

Les bonnes pratiques de sécurité sur Internet

Les conseils suivants vous permettent de sécuriser vos paiements en ligne et de protéger vos informations personnelles.

- [Sécurité des formulaires d'inscription et de paiement en ligne](#)
- [Connexion à vos Espaces sécurisés](#)
- [Pertinence du mot de passe](#)
- [Sécurité de votre mobile](#)
- [Confidentialité sur les forums et réseaux sociaux](#)

Sécurité des formulaires d'inscription et de paiement en ligne

Les navigateurs Internet (Internet Explorer, Google Chrome, Mozilla Firefox...) utilisent des protocoles qui sécurisent vos échanges sur Internet par des règles de cryptage et d'authentification des sites.

Néanmoins, au moment de saisir vos informations personnelles dans un formulaire ou lors d'un paiement en ligne, vérifiez toujours si le site est sécurisé. Comme le montre l'image au dessus, une page internet sécurisée est indiquée par un cadenas et son adresse commence par « **https://** ».

Ne communiquez jamais vos coordonnées bancaires sur des sites qui ne disposent pas d'un niveau de sécurité suffisant ou qui ne mentionnent pas explicitement que le paiement est sécurisé.

Connexion à vos Espaces sécurisés

La plupart des espaces sécurisés vous permettent de vérifier que vous êtes le dernier utilisateur en vous indiquant la date et l'heure de dernière connexion notamment. Si cette info est présente prêtez-y attention.

Le + Carrefour Banque & Assurance :

Sur votre Espace Client la date et l'heure de la dernière connexion sont rappelés au-dessus de vos noms et prénoms. Important, pensez à vous déconnecter de votre Espace Client avant de fermer la fenêtre de votre navigateur.

Pertinence du mot de passe

Pour être efficace, votre mot de passe ne doit pas reprendre votre date de naissance numéro de téléphone, nom, prénom etc. Modifiez le mot de passe de chacun de vos espaces personnels si vous avez un doute sur leurs utilisations frauduleuses.

N'utilisez pas le même mot de passe et pensez à le changer régulièrement. Vérifiez le niveau de sécurité de vos mots de passe à la création de vos comptes utilisateurs. Un mot de passe sécurisé comprend plusieurs caractères différents : majuscules, minuscules, chiffres, caractères spéciaux.

Exemple : ACE12#orange

Connectez-vous à vos comptes utilisateurs depuis votre propre ordinateur et/ou téléphone personnel. Si vous utilisez l'ordinateur d'un cybercafé ou celui d'un tiers, pensez toujours à vous déconnecter de votre session utilisateur. Evitez d'enregistrer vos mots de passe sur votre poste et d'autant plus un poste qui ne vous appartient pas.

Sécurité de votre mobile

Des applications malveillantes peuvent pirater votre téléphone pour voler les informations personnelles qu'il contient ou encore contrôler votre appareil et effectuer des opérations à votre insu.

- Avant de télécharger une application, vérifiez les commentaires associés, certains utilisateurs peuvent avoir signalé un problème.
- Pensez à mettre à jour vos applications, cela peut permettre de corriger des failles.
- Evitez de débrider ou jailbreaker votre téléphone, cette action qui permet de déverrouiller l'ensemble des fonctionnalités du système d'exploitation rend vulnérable votre téléphone mobile.
- Verrouillez votre clavier avec un code d'accès

Confidentialité sur les forums et réseaux sociaux

Quand vous êtes sur des forums, des réseaux sociaux, ce que vous y dites est consultable par tous et peut être utilisé contre vous. Ne divulguez pas d'informations qui pourraient être utilisées contre vous. Paramétrez bien la confidentialité de vos informations.