INFORSUD TECHNOLOGIES
Solutions et impulsions pour l'avenir

PROTÉGER VOS DONNÉES
Les bonnes pratiques en cybersécurité !

En protégeant vos données, vous protégez également celles dont on vous confie la responsabilité.

1 POLITIQUE DES MOTS DE PASSE

Il ne vous viendrait pas à l'idée d'utiliser la même clé pour toutes les serrures, c'est pourquoi il est recommandé d'avoir un mot de passe différent et robuste pour chaque compte.

Un mot de passe robuste selon l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) :
- 12 caractères minimum
- N'ayant aucun lien avec vous (prénom, date de naissance, etc.)
- N'utilisant pas des mots issus du dictionnaire

Voici 2 méthodes pour vous aider à définir vos mots de passe :
- La **méthode phonétique** : « Elle a un mot de passe phonétique » : L@1MDPFon&Tic
- La **méthode des 1ères lettres** : « Allons enfants de la patrie, le jour de gloire est arrivé ! » : aE2lP,lJ2Géa!

Pour faire plus simple et plus sûr, utilisez des logiciels de générateurs et coffres-forts de mots de passe.
Exemple : KeePass, logiciel gratuit et recommandé par l'ANSSI.

2 SÉPARATION DES USAGES PROFESSIONNELS ET PERSONNELS

Les équipements numériques sont de plus en plus sophistiqués, performants et mobiles.
Avec l'évolution des pratiques, comme le télétravail, les collaborateurs peuvent travailler de n'importe où.

L'usage de son équipement personnel à des fins professionnelles pose des problèmes de sécurité des données : en cas de casse, de perte ou de vol, personne ne gère pour vous la sauvegarde de vos données professionnelles sur vos appareils personnels.

À l'inverse, l'usage de son équipement professionnel à des fins personnelles présente tout autant de risques. En cliquant sur un lien frauduleux via sa boîte email personnelle, les données confidentielles de l'organisation pourraient être mises en danger.

3 UTILISATION DE LA MESSAGERIE

Le phishing est une attaque qui consiste à leurrer la cible via un e-mail frauduleux. L'attaquant se fait passer pour un tiers de confiance pour vous rediriger vers un lien malveillant et vous inciter à communiquer des informations confidentielles.

Il est important de se poser les bonnes questions à réception d'un email :
- Connaissez-vous l'expéditeur ?
- Est-il normal de recevoir un email à cette heure-ci et cette date-là ?
- L'objet et le contenu sont-ils en lien avec votre activité ?
- Le lien est-il suspect ? Avez-vous un doute ?

4 MISES À JOUR INFORMATIQUES

Concernant les mises à jour, même si vous êtes en déplacement ou en télétravail, ne pas remettre à demain les mises à jour demandées et réalisez-les rapidement.

Elles sont essentielles à la sécurité de votre environnement informatique et ceci sur tous vos appareils : mises à jour du système d'exploitation, des anti-virus, des navigateurs web, des logiciels etc.

Elles corrigent souvent des failles de sécurité.

5 SAUVEGARDES RÉGULIÈRES

En cas de cyberattaque, de vol, de perte ou de panne, la sauvegarde est souvent le seul moyen de retrouver ses données (photos, fichiers, contacts, messages…).

Sauvegardez régulièrement les données de vos équipements et/ou conservez une copie de vos sauvegardes sur un support fiable et externe à votre équipement.

INFORSUD TECHNOLOGIES
Solutions et impulsions pour l'avenir

PROTÉGER VOS DONNÉES
Les bonnes pratiques cybersécurité !

6

SÉCURISATION DES CONNEXIONS

En distanciel, voici 3 bonnes pratiques indispensables à suivre :

- En déplacement, si vous êtes à l'hôtel ou à l'aéroport, privilégiez l'accès à internet via la fonction partage de connexion de votre smartphone. Celle-ci s'appuie sur une connexion cellulaire plus sécurisée type 3/4/5G. Ce réseau cellulaire est indépendant du réseau wifi public ou partagé même avec un mot de passe, qui lui est à éviter car il n'est pas assez sécurisé.
- Se connecter au réseau de votre structure en utilisant une connexion sécurisée, qui chiffre les échanges de données, type VPN.
- Pour rajouter un niveau de sécurité supplémentaire, chiffrez vos appareils nomades. Il existe pour cela des logiciels spécialisés recommandés : Cryhod, Oxygene, Bitlocker.

7

TÉLÉCHARGEMENT DE LOGICIELS ET D'APPLICATIONS

Pour l'installation de logiciels ou d'applications, l'équipe informatique de votre structure s'en chargera normalement. Dans le cas contraire :

- Limiter tout de même le téléchargement de logiciels et applications car chacun représente un point d'attaque potentiel à surveiller.
- Sur votre ordinateur, installez uniquement des exécutables issus de sources sûres et privilégiez les sites d'éditeurs officiels.
- Dans le cas des smartphones, il est vivement recommandé d'éviter les magasins d'applications non officiels, où les garanties d'authenticité sont faibles, voire absentes.

8

MAÎTRISE DE L'USAGE DES RÉSEAUX SOCIAUX

Les réseaux sociaux professionnels se développent de plus en plus. Ils contiennent de nombreuses données personnelles qui ne doivent pas tomber dans de mauvaises mains.

Ces données personnelles pourraient donner des informations précieuses sur vos mots de passe (date de naissance, prénoms de vos enfants, etc.).

Il est important de :
- Sécuriser l'accès à vos réseaux sociaux avec un mot de passe solide et unique
- Définir les autorisations sur vos informations et publications

9

SE SERVIR D'ANTIVIRUS

Les antivirus permettent de se protéger d'une grande majorité d'attaques et de virus connus.

Il existe de nombreuses solutions selon vos usages et le niveau de protection ou de services recherchés.

Vérifiez régulièrement que les antivirus de vos équipements sont bien à jour et lancer des analyses approfondies au moins une fois par mois, pour vérification.

10

SENSIBILISATION DE TOUS LES COLLABORATEURS

90% des incidents en sécurité informatique ont comme origine un facteur humain. La connaissance est notre meilleure arme de défense !

Alors, qu'attendez-vous pour informer et sensibiliser vos collaborateurs sur les bonnes pratiques à adopter ?