Crédit Mutuel de Bretagne



Adoptez les **bons réflexes** sur le web !

Mieux vaut prévenir que guérir !

Un achat sur internet n'est pas plus risqué qu'un achat en magasin ou un retrait au distributeur automatique. Mais l'adoption de bonnes pratiques sur le web vous évitera d'avoir à effectuer des démarches après un piratage.

Suivez le guide et naviguez sereinement sur internet !

Les règles du mot de passe



Avez-vous choisi des mots de passe robustes ?

Malgré les recommandations de la plupart des sites web à utiliser des mots de passe complexes, il apparaît que le mot de passe le plus utilisé est 123456. Un mot de passe piraté peut entrainer un vol de données, de coordonnées bancaires, un dépôt de plainte... Pour éviter de faciliter à ce point le travail de hackers, voici quelques conseils pour choisir un bon mot de passe :

> Choisissez un terme non-signifiant, c'est-à-dire absent de tout dictionnaire.

> Evitez l'emploi de données personnelles, de suites logiques, de dates historiques, etc.

> Alternez les chiffres et les lettres.

> Ne communiquez jamais votre mot de passe.

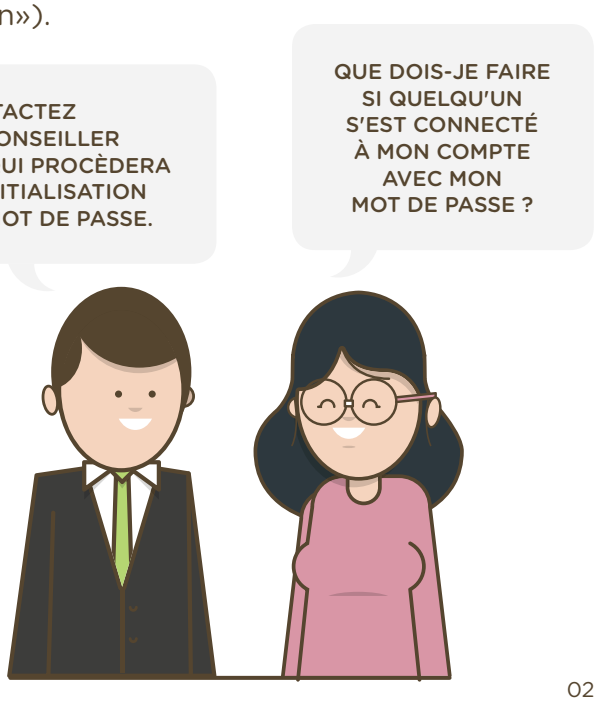
> N'inscrivez pas votre mot de passe sur un papier.

> Même si il est tentant d'enregistrer votre identifiant/mot de passe dans votre navigateur internet, ne le faites jamais. Un pirate peut récupérer ces données à la moindre intrusion sur votre ordinateur.

> Changez régulièrement votre mot de passe et ne réutilisez jamais un ancien mot de passe. Ceci permet de réduire le risque lié à l'intrusion d'un pirate sur votre ordinateur.

> Une bonne méthode est de créer une phrase à partir de lettres et chiffres (exemple : 2mainmat1, pour «demain matin»).

"Le mot de passe **le plus utilisé sur internet est 123456.**"



Le **Phishing** c'est quoi ?



Pour votre sécurité, ne communiquez jamais vos identifiants sur une page web accessible depuis un e-mail.

Le phishing consiste à vous adresser **un courriel non sollicité (spam) en se faisant passer, soit pour une société au nom et à la réputation largement reconnus, soit pour votre établissement bancaire.**

Sous un faux prétexte (exemple : mise à jour de vos données), le mail vous invite à cliquer sur un lien et à vous authentifier à l'aide de vos identifiant et mot de passe.

Le lien fourni vous conduit vers un site Internet identique en tout point à votre site habituel mais à l'adresse subtilement modifiée. Il ne reste plus au pirate qu'à enregistrer par le biais de ce faux site vos identifiant et mot de passe au moment de leur saisie.

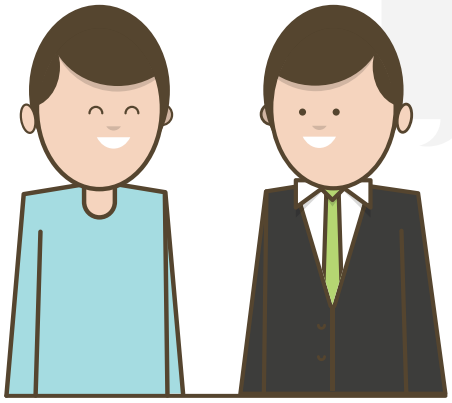
Désormais en possession de vos identifiants, le pirate peut commettre son forfait et se connecter à votre place sur le site de banque à distance ou revendre vos données.

