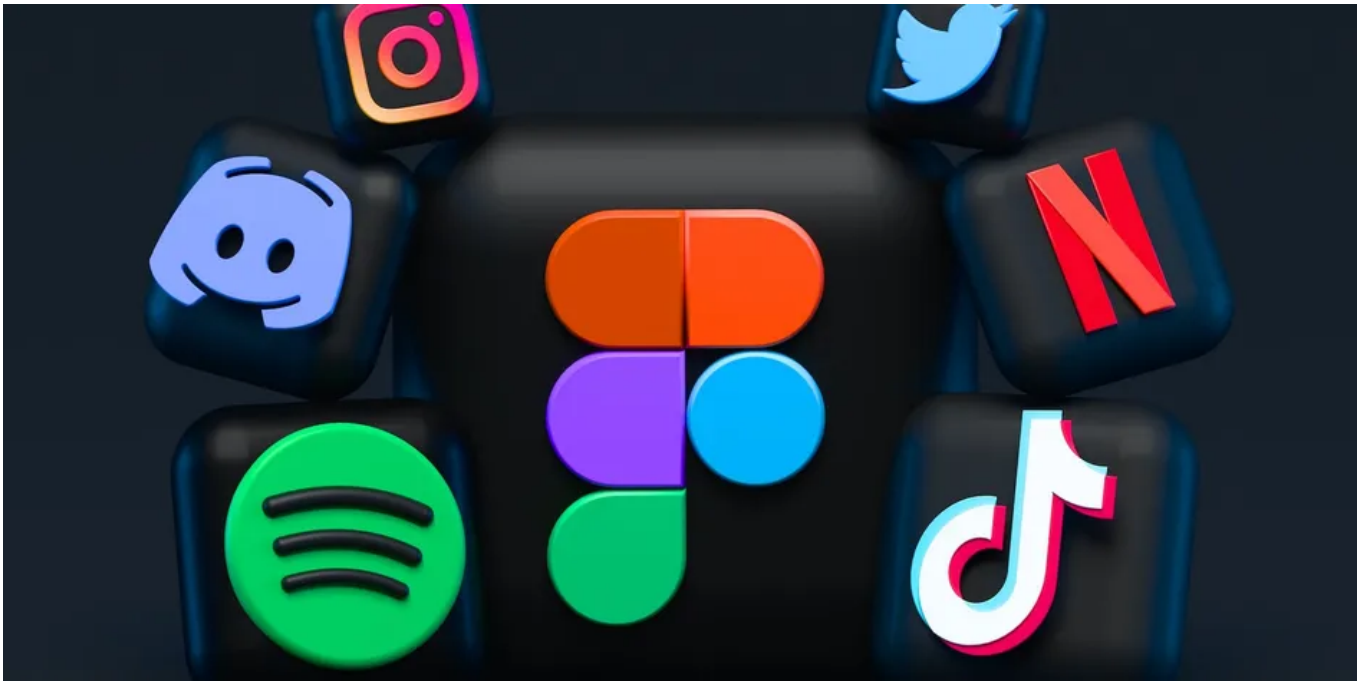
Arrêtez de stocker les numéros de contact sous des étiquettes reconnaissables.
Les voleurs d'identité peuvent usurper votre identité en volant votre téléphone et en envoyant des messages alarmants à tous vos proches.
Ils sauront immédiatement qui cibler.

Au lieu de définir des étiquettes comme Maman, Papa, Mon mari ou BAE, utilisez des étiquettes discrètes comme leur prénom et leur nom de famille.
Cela empêche les pirates d'exploiter vos relations. Leurs attaques d'usurpation d'identité sont moins susceptibles de fonctionner s'ils ne savent pas comment vous vous adressez à vos amis et à vos proches.

4. Photos des pièces d'identité gouvernementales

Vous pouvez utiliser des photos de vos pièces d'identité gouvernementales pour la vérification d'identité dans plusieurs environnements occasionnels et professionnels. Disons que vous visitez un état différent.
Prendre des photos de vos cartes d'identité et cartes est beaucoup plus pratique que de les transporter pendant votre voyage.
De même, ils sont utiles en cas d'urgence, comme le dépôt de rapports de police ou l'admission imprévue à l'hôpital.

