S'adapter et réagir aux situations exceptionnelles : renforcement des mesures de vigilance cybersécurité

19 mars 2020

« Il ne faut pas paniquer sur le cyber. Il faut cependant être très vigilant vis-à-vis de l'adaptation très rapide des petites arnaques : la crise sanitaire est une thématique supplémentaire pour escroquer les gens »

explique ainsi Guillaume Poupard, directeur de l'Agence nationale de sécurité des systèmes d'information (Anssi), le pompier numérique de l'Etat.

SOYONS VIGILANTS

- Les pirates informatiques et escrocs profitent davantage de cette crise que nous traversons. Elle leur offre tout un champ de nouvelles opportunités à travers de nouvelles cibles et un sujet au centre de toutes les attentions.
- Les Cybercriminels ont déjà démontré leur capacité à s'adapter à l'actualité et à profiter des opportunités qui se présentent pour attaquer les systèmes d'information en quête de profit facile.
- Les nouveaux télétravailleurs sont de nouvelles cibles, les nouveaux moyens utilisés pour accéder aux SI de l'entreprise sont de nouvelles cibles, et le sujet même de la pandémie est un inducteur de stress qui modifie les comportements des utilisateurs.

S'adapter et réagir aux situations exceptionnelles : renforcement des mesures de vigilance cybersécurité

almond

19 mars 2020

DES GESTES BARRIÈRES SIMPLES ET DES BONNES PRATIQUES DOIVENT ÊTRE ADOPTÉS ET APPLIQUÉS POUR ÉVITER TOUT RISQUE D'ATTAQUES CYBERCRIMINEL

- Méfiez-vous des messages (mail, SMS, chat…) ou appels téléphoniques **d'origine inconnue ou inattendus,** des liens suspicieux envoyés via whats'app ou Facebook.
- N'installez pas **d'applications en provenance d'un site Internet** : ne téléchargez que des applications appartenant à des magasins officiels (Apple Store et Google Play Store).
- Soyez vigilants aux **fausses informations** : vérifiez toujours la source de l'information et ne propagez aucune information douteuse.
- Faites régulièrement des **sauvegardes de vos données** (ordinateurs, téléphones…) et gardez en une copie déconnectée et en lieu sûr.
- 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.

S'adapter et réagir aux situations exceptionnelles : renforcement des mesures de vigilance cybersécurité

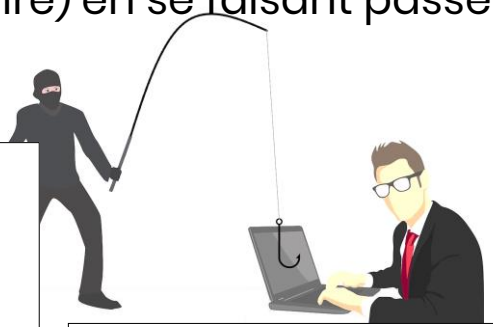
almond

19 mars 2020

PLUSIEURS TENTATIVES ET PLUSIEURS CAS DE FRAUDE ONT DÉJÀ ÉTÉ IDENTIFIÉS DEPUIS CES DERNIERS JOURS

Des campagnes d'hameçonnage

4 000 sites internet liés au nouveau coronavirus avaient été créés dont 5 % utilisés à des fins d'hameçonnage. Une technique qui consiste à extorquer des informations personnelles (mot de passe, code de carte bancaire) en se faisant passer pour un site légitime.



Une nouvelle **campagne de phishing du coronavirus répand le cheval de Troie Emotet**. Elle utilise un faux rapport sur l'épidémie pour inciter les destinataires des e-mails à ouvrir un document qui détaille les mesures à prendre pour prévenir l'infection. Ironiquement, en prenant les mesures détaillées dans l'e-mail, les victimes téléchargent un virus appelé Emotet.

Des e-mails de phishing envoyés par des pirates se faisant passer pour des représentants de l'OMS.

Des courriels d'hameçonnage se sont fait passer pour les centres pour le contrôle et la prévention des maladies, américains dans l'espoir de duper les destinataires.

S'adapter et réagir aux situations exceptionnelles : renforcement des mesures de vigilance cybersécurité

almond

19 mars 2020

PLUSIEURS TENTATIVES ET PLUSIEURS CAS DE FRAUDE ONT DÉJÀ ÉTÉ IDENTIFIÉS DEPUIS CES DERNIERS JOURS

Des virus informatiques et des arnaques liés au Covid-19

Mis à part les courriels qui poussent **des rançongiciels et des virus** exigeant une rançon, ou des logiciels malveillants conçus pour récupérer les identifiants des comptes bancaires...,les autorités craignent davantage, avec cette crise, **l'émergence et la propagation de pratiques commerciales trompeuses**, par exemple des sites qui vendent des masques mais ne les livrent jamais ou qui délivrent du faux gel hydroalcoolique. Des appels aux dons frauduleux sont également à craindre.

Une application mobile « COVID19 Tracker », piège les internautes en leur proposant de suivre en temps réel l'évolution de l'épidémie près de chez soi, pour installer un **ransomware sur le téléphone et le bloque.**