PRECONISATIONS 2025

Outils et bonnes pratiques pour protéger ses données dans le cadre de la vie privée

Savoir Faire

- Chiffrer ses données sensibles
- Sauvegarder régulièrement ses données sensibles
- Utiliser un gestionnaire de mots de passe
- Protéger ses données en utilisant des messageries sécurisées
- Mettre à jour ses logiciels
- Ne pas naviguer avec des droits administrateurs
- Recourir à la double authentification dès que possible
- Utiliser un VPN pour une connexion sécurisée
- Redémarrer régulièrement son téléphone
- Ne pas utiliser de chargeurs publics ou inconnus

Savoir Être

- Séparer les usages professionnels et personnels
- Maîtriser sa communication sur les réseaux sociaux
- Ne pas laisser ses outils nomades sans surveillance
- Ne pas exposer de données sensibles dans des lieux public
- Se méfier des clés USB
- Se méfier des courriels douteux et des pièces-jointes
- Désactiver par défaut wifi, bluetooth et géolocalisation
- Installer les applications depuis des sites fiables
- N’activer que les accès nécessaires pour les applications
- Limiter le nombre d’applications sur ses outils

Protéger ses données sensibles avec des outils de chiffrement

Zed!

LockFiles

VeraCrypt

Des gestionnaires pour générer et protéger des mots de passe robustes

Keepass
https://keepass.info

Dashlane

LockPass

Bitwarden

Utiliser des messageries instantanées sécurisées

Olvid
pour un usage personnel
ou professionnel

Tchap
pour échanger avec
l'administration

Signal
pour les appels gratuits

Citadel
pour les entreprises

Protéger ses données sur Internet et dans un cloud

Cryptobox

Swisstransfer
(usage privé gratuit)

Oodrive

Pour choisir son VPN

VPN Mon Ami
https://vpnmonami.com

Un univers « tout en un »

Proton Mail *

Proton VPN *

Proton Pass

Proton Drive

* Existe en version gratuite mais limitée

Pour naviguer sur Internet

Brave

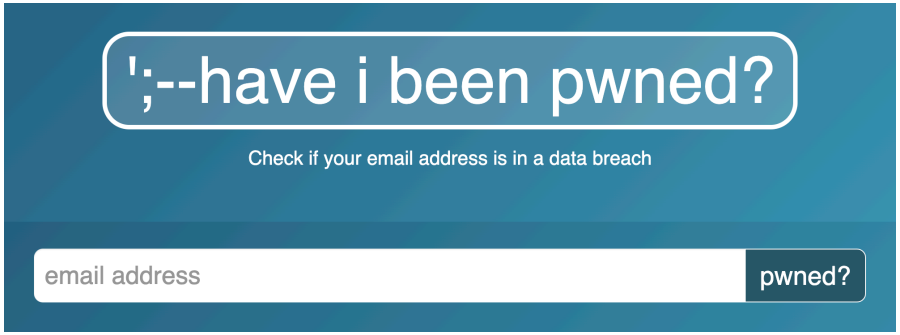
DuckDuckGo

Firefox
navigateur

+

Qwant
moteur de recherche

Mettre en place une veille sur ses adresses de courriel



https://haveibeenpwned.com

En cas de compromission : changer de mot de passe !

Prévenir les usurpations d'identité en appliquant un filigrane sur ses documents

https://filigrane.beta.gouv.fr

→ Cybermalveillance (Cyber 17)

si vous êtes victime d'une attaque informatique
https://www.cybermalveillance.gouv.fr/17cyber

→ Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)

choisir ses outils numériques et se former à la cybersécurité
https://www.cyber.gouv.fr

→ Commission Nationale Informatique et Liberté (CNIL)

exercer ses droits et protéger les données sensibles
https://www.cnil.fr

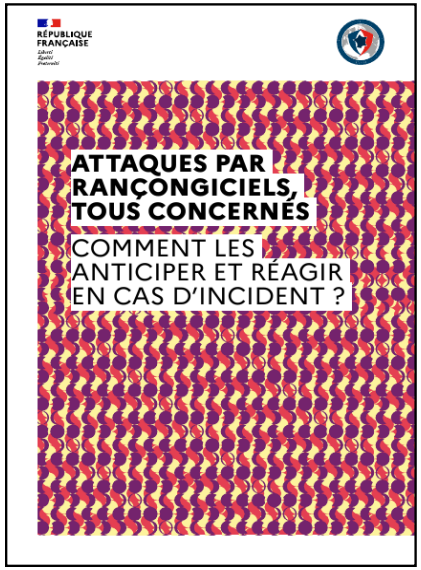
→ Ministère de l'Europe et des Affaires Etrangères

