

FUITES DE DONNÉES : COMMENT RÉAGIR ?

L'ADMINISTRATION FISCALE NE VOUS DEMANDERA JAMAIS
D'INFORMATIONS CONFIDENTIELLES PAR COURRIEL, SMS OU TÉLÉPHONE

1 CONSERVER LA MAÎTRISE

- Méfiance : SMS / mail / appel "urgent", provenant de "banque", "assurance", "mutuelle", etc.
- Ne jamais donner le code (SMS / mot de passe / numéro de CB / données sensibles) à des personnes qui vous contactent inopinément ;
- Recontacter *via* le site, l'application ou le numéro de téléphone officiel. Ne jamais utiliser le lien proposé ;
- Changer le mot de passe du service concerné, surtout si réutilisé ailleurs.



2 SURVEILLER CE QUI COMPTE

- Surveiller tout compte bancaire, crédit ou contrat ouvert à votre nom sans votre accord, en recherchant dans le fichier FICOBA sur votre espace impots.gouv.fr ;
- Vérifier les opérations inhabituelles ;
- En cas de doute : prévenir la banque ;
- Restez vigilant dans le temps, vos données peuvent être réutilisées pendant plusieurs années.



3 ÊTRE GUIDÉ, SIGNALER

- Si fraude / usurpation : conserver les preuves (captures écran, messages, etc.), déposer plainte ;
- Réflexe : appel 17, Ma Sécurité, 17Cyber ;
- Si vos données apparaissent sur des plateformes en ligne, demander leur suppression au site / service qui diffuse vos informations ;
- Ressources : suivre l'actualité sur impots.gouv.fr et Cybermalveillance.gouv.fr.

