RISQUE D'ATTAQUES INFORMATIQUES

DANS CE CONTEXTE DE COVID-19, ON NOTE UNE RECRUDESCENCE DES ATTAQUES INFORMATIQUES :

- Les conditions de travail (télétravail, effectifs réduits, ...) sont inhabituelles et déstabilisantes ;
- L'ambiance anxiogène liée à la gestion de crise est génératrice de comportements à risque ;
- L'actualité est propice à la génération d'escroqueries ou d'actes malveillants.

EXEMPLES D'ATTAQUES SUSCEPTIBLES DE SE PRODUIRE :

- En se faisant passer pour notre direction, un fournisseur ou une connaissance, en prétextant un problème informatique, dans le but de bloquer l'ordinateur, le smartphone de la victime ou de lui soutirer de l'argent ;
- Mise en ligne de fausses attestations de déplacement sans limite de date, dans le but de collecter des données personnelles ou des paiements ;
- Déploiement de logiciels malveillants (type rançongiciels (« ransomware »)) via de fausses applications pour smartphone, censées suivre l'évolution du virus ;
- En utilisant la technique habituelle de l'hameçonnage (« phishing ») pour prendre une fausse identité officielle (site du ministère de la santé par exemple), afin de faire cliquer la victime sur un lien frauduleux dans un mail ou SMS.

BONNES PRATIQUES POUR EVITER CES ATTAQUES

- Vérifier l'identité de leur expéditeur, en cas de doute, supprimer le mail;
- Ne surtout pas cliquer sur les liens suspects ;
- Ne se connecter que sur des sites officiels (ceux qui se terminent par « gouv.fr » par exemple), et ne pas cliquer sur les liens présents dans les emails des pseudos institutions;
- Ne pas propager ces messages ;
- Ne jamais communiquer son mot de passe à quiconque, et verrouiller son ordinateur à chaque départ de son poste de travail, même pour une durée courte ;
- Ne jamais communiquer de données personnelles à quiconque ou sur aucun site sans en avoir vérifié la source ;
- Ne télécharger pas de logiciel, ne supprimer pas de logiciel préinstallé sur votre ordinateur
- Ne pas connecter de périphériques de stockage externe (clé USB par exemple) à son ordinateur.

REFLEXE IMPERATIF EN CAS D'ATTAQUE

En cas de suspicion d'attaque (blocage du poste informatique par exemple), se déconnecter immédiatement et éteindre son ordinateur.