CORONAVIRUS – COVID-19 : Appel au renforcement des mesures de vigilance cybersécurité

Publié le 16 mars 2020

coronavirus Cybersécurité

136250 Temps de lecture : 11 min

La situation de crise mondiale générée par l'épidémie du CORONAVIRUS – COVID19 suscite des craintes légitimes. Comme à chaque événement exceptionnel, il faut avoir conscience que les cybercriminels cherchent à tirer profit de la précipitation et de la baisse de vigilance des personnes directement ou indirectement concernées pour les abuser et qui va se retrouver amplifiée par l'accroissement de l'usage numérique lié aux mesures de confinement. Il est donc primordial de redoubler d'attention pour ne pas tomber dans leurs pièges.

L'épidémie du CORONAVIRUS – COVID19 génère une situation de crise mondiale. Cette situation suscite des craintes et des inquiétudes légitimes des populations qui cherchent à rester informées ou les moyens de se protéger.
Parallèlement, les mesures décidées de confinement et de télétravail vont intensifier les usages numériques et par voie de conséquence, les risques inhérents à leur utilisation.

Cette situation de crise, d'urgence et d'inquiétude représente une véritable aubaine pour les cybercriminels qui jouent sur les peurs et les précipitations pour commettre leurs forfaits.
Ainsi un accroissement des cyberattaques et des cyberescroqueries liées à la crise du CORONAVIRUS – COVID19 est

prévisible. De nombreuses campagnes de cyberattaques liées à cette crise sont déjà observées dans le monde et la France n'a aucune raison de demeurer épargnée.

Voici une liste non exhaustive des pièges à éviter et bonnes pratiques à appliquer.

CORONAVIRUS – COVID-19
Tous publics :

– Méfiez-vous des messages (mail, SMS, chat…) ou appels téléphoniques d'origine inconnue ou inattendus :
L'hameçonnage (ou *phishing*) reste le premier vecteur d'attaque pour vous dérober des informations personnelles, professionnelles ou bancaires en vous attirant sur de faux sites officiels à la promesse d'une (trop) bonne affaire, d'un remboursement, d'une confirmation de commande, d'un colis en attente, d'un problème de sécurité… Ces messages peuvent également contenir une pièce-jointe malveillante (virus) ou vous inciter à vous rendre sur un site piégé pour infecter votre terminal.
Dans certains cas, les virus contenus dans ces pièces-jointes peuvent aller jusqu'à bloquer votre matériel voire chiffrer vos fichiers et vous réclamer une rançon pour en retrouver l'accès (voir les rançongiciels ou *ransomware*) .
Face à ce type de messages, ne cliquez pas sur les liens, n'ouvrez pas les pièces-jointes et en cas de doute, confirmez en contactant directement l'organisme qui prétend vous l'avoir envoyé.

– Ne téléchargez vos applications que depuis les sites ou magasins officiels des éditeurs : Dans le cas contraire, vous prendriez le risque d'installer une application piégée qui pourrait vous dérober vos informations personnelles ou bancaires, voire infecter votre machine avec un rançongiciel (*ransomware*) qui pourrait bloquer l'accès à votre machine ou chiffrer vos fichiers en vous demandant une rançon.
Évitez également tous les sites qui propose « gratuitement » des applications payantes et qui sont généralement piégées.

– Vérifier la fiabilité et la réputation des sites que vous visitez, que ce soit pour vous informer ou réaliser un achat.
Avant de fournir des informations personnelles ou bancaires, assurez-vous du sérieux du site sur lequel vous comptez vous inscrire ou commander en consultant les avis et en recherchant sur votre moteur de recherche d'éventuelles malversations connues.
Au moindre doute, abstenez-vous !
Avec la crise du CORONAVIRUS – COVID19 on voit fleurir de faux sites de ventes de masque chirurgical (FFP2), de gel hydroalcoolique, de téléconsultation médiale, de médicaments miracles ou de vaccins expérimentaux qui n'existent évidemment pas et qui n'ont d'autres objectifs que de vous escroquer. Les cybercriminels pourraient même vous livrer des produits périmés ou contrefaits qui mettraient en danger votre santé ou celle de vos proches.

