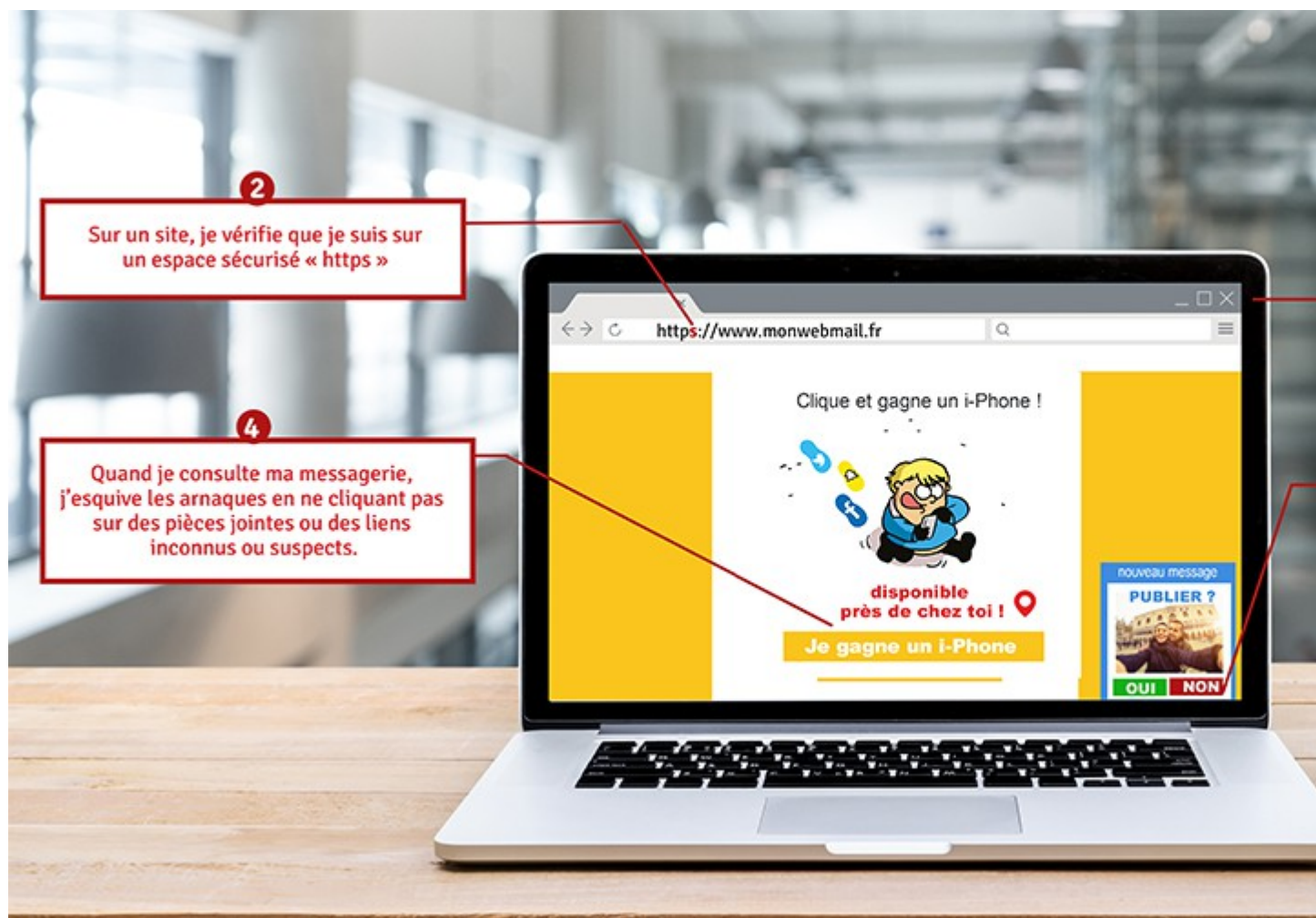


12 conseils pour utiliser un ordinateur public en toute sécurité

23 janvier 2019

Pour les besoins d'une démarche en ligne, vous êtes peut être amené à utiliser un ordinateur partagé sur le lieu d'accueil d'une association ou d'un service public. Voici quelques conseils, pour préserver la confidentialité de vos données et éviter les pièges en ligne.

