COMMENT ME PROTÉGER ?

BONNES PRATIQUES POUR CONSTRUIRE SON MOT DE PASSE

Messageries, réseaux sociaux, banques, administrations et commerces en ligne, réseaux et applications d'entreprise... La sécurité de l'accès à ces services du quotidien repose aujourd'hui essentiellement sur les mots de passe.

Adoptez les bonnes pratiques pour protéger vos comptes.

→ UTILISEZ UN MOT DE PASSE SUFFISAMMENT LONG ET COMPLEXE

• 10 caractères minimum
La longueur est un élément important de votre mot de passe.

• Contenant au minimum les caractères suivants :

→ Des chiffres *(012...9)*
→ Des minuscules *(abc...z)*
→ Des caractères spéciaux *($*%'&)*
→ Des majuscules *(ABC...Z)*

→ UTILISEZ UN MOT DE PASSE DIFFÉRENT POUR CHAQUE SERVICE

→ UTILISEZ UN MOT DE PASSE IMPOSSIBLE À DEVINER POUR LES AUTRES

→ N'ABANDONNEZ PAS VOTRE MOT DE PASSE

Les post-it, bloc-notes, appareils partagés ou messageries en ligne ne sont pas conçus pour stocker vos mots de passe de façon sécurisée.

→ ACTIVEZ LORSQUE C'EST POSSIBLE « L'AUTHENTIFICATION FORTE » SUR VOS COMPTES SENSIBLES

Également appelée « authentification multi facteurs » ou « authentification en deux étapes ».

QUELQUES ASTUCES POUR FACILITER LE QUOTIDIEN :

En panne d'idée pour construire un mot de passe complexe, différent pour chaque service et impossible à deviner pour les autres ?

→ UTILISEZ UNE PHRASE DE PASSE

Une phrase de passe (passphrase en anglais) est un mot de passe robuste créé à partir d'une phrase :
• Choisissez une phrase que vous retiendrez facilement.
• Utilisez la première lettre de chaque mot pour construire votre mot de passe.
• La phrase choisie doit contenir des chiffres et des caractères spéciaux comme une majuscule, un signe de ponctuation ou un caractère spécial ($,#...) et au moins une dizaine de mots.

Exemple de création d'une passphrase :

Les Jeux Olympiques et Paralympiques de Paris 2024 ouvrent grand les Jeux ! → LJOePdP2024oglJ!

Phrase — Mot de passe associé*

** N'utilisez pas ce mot de passe, choisissez une phrase personnalisée pour construire le vôtre.*

→ UN MOT DE PASSE POUR LES GOUVERNER TOUS

Utilisez un gestionnaire de mots de passe pour stocker vos mots de passe en toute sécurité.
Vous n'aurez à mémoriser qu'un seul mot de passe robuste pour accéder à l'ensemble de vos comptes.
Il est conseillé de ne pas mélanger les mots de passe professionnels et personnels dans le même gestionnaire.

Pour en savoir plus...
CNIL – Recommandation pour un bon mot de passe

COMMENT ME PROTÉGER ?

IDENTIFIER UNE TENTATIVE DE PHISHING (MAIL / SMS / APPEL)

L'hameçonnage ou phishing en anglais est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles sensibles (comptes d'accès, mots de passe…) ou bancaires en se faisant passer pour un tiers de confiance.
Il peut s'agir d'un faux message, SMS ou appel téléphonique provenant d'un service du quotidien : banque, réseau social, opérateur de téléphonie, fournisseur d'énergie, commerce en ligne, administrations, etc.

Adoptez les bonnes pratiques pour protéger vos données.

➜ NE COMMUNIQUEZ JAMAIS D'INFORMATIONS SENSIBLES

Paris 2024 ne vous demandera jamais vos mots de passe.
Paris 2024 ne vous demandera jamais vos données bancaires sans sollicitation de votre part.

➜ VÉRIFIEZ L'EXPÉDITEUR DU MAIL

La réception d'un message non sollicité d'une adresse e-mail inhabituelle, que vous ne connaissez pas, doit éveiller votre attention, même si celle-ci est d'apparence légitime.

En cas de doute, allez directement sur le site officiel.

➜ VÉRIFIEZ LE CONTENU DU MESSAGE

Un e-mail ou SMS de phishing est non sollicité et fait souvent part d'une offre alléchante, un besoin urgent ou une menace imminente.

Ne donnez pas suite à ces sollicitations et vérifiez l'information par vous-même auprès du service concerné en cas de doute.

➜ NE CLIQUEZ JAMAIS SUR UN LIEN DOUTEUX

Avant de cliquer sur un lien reçu par e-mail ou SMS, contrôlez que l'URL de destination est légitime.

En cas de doute, naviguez par vous-même directement sur le site officiel du service concerné.

➜ N'OUVREZ PAS DE PIÈCE-JOINTE SI LE MAIL EST DOUTEUX

Si vous recevez un e-mail non sollicité avec un contenu douteux vous incitant à ouvrir une pièce-jointe, procédez aux vérifications précédentes avant d'ouvrir la pièce-jointe pour protéger vos appareils.

En cas de doute, contactez le service concerné.

Pour en savoir plus...
CYBERMALVEILLANCE – Que faire en cas de phishing ou hameçonnage ?

