cecom
Cabinet d'expertise comptable

Socogestion
entreprises

Covid-19 : appel au renforcement des mesures de vigilance Cyber

De quoi s'agit-il ?

Une majorité de professionnels du chiffre est en télétravail. Dans ce contexte très particulier, les cybercriminels sont opportunistes et ne passent jamais à côté de ce type d'occasion, ce qui entraîne un accroissement massif des cyberattaques.

Le site Cybermalveillance du gouvernement (https://www.cybermalveillance.gouv.fr/)appelle à ce propos à un renforcement des mesures de vigilance en matière de cybersécurité pour faire face à l'explosion des actes malveillants sur le net.

Si les techniques utilisées ne sont pas différentes de celles précédemment constatées, elles ont toutes pour point commun d'exploiter la pandémie actuelle et la crainte des télétravailleurs, qui face à l'urgence, sont moins méfiants et tombent parfois dans le panneau.

Quels bons réflexes à adopter ?

Un simple clic sur un lien infecté contenant des informations soi-disant importantes sur le virus peut avoir des incidences dramatiques.

Redoublez donc d'attention pour ne pas tomber dans les pièges des cybercriminels :

+ Vérifiez la fiabilité et la réputation des sites que vous visitez.

Exemple : faux sites de ventes de masque chirurgical, appels aux dons relatifs au coronavirus…

+ **Soyez vigilants aux fausses informations**, pour rester informé sur la situation, référez-vous au site dédié du gouvernement.

Exemple : sites non officiels proposant l'attestation de déplacement dérogatoire pour collecter vos données.

+ **Méfiez-vous des mails sur le thème Covid-19** : ne cliquez pas sur les liens et n'ouvrez pas les pièces-jointes.

Exemple : des cybercriminels ont usurpé l'identité du Conseil National du Barreau via une lettre d'information COVID 19, proposant à ses membres le paiement de la mise à jour des plugins de sécurité des clés avocats. Il s'agit évidemment d'une arnaque !

+ Gardez un esprit critique, ne vous précipitez pas et prenez toujours le temps de la réflexion.

+ **Ne téléchargez vos applications que depuis les sites officiels** des éditeurs et ne téléchargez jamais de programmes depuis un mail si vous n'êtes pas absolument certain de son origine.

+ **Faites régulièrement des sauvegardes de vos données** et gardez une copie déconnectée.

+ **Appliquez les mises à jour de sécurité** sur vos équipements connectés (serveurs, ordinateurs, téléphones, tablettes…) dès qu'elles sont disponibles.

+ **Utilisez des mots de passe uniques et solides**, ne les communiquez jamais (qu'elle qu'en soit la raison) et activez la double authentification chaque fois que possible.

+ **Soyez vigilants aux changements** de RIB de vos fournisseurs et faites un contre-appel à un numéro déjà référencé en cas de doute

…