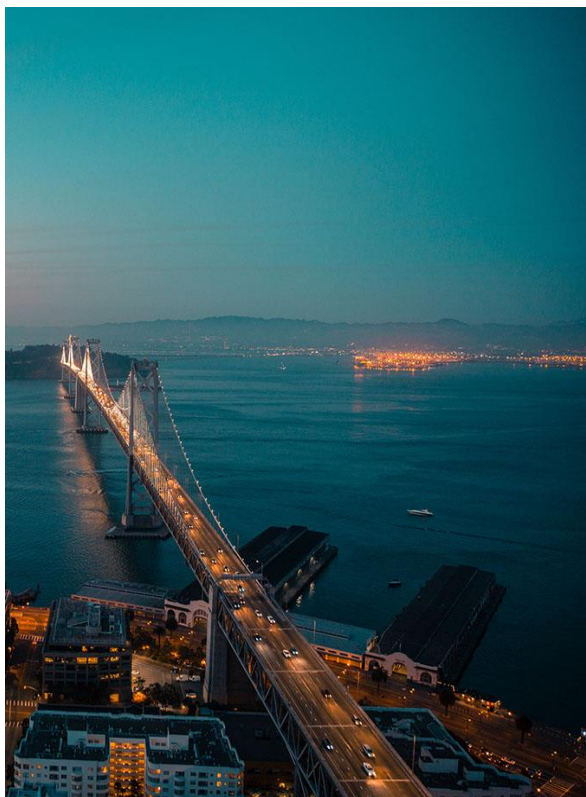


Adoptez les réflexes pour **votre cybersécurité**



Allianz vous accompagne pour mieux vous protéger sur internet, vous, vos données et votre entourage.
Pour en savoir plus, rendez-vous sur allianz.fr, rubrique Cybersécurité.

Naviguez sereinement

- Installez un antivirus, un pare-feu (ou firewall) et un logiciel contre les maliciels (*malwares*) bancaires.
- Effectuez les mises à jour pour bénéficier de la meilleure protection.
- Utilisez les Wi-Fi de réseaux protégés par une clé de sécurité et évitez les Wi-Fi publics.
- Assurez-vous de consulter un site ou une application de confiance en vérifiant qu'il s'agit bien de son adresse officielle (orthographe, présence du cadenas / https ...).

Renforcez la sécurité de vos mots de passe

- Choisissez systématiquement un mot de passe personnalisé et différent sur chacun de vos comptes.
- 8 caractères minimum, contenant des chiffres, des lettres (majuscule et minuscule) et des caractères spéciaux si possible.
- N'utilisez aucune information personnelle (prénoms, dates de naissance....).
- Ne communiquez pas vos mots de passe, même à une personne de confiance.
- Changez vos mots de passe régulièrement.

Emails : consultez-les en sécurité

- Vérifiez systématiquement l'origine du mail et méfiez-vous des chaînes de mails : attention au message vous incitant à réagir en urgence, y compris s'il vient d'un de vos proches.
- Assurez-vous que les contenus, liens et pièces jointes que vous recevez sont sans risque avant de les ouvrir. Préférez un compte email qui propose de vérifier automatiquement vos pièces jointes et messages.
- Saisissez directement l'adresse d'un site au lieu de cliquer sur un lien contenu dans un email.
- Supprimez les éléments suspects et videz régulièrement votre corbeille.

Vies privée et professionnelle, séparez-les

- N'utilisez pas vos ordinateurs et smartphones professionnels pour un usage personnel, et vice-versa. Idem pour vos adresses mails.
- En télétravail, renforcez votre protection en utilisant une connexion via VPN.
- Soyez très vigilants dans l'utilisation de vos comptes de réseaux sociaux. Veillez à ne pas y diffuser vos données sensibles et bien régler vos paramètres de confidentialité.

Espaces personnels : déconnectez-vous

- Une fois vos opérations terminées, utilisez la fonctionnalité de déconnexion, très souvent présente au niveau de votre profil : fermer la fenêtre de navigation ou changer de site ne suffit pas.
- Supprimez les comptes que vous n'utilisez plus.

Préserver votre vie privée et celle de vos enfants

- Ne communiquez jamais par mail ou par SMS vos données personnelles, vos identifiants de connexion ou toute information liée à vos comptes bancaires.
- La diffusion d'une information apparemment anodine peut avoir des conséquences importantes : poster des photos de vacances sur les réseaux sociaux informe aussi de votre absence.
- Vérifiez régulièrement les connexions à vos différents comptes (réseaux, banque, email).
- Sensibilisez vos enfants aux risques des réseaux sociaux et des jeux en ligne : fausse information, harcèlement, paiement frauduleux, mauvaise rencontre ... La prudence est de mise pour tous.

Protégez vos comptes bancaires

- Consultez vos comptes au moins une fois par semaine et vérifiez vos relevés de compte afin d'identifier tout mouvement anormal.
- Evitez d'enregistrer votre carte bancaire sur des sites internet, surtout si vous y allez rarement.
- Privilégiez les paiements avec e-carte bancaire, carte à cryptogramme dynamique, double authentification, ou par un compte de paiement électronique comme Paylib ou Paypal.

Restez informé !

- Soyez attentifs aux actualités et communications sur les arnaques connues. Parlez-en autour de vous : c'est souvent le moyen d'en apprendre encore plus.
- Informez-vous auprès d'interlocuteurs de confiance sur l'évolution des protections disponibles : ne vous laissez pas séduire par l'anti-virus miracle vendu sur internet.

Victime d'une fraude ou tentative de fraude ?

Ayez les bons réflexes



Modifiez tous vos mots de passe, y compris les codes d'accès au wifi



Faites opposition sur votre carte bancaire auprès de votre banque



Déposez plainte, surtout si vous avez perdu de l'argent ou le contenu de votre ordinateur



Déclarez la fraude à l'organisme dont le nom ou la marque ont été usurpés



Signalez le mail frauduleux sur l'un des sites officiels dédiés (cybermalveillance.fr, signal.conso.gouv.fr, cnil.fr...)



Informez votre entourage de votre mésaventure et de ses conséquences

Le présent document est produit à titre d'information uniquement, l'éditeur décline toute responsabilité en cas d'erreur ou d'oubli typographique, technique ou autre inexactitude. Pour plus de conseils, vous pouvez vous référer aux conseils et guides d'hygiène informatique établis par la CNIL et l'ANSSI.



Allianz IARD
Société anonyme au capital de 991.967.200 €
542 110 291 RCS Nanterre

Allianz Vie
Société anonyme au capital de 643.054.425 €
340 234 962 RCS Nanterre

Entreprises régies par le Code des assurances
Siège social : 1, cours Michelet - CS 30051
92076 Paris La Défense Cedex
allianz.fr