À noter l'existence également de nombreux sites qui proposent des **attestations de déplacement dérogatoire** et des **justificatifs de déplacement professionnel** payants ou à remplir en ligne.

L'utilisation de ces sites est fortement déconseillée car elle présente un risque significatif de perte/vol de données personnelles voire d'escroqueries.
Les attestations et justificatifs officiels sont **gratuitement téléchargeables** sur le site du ministère de l'Intérieur.

– **Soyez vigilants aux fausses informations :** Qu'il s'agisse de propos excessivement catastrophistes ou qui évoquent des solutions miraculeuses face au CORONAVIRUS – COVID19, soyez méfiant avec tout ce que vous pouvez voir sur Internet, les forums ou les réseaux sociaux car ils regorgent de fausses informations et de rumeurs infondées et farfelues. Ne relayez pas d'information que vous n'avez pas pu vérifier depuis une source officielle. Pour rester informé sur la situation, référez vous au site dédié du gouvernement.

– **Attention aux appels aux dons frauduleux :** De nombreux appels aux dons et diverses cagnottes relatifs au CORONAVIRUS – COVID19 ne manqueront pas d'être lancés pour faire face aux difficultés individuelles ou collectives engendrées par la situation. Avant de verser des fonds, assurez-vous bien que vous n'êtes pas confronté à une escroquerie comme il ne manquera pas d'en fleurir pour abuser vos souhaits de solidarité.

CORONAVIRUS – COVID-19
Professionnels :

– **Soyez attentifs aux fausses commandes ou aux modifications de virements bancaires frauduleux :** L'accroissement de l'usage du télétravail et de la dématérialisation des procédures qui en découlent, associé aux difficultés économiques inhérentes à la situation de crise du CORONAVIRUS – COVID19 présentent un risque accru d'escroqueries à la fausse commande ou aux modifications de coordonnées de virement bancaire (FOVI/BEC) en usurpant l'identité d'un employé pour récupérer son salaire ou d'un fournisseur pour régler les factures ou encore émanant d'un dirigeant sous le sceau du secret. Avant toute prise en compte de commande suspecte, de demande de changement de RIB ou de demande de virement « exceptionnel », faites confirmer en contactant directement le demandeur et faites valider l'opération par votre hiérarchie.

– **Ne baissez pas la garde, au contraire, montez-là !** L'activité des entreprises et des organisations est déjà impactée par la crise du CORONAVIRUS – COVID19. La préservation de leurs actifs doit donc relever de la priorité de tous et aux premiers rangs desquelles la préservation de la sécurité de leurs systèmes d'information qui sont souvent au coeur de leur fonctionnement. Une intensification des cyber attaques de type «vol de données » et/ou rançongiciels (*ransomware*) sur les réseaux d'entreprises, cherchant à jouer sur leur possible baisse de vigilance ou défaut d'organisation, est donc prévisible. Les mesures de sécurité visant à détecter ou éviter les cyber attaques doivent donc être renforcées : mises à jour de sécurité, renforcement des procédures d'authentification pour le télétravail, supervision de sécurité, sensibilisation du personnel…

Appliquons tous les gestes élémentaires de cybersécurité pour rester au mieux protégés :

– Ne vous précipitez pas et prenez toujours le temps de la réflexion/confirmation

– Faites régulièrement des sauvegardes de vos données (ordinateurs, téléphone…) et gardez en une copie déconnectée

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

– Utilisez des mots de passe uniques et solides et activez la double authentification chaque fois que possible.

Article mis à jour le 19.03.2020

Pour assurer votre cybersécurité et rester informé, suivez Cybermalveillance.gouv.fr sur les réseaux sociaux et consultez/relayez notre kit de sensibilisation aux usages du numérique :

À lire aussi :

La situation de crise et de confinement liée à l'épidémie du CORONAVIRUS – COVID-19 engendre une intensification du recours au télétravail, augmentant considérablement les risques de sécurité pour les entreprises et organisations qui y recourent. Voici les recommandations à suivre pour préserver au mieux la sécurité informatique des collaborateurs et des employeurs.