Malgré ces avantages, stocker des photos de vos pièces d'identité gouvernementales est encore trop risqué.
Les voleurs d'identité n'hésiteront pas à les exploiter pour des activités frauduleuses. Selon les informations que vous exposez, ils pourraient voler vos déclarations de revenus, contracter des prêts sous votre nom ou blanchir de l'argent sale.



Laisser vos comptes de médias sociaux connectés sur votre smartphone est un risque de sécurité critique.
Tout le monde peut y accéder après avoir déverrouillé votre appareil.
Qu'un ami emprunte votre téléphone ou qu'un voleur vous le vole, il pourrait fouiner dans vos profils derrière votre dos.

L'approche la plus simple consiste à vous déconnecter de vos comptes de médias sociaux.
Mais si votre travail ou vos affaires personnelles exigent que vous soyez constamment en ligne, limitez l'accès aux applications avec une autre couche de sécurité.
Vous pouvez verrouiller les applications iPhone avec Face ID ou Touch ID et définir des mots de passe sur les applications Android.

6. Numéros de compte bancaire et NIP

Ne stockez jamais vos numéros de compte bancaire et vos NIP dans votre téléphone intelligent, surtout si vous l'utilisez pour les services bancaires mobiles.
La liste de ces codes crée un maillon faible dans vos applications financières.
Comme avec vos mots de passe, vous devez soit les mémoriser, soit utiliser une application de gestion de mots de passe sécurisée.

Soyez très prudent avec votre appareil si vous utilisez des applications bancaires mobiles. Les escrocs bombardent les victimes de spams et de pages de phishing usurpant l'identité de leurs banques émettrices de cartes - n'entrez vos identifiants de connexion que sur des plateformes vérifiées.

7. Empreintes digitales et reconnaissance faciale

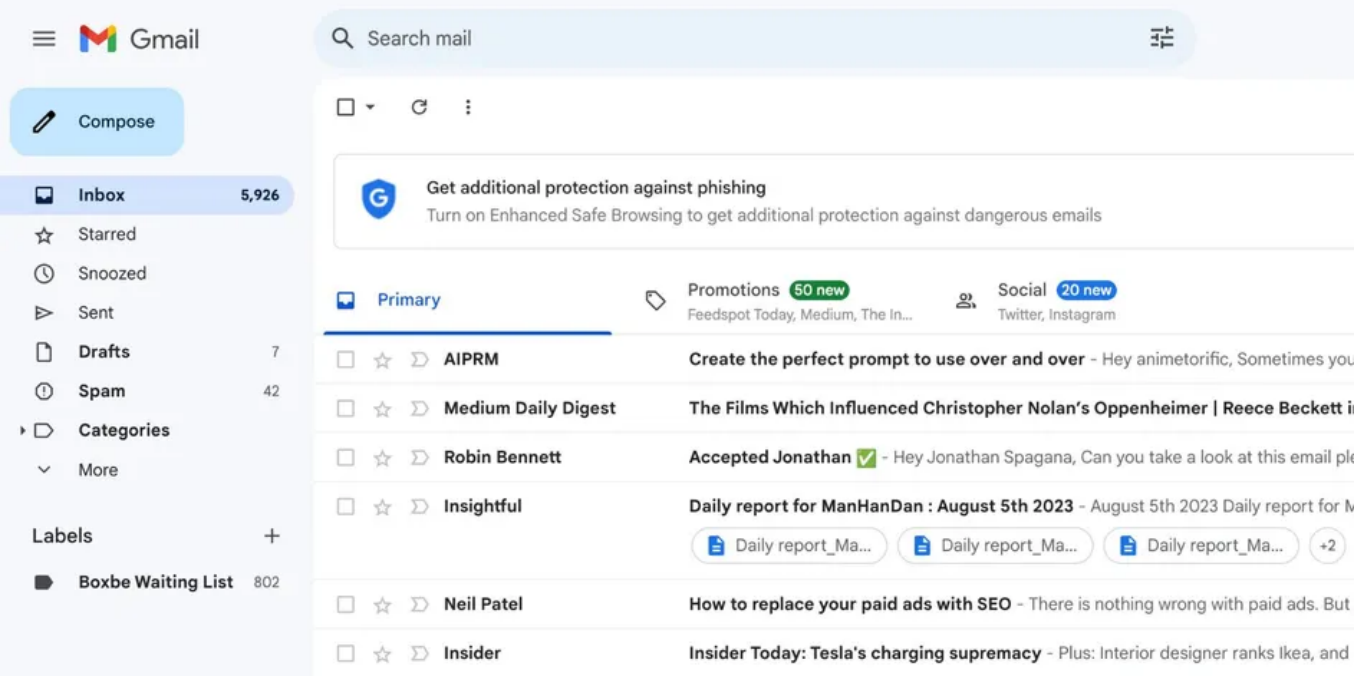
Les technologies de numérisation des empreintes digitales et du visage ne sont pas infaillibles.
Bien qu'ils vous permettent de déverrouiller vos appareils plus rapidement, ils sont également vulnérables à diverses astuces de piratage.
Si quelqu'un essaie de vous apaiser, il pourrait facilement tenir votre doigt sur votre smartphone, par exemple.

