	**Ne communiquez jamais d'informations sensibles par messagerie ou téléphone** : aucune administration ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.
	**Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien** (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou allez directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.
	**Vérifiez l'adresse du site qui s'affiche dans votre navigateur.** Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper. Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante.
	**En cas de doute, contactez si possible directement l'organisme concerné** pour confirmer le message ou l'appel que vous avez reçu.
	**Utilisez des mots de passes différents et complexes pour chaque site et application** afin d'éviter que le vol d'un de vos mots de passe ne compromette tous vos comptes personnels. Vous pouvez également utiliser des coffres forts numériques de type KeePass pour stocker de manière sécurisée vos différents mots de passe.
	Si le site le permet, **vérifiez les date et heure de dernière connexion à votre compte** afin de repérer si des accès illégitimes ont été réalisés.
	Si le site vous le permet, **activez la double authentification pour sécuriser vos accès.**

Source : ***www.cybermalveillance.gouv.fr***