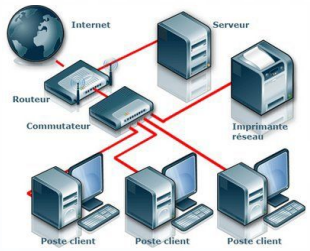
Région de gendarmerie de Nouvelle-Aquitaine
et gendarmerie pour la zone de défense
et de sécurité Sud-Ouest

Information Cyber et Covid-19

La situation particulière que nous vivons actuellement est **propice aux attaques cyber.**
Opportunistes, les pirates informatiques exploitent notre besoin d'information, nos demandes, l'utilisation accrue du réseau informatique et les conditions de télétravail...



I/ Protection du réseau informatique d'une structure

@ Prévenez les menaces

*****Profitez du ralentissement de l'activité pour faire un bilan informatique complet ;**

*****Procédez à des sauvegardes régulières et hors ligne des données, sans oublier de déconnecter à l'issue, votre support de sauvegarde.**

@ Sensibilisez vos salariés/employés

*****Assurez vous de connaître les personnes à contacter ;**

*****Utilisez un Réseau Privé Sécurisé (VPN) de confiance, un antivirus mis à jour…**

*****Rappelez les règles d'utilisation du réseau informatique de votre structure ;**

*****Séparez vos données personnelles de l'activité professionnelle ;**

*****Vérifiez par un contre-appel l'identité d'un interlocuteur ;**

*****Assurez vous de connaître les consignes et personnes à contacter en cas d'incident.**

II/ L'actualité des cybercriminels

Faux sites internet de vente en ligne de produits sanitaires (masques, gel hydroalcoolique, médicaments) : ***Rendez-vous*** sur les sites officiels.

Fausse commande et faux ordres de virement : ***Vérifiez*** les demandes de virement ou un changement de RIB d'une facture, d'un salaire.

L'hameçonnage, le phishing : ***Méfiez-vous*** des mails, SMS et appels téléphoniques non identifiés qui ont pour but de vous soustraire des informations personnelles, professionnelles ou bancaires en vous orientant sur de faux sites.

Dons frauduleux : ***Évitez*** de cliquer sur les liens des appels aux dons et rendez vous directement sur les sites officiels.

Rançongiciel, Ransomware : Attaque empêchant l'accès aux données de l'entreprise et réclamant une rançon pour les libérer. Elle peut s'accompagner d'un vol de données et d'une destruction préalable des sauvegardes.

Elles sont possibles par une intrusion sur le réseau de l'entreprise, un accès à distance (notamment en cette période les accès distant doivent être sécurisés), par la compromission de l'équipement d'un collaborateur ou un défaut de mise à jour du matériel informatique (pièces jointes ou liens présents dans les courriers électroniques).

En cas de doute, la gendarmerie est à vos côtés

En cas d'urgence, contactez le 17 ou le 112

Pour toute question :

cyber-vigilance-nouvelleaquitaine@gendarmerie.interieur.gouv.fr

Région de gendarmerie de Nouvelle-Aquitaine
Division des opérations/Bureau renseignements – Section de recherches/Pôle cybercriminalité