Nous vous suggérons de vous en tenir aux mots de passe texte et numériques pour votre sécurité.
Exécutez vos combinaisons à travers les vérificateurs de force de mot de passe et voyez combien de temps avant que les pirates ne les contournent.
Idéalement, définissez des chaînes alphanumériques ou de longs codes numériques personnalisés.

8. Photos et vidéos privées NSFW

Supprimez les photos explicites de vous-même ou verrouillez-les dans des dossiers protégés par mot de passe.
Les stocker négligemment dans votre galerie de photos vous rend vulnérable à l'extorsion sexuelle.
Les agresseurs vous feront probablement chanter pour obtenir plus d'images d'adultes ou d'argent.

9. Courriels et messages confidentiels



La plupart des gens ne réalisent pas la quantité de données sensibles contenues dans leurs messages.
Les criminels peuvent rassembler diverses informations provenant de vos applications de messagerie instantanée, de vos messages texte et de vos courriels pour exécuter des attaques frauduleuses.
Ils pourraient même frauder votre réseau en volant votre identité.

Organisez donc votre boîte de réception plus souvent pour empêcher les escrocs d'exploiter vos messages privés.
Accumuler des années de conversations sur votre téléphone est un risque inutile – prenez l'habitude de supprimer celles dont vous n'avez pas besoin.

Méfiez-vous des autres erreurs de sécurité de messagerie que les gens commettent inconsciemment, comme l'utilisation de mots de passe simples et la configuration de comptes MFA sur un seul appareil.

10. Documents et documents sensibles

De nombreuses personnes enregistrent sans réfléchir des documents contenant des informations personnelles identifiables (PII) sensibles sur leurs appareils.
Prenons l'exemple des déclarations de revenus.
Les contribuables qui produisent toujours leurs impôts en ligne peuvent conserver leurs formulaires IRS, leurs numéros SSS et les détails de leur employeur sur leurs smartphones.
Bien que pratique, imaginez combien de dommages les voleurs d'identité pourraient faire avec ces informations.

Et cette habitude s'étend à d'autres documents formels.
Les gens ont tendance à oublier leurs anciens fichiers, y compris ceux qui contiennent des données personnelles, médicales et professionnelles confidentielles.
Certains les laissent même dans des systèmes de stockage numérique abandonnés.

Commencez à vous débarrasser des divers encombrements numériques de votre téléphone.
Supprimez définitivement les fichiers confidentiels une fois que vous n'en avez plus besoin et exécutez vos anciens périphériques de stockage via des déchiqueteuses de fichiers numériques.

Débarrassez votre smartphone de vos IPI excessives

Soyez conscient des données que vous stockez sur votre cellulaire.
Supprimez les copies inutiles de vos informations personnelles et financières ou cachez-les dans des applications protégées par mot de passe.

Et méfiez-vous des autres mauvaises cyber-habitudes que la plupart des gens commettent souvent.
Des erreurs apparemment mineures comme partager trop de choses sur vous-même en ligne, faire négligemment confiance aux VPN gratuits et accumuler trop de fichiers vous mettent en danger.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230815
"C'est ensemble qu'on avance"