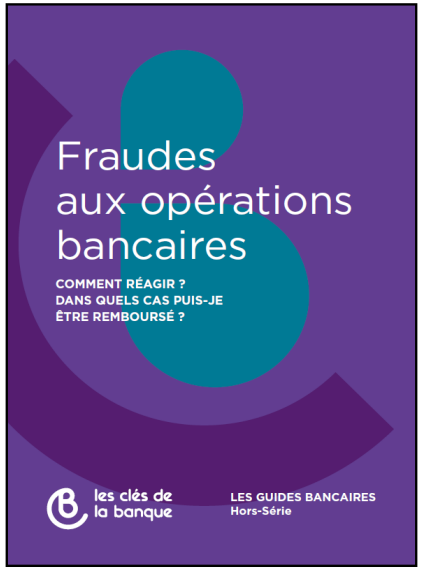
des conseils aux voyageurs et des fiches pour les pays à risque
https://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs

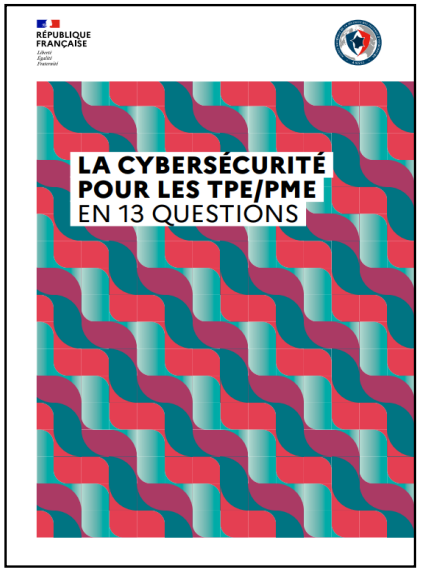
→ Direction Générale de la Sécurité Intérieure (DGSI)

pour signaler des faits de radicalisation
https://www.dgsi.interieur.gouv.fr/nous-contacter-radicalisation

Guides pratiques pour les PME







Les Flashs Ingérences de la DGSI

https://www.dgsi.interieur.gouv.fr

2 INTRUSION DANS LES TÉLÉPHONES PORTABLES DE DEUX SALARIÉS D'UNE SOCIÉTÉ FRANÇAISE LORS D'UN CONTRÔLE AÉROPORTUAIRE À L'ÉTRANGER.

Alors qu'ils s'apprêtaient à rentrer en France à la suite d'un événement à l'étranger auquel ils avaient été conviés dans un cadre professionnel, deux salariés d'une société française ont été interrogés durant plusieurs heures à l'aéroport par les autorités locales.

Ces entretiens ont notamment porté sur le déroulement de leur visite dans ce pays, leurs parcours professionnels respectifs et les contrats internationaux de leur société. Les agents locaux de l'aéroport ont notamment indiqué aux deux salariés français qu'ils étaient susceptibles d'être de nouveau interrogés lors d'un futur séjour dans ce pays, y compris si ce séjour se déroulait dans un cadre privé.

Les salariés ont été contraints de remettre aux agents leurs téléphones professionnels et personnels ainsi que leurs codes de déverrouillage. Les appareils ont été restitués à l'issue des interrogatoires, avec des traces évidentes d'intrusion dans leurs systèmes : les batteries des téléphones étaient totalement rechargées alors qu'elles ne l'étaient qu'à moitié avant les interrogatoires, les icônes avaient été déplacées et les menus de réglages avaient été configurés dans la langue du pays étranger.

Une analyse technique, conduite par la DGSI au retour des salariés en France, a permis de constater l'installation d'une application permettant la récupération des données de messagerie, d'appels, de navigation et de géolocalisation.

Le service a recommandé à la société l'usage d'appareils électroniques dédiés aux déplacements à l'étranger, afin de limiter le risque de captation d'informations en ne stockant sur ces appareils que les données nécessaires aux seuls besoins de la mission.

Commentaires

Le ciblage de ressortissants français travaillant pour des entreprises stratégiques lors de déplacements à l'étranger a fait l'objet d'une vigilance croissante de la part de la DGSI au cours des dernières années. Mode opératoire fréquemment utilisé par plusieurs États étrangers afin de collecter des renseignements sur leur territoire, le contrôle aéroportuaire présente un risque important en matière de captation de données ou de piégeage informatique.

Au cours des dernières années, la DGSI a régulièrement consacré des éditions du « flash ingérence » aux risques associés aux déplacements à l'étranger, qu'ils soient effectués dans un cadre public ou privé. De même, la thématique de la protection des données informatiques et des vigilances élémentaires liées au transport et à l'usage d'appareils électroniques a fait l'objet de nombreuses préconisations du service. La mise en place de bonnes pratiques avant, pendant et après chaque déplacement à l'étranger permet de limiter considérablement les risques d'ingérence étrangère.