Ordonnances du docteur : Se protéger contre les logiciels malveillants et les rançongiciels

Bienvenue à la dernière semaine du Mois de la sensibilisation à la Cyber Sécurité (MSCS)! Cette semaine, nous traiterons des logiciels malveillants et des rançongiciels. Personne n'aime être infecté, y compris vos appareils. Il est important de connaître la manière de prévenir les attaques par des logiciels malveillants et des rançongiciels pour vous garder, vous et votre organisme en sécurité!

Bilan de santé cybernétique du MSCS

Infection : Logiciel malveillant

Un logiciel malveillant, aussi connu sous le nom de « maliciel », est un logiciel ou un code déployé sur un appareil dans le but de compromettre la confidentialité, l'intégrité ou la disponibilité de vos données ou de votre système. Les logiciels malveillants peuvent comprendre des virus, des vers et des chevaux de Troie. Vous pouvez être infecté en téléchargeant accidentellement un logiciel malveillant alors que vous essayez de télécharger ce que vous pensez être un logiciel ou un document légitime.

Prévention :

- Soyez attentif et vigilant lorsque vous téléchargez des logiciels ou des documents.
- Vérifiez toujours que l'adresse Web (URL) est exacte en vérifiant les fautes d'orthographe et les logos mal représentés avant de cliquer.
- Évitez les attaques par hameçonnage. Le fait de cliquer sur un lien ou de télécharger un fichier à partir d'un courriel malveillant est l'une des méthodes de diffusion les plus courantes utilisées par les cybercriminels pour déployer des logiciels malveillants ou des rançongiciels sur leurs victimes. Voir notre Article de la deuxième semaine du MSCS pour plus de détails sur l'hameçonnage.

Infection : Rançongiciel

Un rançongiciel est un type de logiciel malveillant qui rend les données inaccessibles en verrouillant votre appareil ou en cryptant vos fichiers. Il peut se propager à partir de votre appareil et infecter le reste des données de votre organisme. Les auteurs de menaces demandent souvent de l'argent en échange de l'accès à vos fichiers ou menacent de divulguer des renseignements privés s'ils ne sont pas payés.

Prévention :

- Pour obtenir les derniers conseils et astuces sur la gestion des rançongiciels, consultez cette ressource sur les cyberattaques.

- Sauvegardez régulièrement vos données afin de pouvoir récupérer les données compromises par une attaque de rançongiciel.

Remède : Logiciel malveillant et rançongiciel

- Signalez l'attaque à votre organisme et aux forces de l'ordre pour éviter que d'autres attaques ou une infection par un logiciel malveillant ne se propagent.
- Changez tous les mots de passe de vos comptes en ligne. Pour plus de conseils, consultez cet article sur les mots de passes.

Une enquête menée par CyberEdge en 2021 a révélé que 61,2 % des répondants canadiens ont eu affaire à des rançongiciels en 2021. Il est important de prendre des mesures préventives, mais il est également important de penser au MOMENT où vous serez attaqué et non à la POSSIBILITÉ d'être attaqué. Veillez à rester à jour dans vos formations de sensibilisation à la cybersécurité afin d'être prêt à vous protéger, vous et votre organisme, contre les attaques de logiciels malveillants ou de rançongiciels!