COMMENT ME PROTÉGER ?

IDENTIFIER UN SITE LÉGITIME

Attirés par le gain financier, les cybercriminels redoublent d'effort et n'hésitent pas à mettre en ligne des sites internet usurpant les services du quotidien : des messageries en ligne, des sites e-commerce, des services bancaires ou encore administratifs par exemple.

Lors de la navigation sur internet, il faut donc porter une attention particulière à la légitimité des sites web visités. Les transactions sensibles ne doivent être réalisées que depuis des sites officiels.

Adoptez les bonnes pratiques pour naviguer en ligne en toute sécurité.

→ MAINTENEZ VOTRE NAVIGATEUR INTERNET À JOUR

Les principaux navigateurs Internet (e.g. Chrome, Firefox, Safari...) alertent désormais les internautes lorsque la navigation est dangereuse.
Ne consultez pas les sites jugés dangereux par votre navigateur.

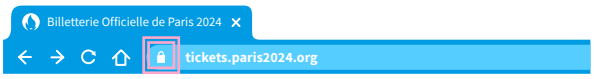
→ VÉRIFIEZ LA QUALITÉ DU CONTENU

La qualité du contenu d'un site web malveillant est souvent douteuse : fautes d'orthographe, fonctionnalité qui ne marche pas, contenu manquant...

→ VÉRIFIEZ L'ADRESSE DU SITE QUI S'AFFICHE DANS VOTRE NAVIGATEUR

En cas de doute, procédez aux 3 étapes de vérifications suivantes :

LE PROTOCOLE



Vérifiez la présence du https dans l'URL ou le cadenas. Si vous rencontrez un site web ne présentant pas le protocole sécurisé https, il est fort probable que le site ne soit pas légitime. En l'absence du protocole sécurisé https, ne réalisez pas de transactions sensibles.

LE NOM DE DOMAINE

Vérifiez que le nom de domaine correspond à celui du site officiel. Les sites officiels Paris 2024 utilisent le nom de domaine « paris2024.org ».

NE PAS CONFONDRE SOUS-DOMAINE OU CHEMIN AVEC LE NOM DE DOMAINE

Vérifiez que le nom de domaine correspond à celui du site officiel. Les sites officiels Paris 2024 utilisent le nom de domaine « paris2024.org ».

- Le **sous-domaine** se situe juste avant le nom de domaine. Il est séparé du nom de domaine avec un « . »
- Le **chemin** commence au premier « / » (slash) rencontré après le nom de domaine.

Exemples de décomposition d'URL :

✓ **URL conforme :** https://tickets.paris2024.org/test

Protocole	*Sous-domaine*	*Nom de domaine*	*Chemin*
https://	**tickets.**	**paris2024.org**	**/test**
Communications sécurisées		*Le nom de domaine est ici « paris2024.org », il s'agit bien d'un site officiel.*	

× **URL malveillante :** https://paris2024.tickets.org/test

Protocole	*Sous-domaine*	*Nom de domaine*	*Chemin*
https://	**paris2024.**	**tickets.org**	**/test**

Attention ! « paris2024 » et « tickets » ont été inversés, le nom de domaine devient désormais tickets.org, il ne s'agit pas d'un site officiel. La présence du terme paris2024 dans le sous-domaine n'est pas gage de légitimité. Seul le nom de domaine permet de vérifier la légitimité du site web.

× **URL malveillante :** https://siteweb.malveillant.org/abc?test=paris2024.org

Protocole	*Sous-domaine*	*Nom de domaine*	*Chemin*
https://	**siteweb**	**malveillant.org**	**/abc?test=paris2024.org**
		Le nom de domaine est ici « malveillant.org »	*La présence de paris2024.org dans le chemin n'est pas gage de légitimité*

Pour en savoir plus...
CYBERMALVEILLANCE – Que faire en cas de phishing ou hameçonnage ?

COMMENT ME PROTÉGER ?

METTRE À JOUR MES ÉQUIPEMENTS

Les appareils numériques et les logiciels que nous utilisons au quotidien peuvent présenter des failles de sécurité plus ou moins exploitées par les cybercriminels. Face à ces risques, les éditeurs et les fabricants proposent des mises à jour (patch en anglais) visant à corriger ces failles. Si l'opération de mise à jour est souvent ressentie comme une contrainte, il s'agit toutefois d'un acte essentiel pour se protéger.

Adoptez les bonnes pratiques pour prendre soin de vos équipements.

→ METTEZ À JOUR L'ENSEMBLE DE VOS APPAREILS ET LOGICIELS SANS TARDER

→ ACTIVEZ L'OPTION DE TÉLÉCHARGEMENT ET D'INSTALLATION AUTOMATIQUE DES MISES À JOUR

→ TÉLÉCHARGEZ LES MISES À JOUR UNIQUEMENT DEPUIS LES SITES OFFICIELS*

* ou magasin d'applications

→ FAITES DES SAUVEGARDES RÉGULIÈRES DE VOS DONNÉES ET DE VOS LOGICIELS

Il convient en particulier de vérifier l'existence d'une sauvegarde avant une opération de mise à jour.

Pour en savoir plus...

CYBERMALVEILLANCE – Pourquoi et comment bien gérer ses mises à jour ?