

Note de service

- Destinataire :** Tout le personnel du CIUSSS de l'Est-de-l'Île-de-Montréal
- Expéditeur :** Élodie Dormoy, directrice adjointe de la qualité, gestion des risques et éthique (DQÉPÉ)
Stéphane Gagnon, conseiller cadre – responsable de la sécurité de l'information (DQÉPÉ)
Olivier Tine, officier de sécurité de l'information (DRT)
- Date :** Le 21 septembre 2020
- Objet :** Rançongiciel – Hausse des cyberattaques
-

Bonjour,

Le secrétariat du Conseil du trésor a porté à l'attention du centre opérationnel de cyberdéfense du secteur de la santé (COCD) d'une augmentation d'incidents de sécurité. L'utilisation de logiciels malveillants de type « rançongiciel » est en cause.

Un rançongiciel est un logiciel malveillant qui s'installe sur votre appareil à votre insu. En quelques secondes, il crypte vos données ou encore limite l'utilisation de votre appareil en ayant pour unique objectif de demander une rançon.

Conseils pour se protéger contre les rançongiciels

- Pensez avant de cliquer sur un lien ou une pièce jointe dans un courriel qui semble vous offrir un bénéfice sans que vous n'ayez rien demandé.
- Validez la légitimité du courriel ou du site Web avant de fournir quelques informations ou quelques accès que ce soit (code d'utilisateur et mot de passe)
- Mettez à jour régulièrement tous les logiciels de votre appareil (incluant votre logiciel antivirus). Les mises à jour incluent des protections supplémentaires contre les récentes attaques répertoriées.
- Sauvegardez! Sauvegardez! Sauvegardez! Faites régulièrement des copies de sauvegarde afin de pouvoir récupérer vos données en cas d'attaque.

Si vous êtes victime d'un rançongiciel sur votre appareil au bureau, vous devez contacter le plus rapidement possible le service informatique via une requête Octopus ou en contactant le 5656.

Nous vous remercions de l'attention que vous porterez à ce message.