COMMENT RECONNAITRE UN MAIL FRAUDULEUX ?

LES MAILS FRAUDULEUX IMITENT DES MAILS DE GRANDES ENTREPRISES ET, EN CELA, PEUVENT ÊTRE DIFFICILES À DÉMASQUER.

COMMENCEZ PAR VÉRIFIER L'ADRESSE E-MAIL DE L'ÉMETTEUR DU MAIL. PAR EXEMPLE, UN MAIL EMIS PAR LE CMB SERA OBLIGATOIREMENT AU FORMAT @CMB.FR.

PENSEZ ÉGALEMENT À VÉRIFIER L'ADRESSE QUI S'AFFICHE DANS VOTRE NAVIGATEUR INTERNET SI VOUS AVEZ CLIQUÉ SUR UN LIEN.



Comment **se protéger du Phishing ?**



Comment réagir en cas de doute ?

> **Ne communiquez jamais vos identifiants et coordonnées bancaires par mail** ou sur une page web accessible depuis un e-mail. Accédez uniquement à votre site de banque à distance en saisissant l'adresse du site dans le champ de saisie de votre navigateur.

Utilisez des navigateurs à jour, souvent équipés d'un filtre anti-phishing.

> Si le mode d'authentification de votre site a subitement changé sans que vous n'en ayez été averti au préalable, ne saisissez aucune donnée et prenez contact avec l'assistance téléphonique de votre site bancaire.

> Avant de saisir vos identifiant et mot de passe, assurez-vous que l'adresse de votre site bancaire commence bien par le terme «https://» et vérifiez son authenticité (certificat de sécurité) en cliquant sur le petit cadenas situé en bas à droite ou dans la barre d'adresse de votre navigateur.

> **Ne communiquez à personne** vos identifiant et mot de passe, ni vos codes de validation reçu par SMS.

Mettez-vous à jour !

57%

Le **pare-feu (ou firewall)** bloque les intrusions sur votre ordinateur, tablette ou smartphone. **L'antivirus** permet de nettoyer les fichiers infectés. Mais pour que ces outils indispensables - même sur smartphone - soient réellement efficaces, pensez à effectuer leur mise à jour régulièrement !

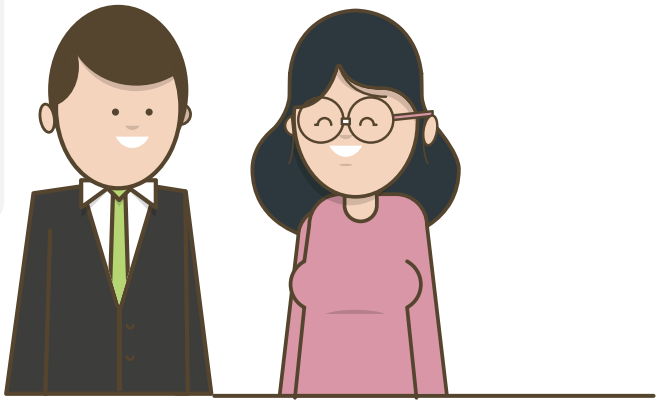
Les équipes de développement de vos **navigateurs internet** et, de manière générale, de **vos programmes** proposent aussi régulièrement des mises à jour de sécurité, corrigeant les éventuelles failles exploitées par les pirates. Pensez à les appliquer pour protéger vos données !

Quant à votre smartphone ou votre tablette, téléchargez uniquement les applications disponibles sur les stores Google, Apple et Microsoft. Ces derniers sont les garants de la propreté des applications qu'ils proposent !

"Un pare-feu permet de vous protéger des tentatives d'intrusions des pirates sur votre ordinateur (réseau local et Internet)"

COMMENT METTRE À JOUR MES PROGRAMMES?

SOUVENT, LES PROGRAMMES PROPOSENT LA MISE À JOUR AUTOMATIQUE.
SI CE N'EST PAS LE CAS, PENSEZ À REGARDER DANS LES MENUS DU LOGICIEL L'ONGLET «MISE À JOUR». SUR TABLETTE ET SMARTPHONE,
VOUS RECEVEZ UNE NOTIFICATION VOUS INCITANT À PROCÉDER AUX MISES À JOUR. ADOPTEZ LE BON RÉFLEXE :
APPLIQUEZ LES DIRECTEMENT !



