Comme si nous n’avions pas assez de soucis avec le virus Covid19, depuis plusieurs jours une vague d'attaque utilisant le logiciel malveillant "emotet" se déroule sur internet.

Ce malware (virus, logiciel malveillant) est **particulièrement dangereux, sournois et difficile à éradiquer**.
Il a pour objectif premier de **récupérer** sur les machines infectées **les mots de passe, comptes de courriels et adresses de messageries** (liste de contact) etc.

Sa principale méthode d'infection est l'envoi de mails créés de toutes pièces et qui présentent quelques-unes des caractéristiques suivantes:
- adresse d'expéditeur qui semble légitime (expéditeur connu et de confiance),
- sujet du message indiquant un message à une réponse précédente ("Re:..."),
- reprise d'une partie d'un véritable message de l’expéditeur (récupéré sur la machine infectée par le logiciel malveillant),
- pièce jointe de type suite MS Office (actuellement, plutôt word : .doc ou .docx).

En conséquence:
- n'ouvrez pas les pièces jointes par défaut (word, excel, PowerPoint, pdf, etc.)
- en cas de doute, validez l'envoi du mail par un appel téléphonique auprès de l’expéditeur du mail
- si malgré tout cela, le drame est arrivé, déconnectez immédiatement la machine infectée du réseau.

Et n'oubliez pas: seule une sauvegarde non connectée (disque dur USB débranché par exemple) à la machine pourra vous permettre de restaurer votre système contaminé…

Plus d’information (en français) : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-019/