Trois conseils de cybersécurité

C’est le Mois de la cybersécurité! Chaque octobre, le Groupe Erb observe le Mois de la cybersécurité, qui représente une occasion en or pour son département des TI de partager son expertise et d’informer le personnel de l’importance de la cybersécurité. En effet, la sensibilisation à la cybersécurité empêche les employés de cliquer potentiellement sur un lien vers une fraude qui porte atteinte à la sécurité ou qui expose des informations privées. La cybersécurité en entreprise est essentielle à chaque secteur de l’industrie. Toutefois, la cybersécurité est devenue une priorité dans le domaine du transport et de la logistique, puisqu’un grand nombre d’entreprises de transport commencent à utiliser des infrastructures et des plates-formes numériques dans le cadre de leurs activités commerciales.

On se préoccupe de plus en plus de cyberattaques. Une seule cyberattaque peut s’avérer coûteuse à l’entreprise en termes de ressources, de temps et de cas d’atteinte à la vie privée. En fait, selon le Cyber Defense Report, publié en 2021, 86 % des entreprises canadiennes ont été victimes d’au moins une cyberattaque en moins d’un an. Il est donc primordial d’être au fait des meilleures pratiques en matière de cybersécurité, car aucune entreprise ni aucun individu n’est à l’abri d’une cyberattaque.

Tout au long du mois d’octobre, notre talentueuse équipe des TI enverra un nouveau conseil en matière de cybersécurité chaque semaine, et ce, pour aider les employés à se sentir en sécurité en ligne, autant à la maison qu’au travail! Voici trois de nos meilleurs conseils de cybersécurité pour vous aider à rester en sécurité en ligne cette année.

Authentification multifactorielle (AMF)

Vous est-il déjà arrivé de saisir un code unique en plus de votre mot de passe? C’est ce qu’on appelle l’AMF. Comme le nom le sous-entend, il s’agit d’une mesure supplémentaire qui vous permet d’accéder au compte voulu. L’AMF ne rend pas pour autant impénétrables vos comptes en ligne. Par contre, elle vous permet de savoir si quelqu’un d’autre tente d’y accéder. L’AMF se présente normalement sous la forme

d’un code envoyé par courriel, par message texte ou par appel téléphonique au moyen d’une application d’authentification tierce offerte par Google ou Microsoft.

L’AMF constitue la meilleure mesure possible pour protéger vos comptes en lignes. Dans le cas d’un piratage informatique d’un site Web ou d’une entreprise, votre compte reste inaccessible au pirate informatique, car il doit avoir votre téléphone en sa possession pour accéder au code. Et même s’il connaissait votre mot de passe, il aurait besoin de votre code unique pour y accéder. Alors, ne donnez jamais votre code AMF à qui que ce soit!

Phishing

Chacun sait qu’un hameçon sert à faire la pêche, mais l’hameçon qu’on utilise en ligne, c’est une tout autre affaire. Si vous utilisez un ordinateur ou un cellulaire, vous avez probablement été témoin d’une tentative d’hameçonnage, que vous en soyez conscient ou non. L’hameçonnage est un type de fraude psychologique qui vise à duper quelqu’un, afin qu’il fournisse des informations sensibles telles que les mots de passe ou qu’il télécharge un logiciel malveillant. Un courriel, un appel téléphonique ou un message texte peut contenir de l’hameçonnage. Alors, ne donnez jamais vos renseignements à un inconnu!

Les experts en cybersécurité prévoient qu’environ 98 % des cyberattaques emploient des méthodes liées à la fraude psychologique, laquelle implique l’utilisation de la peur et l’incertitude de l’utilisateur afin qu’il révèle les informations voulues. Vous pouvez vite comprendre qu’il s’agit de l’hameçonnage en analysant le message. Par exemple, il peut contenir une phrase comme : « Vous avez gagné un voyage! Veuillez entrer vos renseignements personnels » ou « Votre compte sera verrouillé à moins que… ». Si vous tombez sur de l’hameçonnage au travail, signalez-le au département des TI puis supprimez le message. À la maison, supprimez le message, puis bloquez et signalez l’expéditeur. Vous croyez déjà avoir été victime d’une fraude en ligne? Modifiez le mot de passe de votre compte compromis et effectuez immédiatement une analyse antivirus pour vous débarrasser des fenêtres publicitaires ou d’autres choses qui ralentissent votre ordinateur.

Fausse extension de Google Chrome

Aujourd’hui, Google Chrome est un navigateur Web des plus populaires et fiables. En effet, plus de six personnes sur dix utilisent Google Chrome. Plus les utilisateurs font confiance à cette plate-forme, plus les occasions pour les fraudeurs en ligne de créer de faux logiciels malveillants et de se présenter comme s’ils étaient de la marque

Google sont nombreuses. Ensuite, ils ciblent une personne qui n'est pas équipée pour identifier une cybermenace.

Les pirates informatiques ont créé une fausse extension de Google Chrome appelée *Internet download manager* (gestionnaire de téléchargements) qui est disponible depuis longtemps et qui nuit à votre ordinateur à votre insu. Avant de télécharger une « extension de Chrome » ou une mise à jour à ajouter à votre navigateur Web, assurez-vous d'abord de vous **renseigner** sur elle ou de **demander** des précisions au département des TI si vous êtes incertain. En plus, lorsque vous cliquez sur un lien, veuillez porter une attention particulière aux éléments suivants :

- L'ouverture d'un nouvel onglet;
- Les sites Web non pertinents; et
- Les fenêtres publicitaires qui vous demandent de télécharger d'autres logiciels ou fichiers.

Plus Erb devient une entreprise sans papier, plus nous sommes reconnaissants envers notre équipe de professionnels en TI qui protègent nos systèmes et qui travaillent d'arrache-pied pour créer des ressources et des outils permettant aux employés d'être conscients des cybermenaces, de la prévention et des processus. Il s'agit d'une merveilleuse expérience d'apprentissage dans le contexte du Mois de la cybersécurité!

« Je pense qu'il est primordial de reconnaître le Mois de la cybersécurité, car il renforce notre engagement de tenir les employés au fait de la sécurité en ligne et de constamment rester à l'affût des cybermenaces, surtout dans les courriels, qu'ils utilisent chaque jour » nous dit Darryn Nafziger, vice-président des technologies de l'information (TI) d'Erb.

À l'ère numérique, les menaces de cybersécurité ne cessent de s'accroître partout dans le monde à une plus grande vitesse année après année. Les pirates informatiques deviennent de plus en plus créatifs, ce qui signifie que le nombre de violations ne cesse d'augmenter et de cibler ceux qui sont vulnérables aux cyberattaques. Dans le fond, la cybersécurité est un sport d'équipe, allant de ceux qui établissent les stratégies de cybersécurité, les politiques et les cadres à ceux qui les mettent en pratique. Tout le monde doit y participer. Cette Halloween, je vous invite à suivre ces trois conseils pour vous permettre d'aider vos collègues et vos amis à rester calmes et à lutter contre la cybercriminalité un clic à la fois.