Soyez vigilant

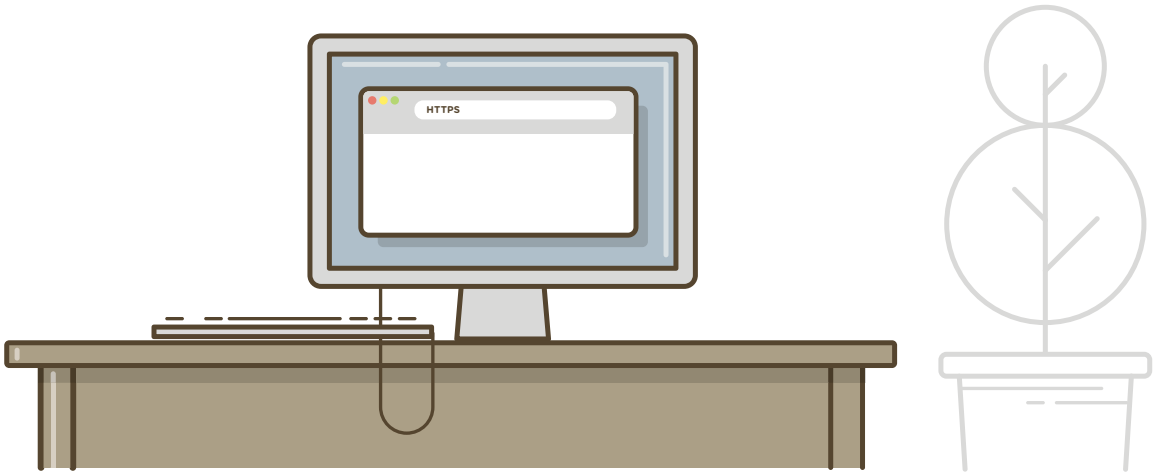


La meilleure des protections sur le web, c'est vous-même et vos bonnes habitudes ! Par exemple, quand vous **installez un programme**, faites attention aux cases pré-cochées : elles vont bien souvent installer sur votre ordinateur des programmes non-désirés. Prenez l'habitude de décocher ces cases malicieuses à chaque installation.

Quand vous souhaitez effectuer un achat sur un site web que vous connaissez, vérifiez la présence du **HTTPS** dans la barre d'adresse. En cas de doutes, effectuez une recherche sur le commerçant en ligne sur un moteur de recherche, en tapant par exemple «fraude + nom du site».

Pensez également à ne pas divulguer sur le web des informations compromettantes : ne renseignez pas des données sensibles sur les **réseaux sociaux ou forums**, et ne communiquez jamais vos **mots de passe** ou **numéros de cartes bancaires** suite à une demande par mail.

"La meilleure des protections sur le web, c'est vous-même et vos bonnes habitudes !"



Sécurisez vos achats en ligne !

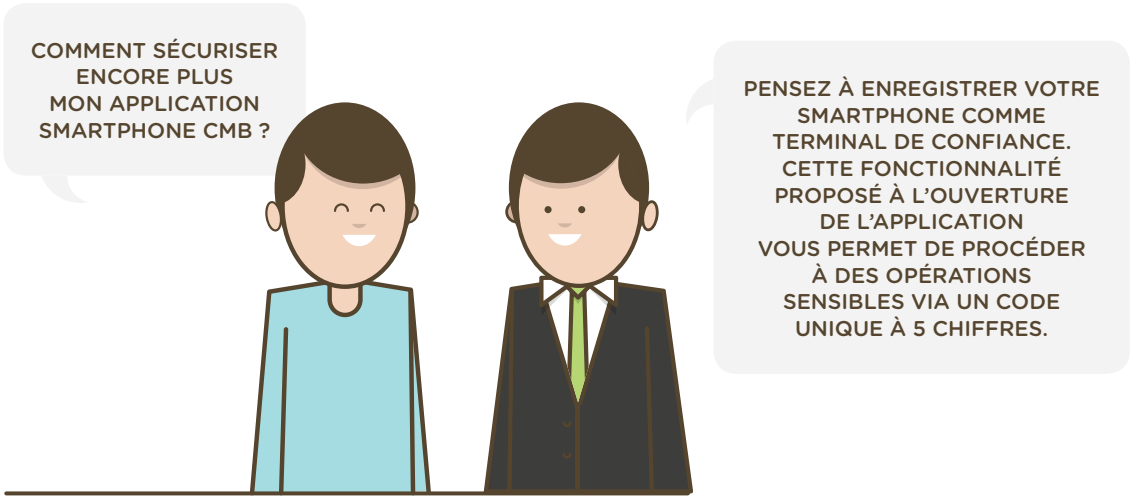
Plusieurs solutions du Crédit Mutuel de Bretagne permettent de payer en ligne sans pour autant avoir à renseigner votre numéro de carte réelle.

Virtualis

Vous pouvez par exemple créer des **numéros de carte virtuels**, à usage unique, via le service gratuit Virtualis (accessible de notre site internet, de l'appli CMB et de notre appli moyens de paiement).

