Les bases de la cybersécurité pour les utilisateurs

Les mots de passe :

Pas les mêmes sur tous les sites : utilisez un mot de passe unique pour chaque compte. Cela limite les risques si un mot de passe est compromis.

Utilisez des mots de passe complexes :

Au moins 12 caractères.

Inclure des majuscules, des minuscules, des chiffres et des symboles.

Évitez les mots évidents comme votre nom, prénom, date de naissance, ou le nom de votre animal de compagnie.

Gestion des mots de passe :

Utilisez un gestionnaire de mots de passe pour stocker vos mots de passe en toute sécurité (par exemple KeePass...).

Ne jamais enregistrer vos mots de passe dans votre navigateur.

Authentification à 2 facteurs (A2F) :

Activez l'authentification à 2 facteurs (via SMS, e-mail ou application dédiée) chaque fois que c'est possible pour une couche de sécurité supplémentaire.

Les sauvegardes :

Faire des sauvegardes régulières :

Sauvegardez vos données importantes sur un support externe (disque dur, clé USB) ou dans un service cloud sécurisé.

Automatiser les sauvegardes pour ne pas les oublier.

Vérifier les sauvegardes :

Testez régulièrement vos sauvegardes pour vous assurer qu'elles sont fonctionnelles et à jour.

Vulnérabilité aux attaques :

Liens et pièces jointes inconnus :

Ne cliquez jamais sur les liens ou n'ouvrez jamais les pièces jointes provenant de sources inconnues ou suspectes.

Si un e-mail semble louche, même s'il provient d'un contact connu, vérifiez l'adresse et demandez une confirmation directe.

Système et logiciels à jour :

Maintenez votre système d'exploitation et vos logiciels à jour pour corriger les failles de sécurité connues.

Activez les mises à jour automatiques si possible.

Antivirus et pare-feu :

Installez un logiciel antivirus et activez le pare-feu de votre système pour une protection de base.

Utilisation des périphériques :

Clés USB et disques durs :

Ne branchez jamais une clé USB ou un périphérique inconnu à votre ordinateur. Ces derniers pourraient contenir des logiciels malveillants.

Utilisez uniquement des périphériques provenant de sources fiables ou approuvées.

Matériel partagé :

Si vous utilisez un ordinateur partagé, veillez à vous déconnecter de vos comptes une fois votre session terminée.

Verrouillez votre session à chaque fois que vous quittez votre poste de travail, même pour une courte absence.

Navigation en ligne :

Wi-Fi :

Évitez les réseaux Wi-Fi publics non sécurisés. Si vous devez les utiliser, connectez-vous via un VPN pour protéger vos données, éviter d’effectuer des transactions lorsque vous êtes connecter ur un réseau publique.

Sites sécurisés :

Assurez-vous que les sites sur lesquels vous entrez des informations sensibles sont sécurisés (vérifiez la présence de "https://" et du cadenas dans la barre d'adresse).

Réseaux sociaux et partage d'informations :

Protéger votre vie privée :

Ne partagez pas d'informations sensibles (numéro de téléphone, adresse, documents personnels) sur les réseaux sociaux.

Configurez vos paramètres de confidentialité pour limiter la visibilité de vos publications (compte privé de préférence).

faire gaffe a ne pas poster des photos proche des endroits ou vous habiter ou qui semble être reconnaissable.

Méfiance :

Ne cliquez pas sur les liens envoyés par des inconnus ou des messages inhabituels de vos contacts.

Si vous recevez un SMS ou un e-mail de la part d’une entité comme une banque, un organisme gouvernemental ou un service postal, vous demandant de vous connecter à votre compte ou de réaliser une action, ne cliquez pas sur le lien fourni dans le message. Rendez-vous directement sur le site officiel en tapant son adresse dans votre navigateur ou en utilisant votre application habituelle.