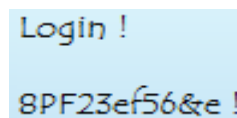


Commencez par faire les mises à jour de l'ordinateur et de votre smartphone régulièrement (système, antivirus, pilotes & logiciels) pour combler les failles de sécurité et bénéficier de nouvelles fonctionnalités.

- Programmez une analyse régulière par votre AntiVirus de votre ordinateur
- N'utilisez que des **moteurs de recherche** connus et fiables tels qu'Exalead (français), Qwant (validé pour les enfants), Google, Bing, ... et ne cliquez pas sur les liens sponsorisés qui peuvent être piégés.
- Assurez-vous que le site est certifié «  <https://www.> » avant de mettre en ligne des données personnelles ou effectuer des achats en ligne. Dans ce dernier cas, **vérifiez l'identité du vendeur, de préférence Français ou Européen** si vous avez besoin d'un recours, **et sa e-réputation** avec une recherche sur Internet associée au mot « arnaque ».

- Limitez les inscriptions sur des sites Internet et renouvelez vos mots de passe tous les 6 mois minimum (8 caractères minimum dont au moins une majuscule, minuscules, chiffres & caractères spéciaux) avec un différent par site sans les faire mémoriser par votre navigateur.



Login !
8PF23ef56&e !

Ne les écrivez pas sur un autre support qu'un coffre d'identifiants sécurisés (ex : KeePass)

Ne cliquez pas sur les bannières publicitaires qui peuvent être piégées !

- Prenez le temps de **bien lire les messages d'avertissements** des systèmes, applications, sites internet, ... avant d'exécuter un programme ou d'ouvrir un fichier. Ne prenez pas de risques si vous avez un doute.

- Privilégiez le **partage de connexion sur un téléphone mobile** de confiance plutôt que de vous connecter à un réseau Wifi Public (HotSpot, Hôtel, Restaurant, ...).



- Privilégiez le **déverrouillage de vos matériels par reconnaissance faciale ou empreinte digitale**
Sur votre Ordinateur, **verrouillez votre session avec Windows+L** lorsque vous devez vous absenter.

- De même, faites attention à la **provenance des clés USB** que vous connectez à vos ordinateurs.

- Faites **attention aux données diffusées** sur internet, notamment sur les réseaux sociaux (Facebook, Twitter, ...), par messagerie, tchat ainsi que les nuages (Cloud). **Désactivez la transmission des informations personnelles** lorsque ce n'est pas indispensable et ne les divulguiez jamais à un **inconnu** : départs en vacances, critères physiques (surtout pour les mineurs) afin d'éviter les cambriolages, attaques personnelles, ...

Les réseaux sociaux sont interdits au moins de 15 ans sans autorisation parentale !

- En cas de doute sur un message suspect (en anglais, mal traduit, ...) :
 - Vérifiez l'authenticité auprès de l'expéditeur via un autre canal (Téléphone, SMS ...),
 - N'ouvrez pas les pièces jointes, en particulier les fichiers de type fausses factures, faux actes notariés, ... ou .exe qui sont en fait des applications,
 - Ne cliquez pas sur les liens : connectez-vous directement sur le site souhaité en tapant son adresse,
 - Vérifiez aussi la cohérence de la liste des destinataires,
 - Supprimez le message sans le transférer.

Ne communiquez jamais vos identifiants, y compris par messagerie.

● Eviter de faire suivre les « chaînes » afin de ne pas diffuser votre adresse et vos données personnelles inutilement, encombrer les réseaux, participer à la désinformation, devenir des vecteurs publicitaires, ...

Si vous avez besoin de faire un envoi à plusieurs contacts qui ne se connaissent pas, privilégiez le champ CCI

A :

Cc :

Cci :

● Tenez à jour votre carnet d'adresses en **supprimant les contacts obsolètes** régulièrement. En cas de piratage de votre messagerie, cela réduit la propagation des menaces existantes.

● N'oubliez pas de faire régulièrement une **sauvegarde** de vos fichiers importants sur des supports différents et de **supprimer les fichiers obsolètes** contenant des informations personnelles.

● N'installez que des logiciels utiles, téléchargés à partir des sites officiels (<http://offurl.fr/> peut vous guider), tout en faisant attention à décocher toute demande d'ajout de logiciels tiers et/ou toolbar qui sont sélectionnés par défaut.

Offres en option

Oui, je souhaite installer l'utilitaire

80% des logiciels piratés contiennent des virus

● Mettez un cache devant votre WebCam pour éviter que des pirates l'utilisent à vos dépens.

● Si vous n'utilisez pas les fonctionnalités avancées de vos logiciels Adobe, désactivez Javascript : <https://helpx.adobe.com/fr/acrobat/11/using/javascripts-pdfs-security-risk.html>

● En cas d'infection ou attaque :

- déconnectez immédiatement votre matériel du WiFi ou du réseau,
- ne l'éteignez pas tant qu'il n'aura pas été étudié par votre professionnel habituel,
- n'appellez surtout pas le numéro qui apparaîtrait à l'écran, il s'agit probablement d'une arnaque,
- prenez votre écran en photo pour le dépôt de plainte.

Annexes

● La Ville de Limoges vous propose plusieurs Ateliers pour vous aider à maîtriser vos usages numériques :

- Ateliers Multimédias de la Bibliothèque : <https://bfm.limoges.fr/espaces-multimedia>
- Ateliers Informatique – Internet du CCM Jean Le Bail : <http://www.centres-culturels-limoges.fr/>
- Ateliers Clubs Loisirs Seniors : <https://www.limoges.fr/fr/pratique/animations-et-conivialite>
- Ateliers Centre Social La Bastide : 32 rue Camille Pissaro 87000 LIMOGES : 05 55 38 36 02

● Le site <https://www.cybermalveillance.gouv.fr/> vous délivre nombre de bonnes pratiques

● Un autre site officiel permet de se former jusqu'en Avril 2021 : <https://secnumacademie.gouv.fr/>

● Plateforme d'information du Ministère de l'Intérieur pour sensibiliser et protéger les internautes : <https://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet>

● Le Ministère de la Défense recrute des Combattants numériques volontaires pour la cyberdéfense : <https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/recrutement/combattant-numerique-pourquoi-pas-vous>

● Dans le cadre du plan d'action contre la radicalisation et le terrorisme du Ministère de l'Intérieur, il est demandé d'être particulièrement vigilant sur tous contenus visant le recrutement et la propagande (contenu vidéo Youtube, pages réseaux sociaux, ...)