Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET
DE SAÔNE-ET-LOIRE

Mâcon, le 12 avril 2020
11h00

# INFORMATION

En toute saison, les virus informatiques sont actifs. Ennemis invisibles, les cyberdélinquants sont à l'action de façon encore plus intense depuis les mesures de confinement. La sollicitation quotidienne et généralisée des systèmes d'information de communication (télétravail, école à distance, audio et visioconférence,...) nécessite une vigilance accrue et l'application de mesures, souvent simples, de protection. Veillons à ne pas ajouter à la crise sanitaire une crise numérique et informatique qui paralyserait nos moyens de communication, d'échange et de travail.

Les menaces d'attaques sont variées. Les plus fréquentes sont les campagnes de « phishing » (ou hameçonnage). Elles consistent à l'envoi d'emails frauduleux utilisant différentes thématiques d'actualité (santé, économie, appels aux dons…) en usurpant souvent l'identité d'organismes officiels (organisation mondiale de la santé, agence régionale de la santé, direction générale des finances publiques, impôts.gouv.fr, banques, plateforme de livraison,...) afin de recueillir des informations personnelles, le plus souvent coordonnées bancaires et codes secret. Aucun organisme officiel ne sollicite ce type d'information ni par messagerie, ni pas SMS ni même par appel téléphonique. D'autres formes d'arnaques ont pu également être constatées comme des sites frauduleux mettant en vente des masques ou du gel hydroalcoolique, des chantages à la webcam prétendue piratée, ou des applications prenant le contrôle de l'appareil jusqu'au versement d'une rançon.

Redoublez de vigilance et appliquez quelques « mesures barrière » et conseils simples pour protéger ordinateurs professionnels et personnels face aux virus et aux personnes malveillantes :
- utilisez des mots de passe de qualité, complexes (au moins 8 caractères, majuscules, chiffres, signes spéciaux) et différents selon vos outils numériques et vos applications ;
- ayez un système d'exploitation, des logiciels et un antivirus à jour, et effectuez des sauvegardes régulières ;
- assurez une étanchéité entre vos outils personnels et professionnels, en n'utilisant pas par exemple de clé USB entre les deux systèmes ;
- ne cliquez trop vite sur des liens dans les emails, soyez vigilant avant d'ouvrir des pièces jointes à un message, même lorsqu'il provient d'un correspondant qui paraît fiable;
- contrôlez la diffusion d'informations personnelles y compris sur les réseaux sociaux ;
- ne relayez jamais de canulars ou de messages de type chaînes (lettres, porte-bonheur ou pyramides financières, appel à solidarité, alertes virales, etc) qui saturent les systèmes et propagent les virus.

Que vous soyez particulier ou professionnel, retrouvez tous les conseils pour vous prémunir contre les cybermenaces sur les sites publics officiels :
- site d'assistance et de prévention et du risque numérique : https://www.cybermalveillance.gouv.fr
- site de l'Agence nationale de sécurité des systèmes d'informations (ANSSI): https://www.ssi.gouv.fr
- site de la commission nationale informatique et liberté (CNIL), en particulier sa page dédiée en situation de pandémie coronavirus : https://www.cnil.fr/fr/coronavirus-covid-19