

Consignes de sécurité pour les Professionnels ou les Entreprises

Afin de vous aider à lutter efficacement contre toute tentative de fraude, votre banque vous recommande de respecter les principes suivants :

Principe n°1 : maintenir un environnement informatique sûr.

- Mettez à jour votre matériel informatique* pour éviter des difficultés de compatibilité.
- Equipez votre matériel informatique* d'anti-virus et de pare-feu (firewall), régulièrement mis à jour.



Ne téléchargez jamais de logiciel de prise en main de votre matériel informatique sous divers prétextes (tests, ...).

Ne cliquez jamais sur un lien hypertexte ou fichier dans un mail, même si votre banque y est mentionnée.

Principe n°2 : prendre en compte les consignes communiquées par votre banque.

- Déconnectez-vous systématiquement de votre espace personnel à la fin de votre navigation.
- Si vous êtes titulaire d'une solution d'authentification (Safetrans, KSign, autre certificat électronique...), utilisez-la systématiquement pour réaliser vos opérations. A la fin de votre navigation, déconnectez la clé USB ou le boîtier de votre matériel informatique et conservez-les dans un lieu sécurisé.
- Veillez à utiliser le même niveau de sécurité pour toutes les personnes accédant au même espace personnel.
- Consultez régulièrement les informations sécuritaires sur le site de votre banque.



Ne communiquez jamais vos données confidentielles permettant l'accès à votre espace personnel ou à la réalisation d'opérations.

N'effectuez jamais d'opérations de paiement (virements,...) à la demande de personnes prétendant appartenir à votre banque (prétexte de test informatique, vérification SEPA...).

Principe n°3 : définir une stratégie de prévention de la fraude.

- Rédigez des procédures internes et assurez-vous de les faire respecter.
- Mettez en place les contrôles manuels et automatiques nécessaires à la prévention de la fraude.
- Sensibilisez régulièrement l'ensemble de vos collaborateurs aux différents types de fraude et à leur prévention.



Nos conseils pour optimiser la sécurité au sein de votre entreprise :

Limitez les accès Administrateur sur votre matériel informatique* afin d'éviter des téléchargements de logiciels malveillants.

Limitez au plus juste le nombre de postes informatiques* pour réaliser vos opérations bancaires.

* ordinateur, smartphone, tablette ou tout autre appareil électronique ayant un accès à internet.