

Coronavirus : le Cesin met en garde contre le phishing

Comment se protéger des cyber-attaques, en pleine crise sanitaire du coronavirus ? La présidente du Cesin, Club des experts de la sécurité de l'information et du numérique, a adressé [un message](#) de soutien et de mise en garde à ses membres : « Nous avons pu observer les premiers malwares qui infectent des sites et Apps concernant le coronavirus. Par exemple, un malware Corona-virus-Map.com.exe. Et bien d'autres. » souligne [Mylène Jarrossay](#).

Première recommandation : une communication soutenue vers les collaborateurs peu habitués au télétravail et susceptibles de se faire piéger par des campagnes de phishing en lien avec le coronavirus.

Et de citer :

- « – des messages invitant à se connecter sur des espaces partagés online frauduleux, glissés au milieu du foisonnement d'espaces partagés légitimes montés en urgence
- des mails malveillants semblant venir du Ministère de la Santé et autres autorités
- des mails malveillants usurpant l'identité du helpdesk
- des fausses demandes RH liées à l'organisation du travail à domicile
- Des apps et sites malveillants supposés donner des renseignements sur la crise
- Des faux appels téléphoniques du help desk »

Pour les RSSI, la présidente énumère des chantiers prioritaires qui s'imposent sur les agendas :

- » – La résistance des connexions VPN et des solutions de MFA
- Les postes de travail massivement sortis de l'entreprise : pour certaines personnes, c'est nouveau, les règles de protection de l'accès physique et logique du poste à la maison n'est pas encore acquise
- La non-disponibilité de certains prestataires débordés
- Certaines fonctions de surveillance ou d'administration que vous aviez interdit de faire à distance
- Les listes de personnes et de coordonnées qui circulent assez largement pour la réorganisation du travail « .