Lorsque je navigue sur internet

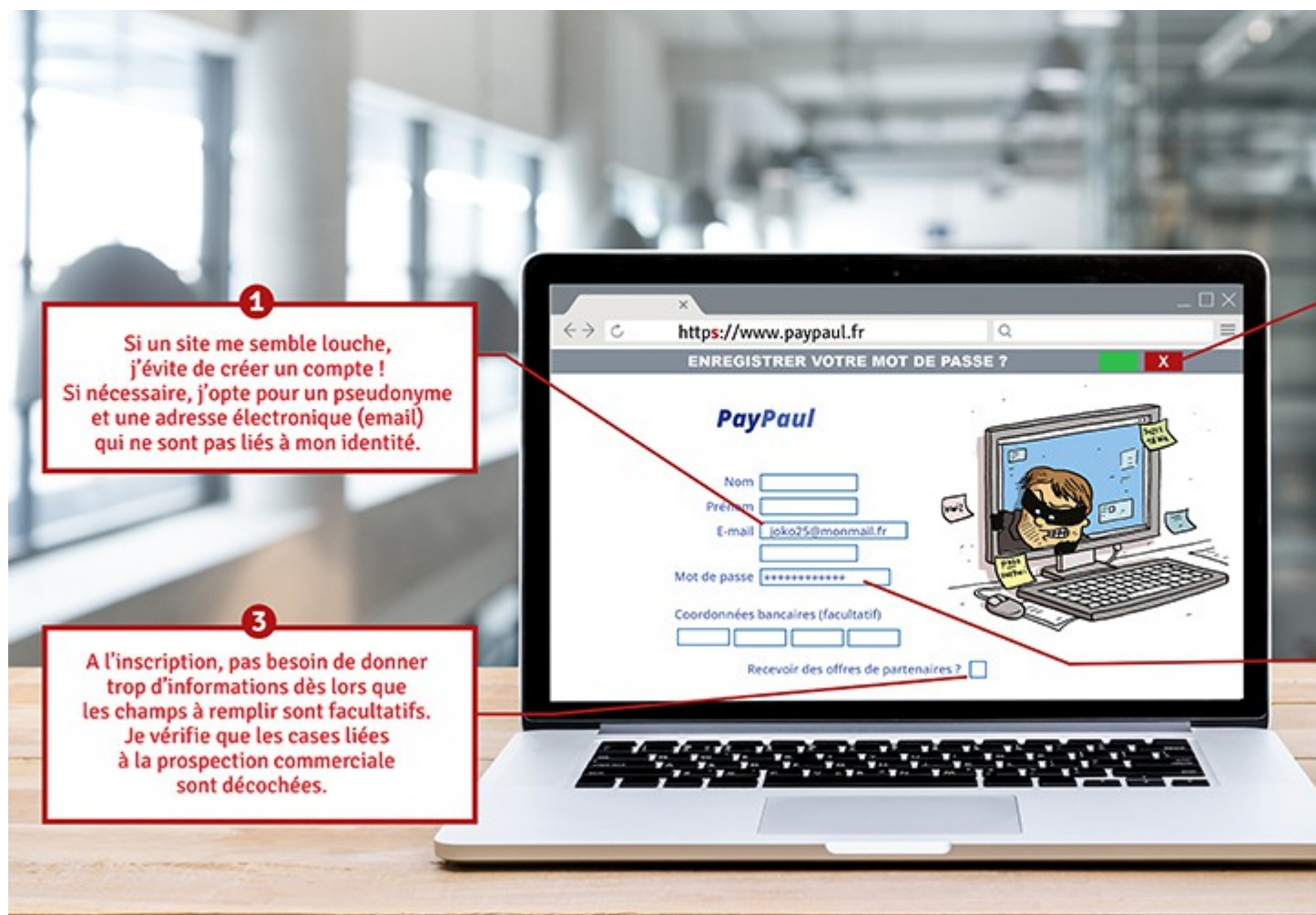


1. J'ouvre le mode « navigation privée » de mon navigateur. Cela permettra de ne pas laisser de traces derrière moi (mots de passe, historique de navigation, etc.).
2. Sur un site, je vérifie que je suis sur un espace sécurisé « *https* » et que le site propose un minimum d'informations sur l'utilisation de mes données et une adresse de contact pour exercer mes droits.
3. Je prends connaissance des politiques de confidentialité des sites que je consulte ainsi que de leurs règles d'utilisation. Si je ne les comprends pas, je peux demander de l'aide à un

intervenant social ou numérique au sein d'un espace public numérique (EPN), d'un guichet social, etc.

4. Lorsque je consulte mon service de messagerie, j'esquive les arnaques : je n'ouvre pas les pièces jointes d'émetteurs inconnus et je ne communique pas mes codes secrets !
5. Sur les réseaux sociaux, je ne publie pas de photos ou de vidéos trop personnelles sur ma vie ou celle des autres. Je fais un tour dans les paramètres de confidentialité pour m'assurer que seules les personnes que j'ai choisies ont accès à mes profils.

Lorsque je m'inscris sur un service en ligne



6. Pour chaque compte important, je crée un mot de passe que je renouvelle régulièrement, qui ne dit rien sur ma vie et qui est composé de 12 caractères avec des chiffres, des caractères spéciaux, des minuscules et des majuscules.
7. Dès que je suis connecté à mon compte, une fenêtre me propose de retenir mes mots de passe : je dis toujours « NON » lorsque je suis sur un ordinateur public. Je préfère l'enregistrer dans le meilleur des coffres-forts : ma mémoire ou un gestionnaire de mots de passe !
8. Par principe, mon mot de passe est secret. Je ne le communique jamais sauf si cela est nécessaire dans le cadre de l'accompagnement social ou numérique. Je ne le communique jamais par courrier électronique (e-mail) ou par téléphone. En effet, aucun organisme ne doit me les demander par ces moyens-là.

9. Si un site me semble louche, j'évite de créer un compte ! Si nécessaire, j'opte pour un pseudonyme et une adresse électronique (adresse e-mail) qui ne sont pas liés à mon identité. Cela protège mes nom et prénom mais ne me rend pas anonyme pour autant. J'utilise différentes adresses électroniques en fonction de mes activités (professionnelles, personnelles, associatives, sociales, etc.).
10. **A l'inscription**, pas besoin de donner trop d'informations dès lors que les champs à remplir sont facultatifs. Je vérifie que les cases liées à la prospection commerciale sont décochées.

Lorsque je quitte mon poste



11. Je supprime les documents personnels enregistrés sur l'ordinateur ainsi que mon historique de navigation.
12. Je quitte ma session (bouton de déconnexion de session) et n'oublie rien dans l'imprimante
- ...

Texte reference

Pour approfondir

> [Je crée un mot de passe sûr](#) 

> [Je fais le ménage dans l'historique de navigation](#) 

> J'utilise la navigation privée 

> Je vérifie que je suis sur la version https des sites importants 

> Je me méfie des arnaques en ligne et par courrier électronique (e-mail) 