

Fuites de données : comment réagir ?

L'administration fiscale ne vous demandera jamais d'informations confidentielles par courriel, sms ou téléphone?

Conserver la maîtrise

- méfiance : sms / mail / appel "urgent", provenant de "banque", "assurance", "mutuelle", etc.
- ne jamais donner le code (sms / mot de passe / numéro d 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.

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.

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.

Besoin d'aide ? Vous pouvez appeler le 0 809 401 401 (service gratuit + prix appel)