Sensibilisation aux risques de cybersécurité

Le télétravail se met en place chez France Médias Monde depuis octobre 2019.

Cette brochure vous présente les recommandations à mettre en œuvre pour l'utilisation du réseau de l'entreprise depuis votre domicile.

Rappelez-vous ! la cybersécurité est la responsabilité de chacun.

Les cyberattaques dont le groupe fait parfois l'objet, nous imposent la plus grande vigilance. La sécurité est l'affaire de tous.

France Médias Monde
80, rue Camille Desmoulins
92130, Issy Les Moulineaux

Télétravail :

Règles à suivre pour la **sécurité informatique** du Groupe

Comment travailler à distance en toute sécurité

rfi FRANCE 24 MCD مونت كارلو الدولية FRANCE MÉDIAS MONDE

Quels risques ?

Le télétravail implique une connexion avec le réseau interne du Groupe, pouvant laisser la porte ouverte sur les données sensibles voir confidentielles de l'entreprise. Votre plus grande vigilance est donc requise dans ce cadre d'utilisation.

Votre domicile est en effet un lieu non maîtrisé par le groupe pouvant être soumis aux risques suivants :

- Perte ou vol du matériel
- Compromission du matériel pendant par exemple une absence temporaire
- Compromission des informations contenues dans le matériel
- Accès illégitime au SI du Groupe
- Interception des informations (perte de confidentialité / d'intégrité)

« Erreur courante : penser ne pas représenter un intérêt suffisant pour faire l'objet d'une cyberattaque »

Comment se protéger ?

Pour limiter les risques informatiques, plusieurs mesures simples doivent être appliquées :

- **Protéger votre connexion WiFi** à l'aide d'un mot de passe suffisamment sécurisé combinant minuscule, majuscule, chiffre et caractères spéciaux sur au moins 12 caractères.
  En effet, avec un mot de passe trop simple, une personne pourrait utiliser votre connexion à votre insu et récupérer des données sur votre PC.

- **Si votre poste est partagé** avec la famille, le mieux est de **créer votre propre session** pour plus de sûreté, au niveau des préférences systèmes. Procédures sur internet :
  https://support.apple.com/fr-fr
  https://support.microsoft.com/fr-fr

  Penser à verrouiller votre session dès que vous quittez votre poste.

- **Authentification forte via l'utilisation d'un mot de passe complexe et unique** pour ouvrir votre session.
  Si votre mot de passe est trop simple, il sera en effet trop vulnérable face au piratage.
  Et surtout ne pas utiliser le même mot de passe partout, ne pas l'écrire sur un post-it à proximité ni le stocker sur votre téléphone.

- Penser à **effectuer régulièrement les mises à jour** sur votre poste, notamment pour l'antivirus.
  Des failles peuvent exister sur vos logiciels ou applications permettant à des personnes malveillantes de s'introduire dans votre système et voler ou détruire vos données.
  Lorsque ces failles sont découvertes par les éditeurs, elles sont corrigées via des patchs de sécurité.

- **Limiter au maximum l'utilisation de périphériques externes, telles que clé USB, disques durs, etc.** En effet, méfiez-vous ! un malware (programme malveillant) pourrait être présent dessus et se diffuser sur votre ordinateur et le réseau de l'entreprise.

- **Séparer bien les usages professionnels de vos usages privés**. Utiliser uniquement votre messagerie professionnelle pour vos échanges professionnels.

- **Ne sauvegarder aucun document professionnel sur votre poste personnel ou tout autre support non sécurisé (clé USB, disque dur, smartphone, etc.)**, mais penser à sauvegarder régulièrement vos documents sur le Cloud via Office365.

- **Faire attention à votre identité numérique.** Attention à ce que vous publiez sur les sites internet. Vos données personnelles pourraient permettre à des personnes malveillantes de retrouver vos mots de passe ou être utilisées contre vous.

REAGIR ! En cas d'attaque ou de suspicion, contactez-nous sur notre boite mail : suspect@francemm.com