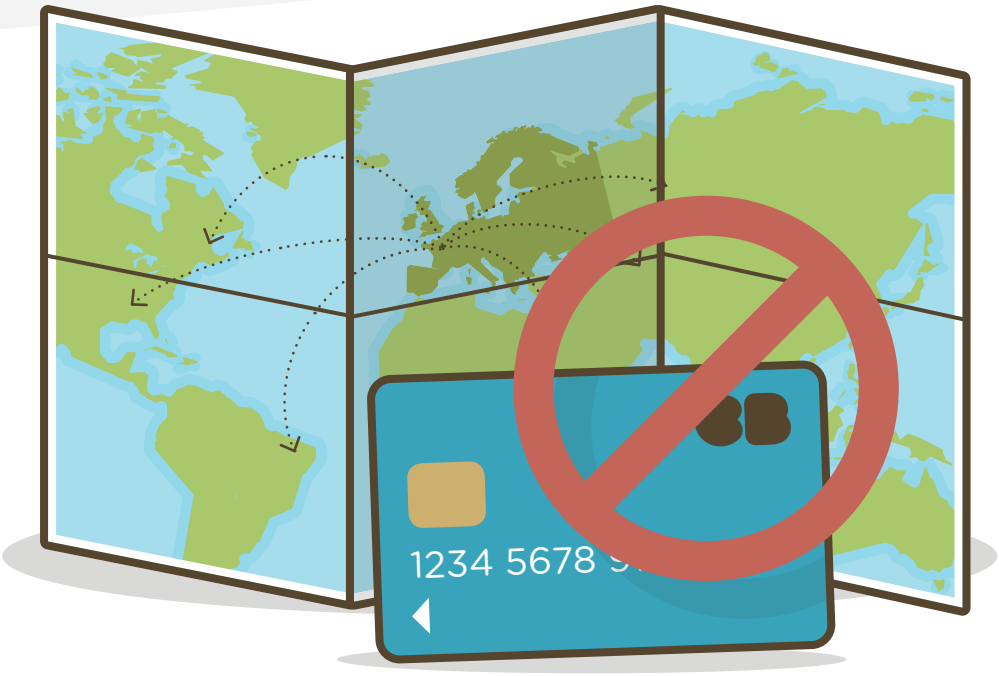
paylib

Tout aussi gratuit, Paylib est un service qui vous permet de payer avec de simples identifiant et mot de passe. Pour cela, vous devez au préalable avoir activé Paylib sur cmb.fr ou dans votre application CMB, et renseigné votre mobile/tablette comme terminal de confiance, pour vous assurer que le service ne soit utilisé que sur votre matériel. Il ne vous reste alors plus qu'à effectuer vos achats en ligne via Paylib. **Plus de 100 sites d'e-commerce** proposent ce **paiement simple, rapide et sécurisé**.



L'ensemble de ces services est destiné aux personnes physiques titulaires d'une carte bancaire de paiement délivrée par une Caisse de Crédit Mutuel de Bretagne et ayant adhéré aux services de Banque à distance. Pour Paylib, certains pré-requis techniques sont nécessaires : accès internet et réseau de téléphonie mobile, terminal mobile disposant des versions minimales Apple IOS 6.1 ou Google Android 2.3.

Bloquez l'utilisation **de votre carte** hors europe



Grâce à cette fonctionnalité gratuite du Crédit Mutuel de Bretagne, vous pouvez piloter le fonctionnement de votre carte à l'étranger (hors Europe) :

- soit être informé par SMS dès que votre carte est utilisée hors Europe pour toutes transactions non sécurisées.
- soit bloquer toute utilisation de la carte hors Europe.

Ceci vous permet donc de limiter les risques de fraude liés à la contrefaçon de la piste de votre carte bancaire. Vous pouvez bien entendu débloquer temporairement votre carte lorsque vous voyagez en dehors de l'Europe.

Tout ceci, vous pouvez le faire d'un clic sur la page «mes cartes» de votre espace sécurisé sur cmb.fr. C'est simple et rapide !

Les services d'alertes sms et geoblocking sont réservés aux personnes physiques titulaires d'une carte bancaire de paiement délivrée par une Caisse de Crédit Mutuel de Bretagne et ayant adhéré aux services de Banque à distance.

En cas d'anomalie constatée
sur votre compte,
contactez votre conseiller
en agence.

Crédit Mutuel
de Bretagne

Pour en savoir plus, rendez-vous sur :

https://www.cmb.fr/securite

Crédit Mutuel Arkéa - S. A. coopérative de crédit à capital variable et de courtage d'assurances. N° ORIAS 07 025 585.
Siège social : 1 rue Louis Lichou - 29480 Le Relecq-Kerhuon - Siren 775 577 018 - RCS Brest. 10/2016