

10 règles simples pour limiter les risques d'attaque informatique

- ✓ Choisir des mots de passe complexes : 12 caractères (composés de majuscules, minuscules, chiffres, caractères spéciaux) sans lien avec ses noms, date de naissance... et différent pour chaque accès
- ✓ Mettre à jour régulièrement logiciels et système d'exploitation : navigateur, antivirus, bureautique, pare-feu
- ✓ Effectuer des sauvegardes fréquentes : quotidiennes de préférence ou hebdomadaires, sur des supports ou systèmes distincts de votre système d'information
- ✓ Se méfier du WI-FI : sécuriser l'accès au WI-FI de l'entreprise et éviter de se connecter au WI-FI public à l'extérieur, non sécurisé
- ✓ Séparer compte "utilisateur" et compte "administrateur" : n'ouvrir que des comptes utilisateurs aux salariés
- ✓ Ne pas mélanger personnel et professionnel : ne pas utiliser de clés USB ou disques durs externes personnels sur un terminal professionnel et inversement
- ✓ Ne jamais ouvrir les mails douteux : ne pas cliquer sur une pièce jointe, liens ou messages d'un expéditeur inconnu sans vérifier sa provenance
- ✓ Naviguer sur des sites officiels : privilégier la saisie de l'adresse du site dans la barre d'adresse du navigateur
- ✓ Rester prudent lors des déplacements : se limiter aux données nécessaires à la mission, surtout à l'étranger
- ✓ Être aussi prudent avec les smartphones, tablettes, objets connectés moins bien sécurisés que les ordinateurs

Votre entreprise est victime d'une attaque, comment réagir ?

- ✓ Déconnecter les machines compromises du réseau sans les éteindre
- ✓ Alerter immédiatement le responsable sécurité SI ou le prestataire informatique disposant du label CERT-FR (centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques)
- ✓ Sauvegarder les fichiers importants sur des supports de données isolés
- ✓ Porter plainte auprès d'un service de Police ou de Gendarmerie
- ✓ Réinstaller entièrement le système d'exploitation et appliquer tous les correctifs de sécurité avant de le reconnecter