BLOQUONS LES PIRATES INFORMATIQUES QUI NOUS INFECTENT EN CETTE CRISE DE CORONAVIRUS (COVID-19)

Certains pirates informatiques sans scrupules ne se laissent pas attendrir par les effets tragiques du coronavirus (covid-19). Bien au contraire, ils y voient une occasion en or pour donner libre cours à leurs activités d'escroquerie et abuser de l'inquiétude généralisée. Ils scrutent nos recherches sur Internet pour obtenir plus de renseignements sur la situation ou trouver des références susceptibles de nous protéger … et nous attendent au détour.

Soyons d'une grande vigilance. Que ce soit à titre de personne, d'employé, d'employeur ou d'organisation, nous sommes tous à risque de poser une action qui permettrait à des pirates informatiques pernicieux de prendre le contrôle de notre équipement, ordinateur ou téléphone intelligent. Ils font preuve d'ingéniosité pour bloquer l'utilisation de nos appareils, nous soutirer nos informations ou même nous escroquer.

La situation requiert une attention particulière sur les façons de nous protéger contre plusieurs types d'attaques. Les pirates informatiques sont astucieux. Soyons-le tout autant en posant les bonnes actions pour contrecarrer leurs intentions frauduleuses.

TOP 5 DES ACTIONS À ÉVITER

1.Ouvrir un courriel qui pourrait nous hameçonner. Il faut être vigilant et détecter certains signes.

Un courriel provenant d'une connaissance ou d'une source sérieuse devrait présenter certaines caractéristiques :

- L'identité de l'émetteur du courriel doit être vérifiable et non pas seulement nous fier au nom affiché (pointer votre curseur sur le nom de l'émetteur pour afficher le courriel). Le compte pourrait également avoir été piraté et utilisé par un pirate informatique.
- Tout courriel véridique devrait contenir un objet portant sur son contenu et non pas un sujet vide ou générique qui pourrait être le signe d'un courriel frauduleux.
- Le courriel devrait contenir un texte complet et non pas seulement une directive d'ouvrir un fichier joint sans doute malintentionné.
- Le contenu d'un courriel en provenance d'une connaissance devrait être représentatif de la personne et non pas contenir un texte générique avec plusieurs fautes d'orthographe.
- Toutes les combinaisons de ce qui précède devraient nous alerter.

Tous les points suivants s'appliquent aux courriels.

2.Ouvrir un fichier, une photo ou un vidéo reçu par courriel et provenant de sources inconnues ou disponibles sur un site non officiel

- Le fichier pourrait contenir un logiciel malicieux (virus, rançongiciel, trousse administrateur pirate, logiciel espion, cheval de Troie, ver informatique, etc.) habileté à prendre le contrôle de notre ordinateur ou de notre téléphone intelligent.
- Dans certains cas, le fichier joint est protégé par un mot de passe pour éviter d'être détecté par les antiviraux.
- La même règle s'applique pour un courriel avec un contenu douteux en provenance d'une connaissance, car son ordinateur pourrait avoir été infecté par un logiciel malfaisant.

3.Sélectionner un lien vers un site sans connaitre ou vérifier sa validité

- Les pirates informatiques utilisent dans leurs courriels et sur des sites web, incluant des sites de références, des liens qui nous redirigent vers des sites hostiles qui nous fournissent de fausses informations en vue d'exécuter du code malicieux et infecter nos appareils ou encore nous demander des informations confidentielles. Même les téléphones intelligents sont vulnérables à ces types d'attaques.
- Très souvent le nom du lien joint n'est pas le vrai lien (il faut pointer notre curseur pour afficher le lien réel).
- Ne participons pas à des campagnes de financement sans en vérifier l'authenticité, car il s'agit d'un autre moyen pour nous soutirer de l'argent. Soyons sur nos gardes lorsque ces sites ne sont pas officiels et ne présentent que des motifs peu élaborés ni aucune référence sur ses responsables. Les pirates informatiques sont des experts au jeu des émotions et misent sur nos cordes sensibles pour nous arnaquer.

4.Fournir nos informations personnelles par courriel ou sur un site web.

- Cette approche est régulièrement utilisée par des pirates informatiques pour obtenir nos noms d'usager et mot de passe ainsi que notre information personnelle. Aucune entreprise ne procèderait de la sorte. Advenant un problème, nous recevrions alors une communication officielle qui, à la suite d'un processus d'identification formel, nous permettrait d'accéder à l'application en ligne de l'entreprise.
- Attention aux courriels en provenance d'une soi-disant connaissance qui nous demande des informations, de l'argent ou de poser une action. Cette approche est fréquemment utilisée pour déjouer notre vigilance à partir d'un compte piraté et d'ordinateur infecté par un logiciel malhonnête.
- Méfions-nous également des appels téléphoniques prétendant provenir d'entreprises ou d'instances gouvernementales. Il vaut mieux communiquer soi-même au numéro officiel pour valider le tout.

5. Installer un logiciel sur notre ordinateur ou téléphone intelligent sans en connaitre la validité.

- Installer de nouveaux logiciels sous prétexte qu'ils nous fourniront des informations ou faciliteront certaines actions face au coronavirus, est évidemment à proscrire. Très souvent, ces logiciels sont malveillants et prennent le contrôle de notre ordinateur ou téléphone dans le but de s'emparer de nos données (information et chiffres).

Les pirates informatiques font preuve d'une imagination débordante dans leurs approches pour tirer profit d'une situation, aussi catastrophique soit-elle. Demeurons particulièrement alertes et vigilants, même lorsque le contexte nous pousse à une plus grande ouverture d'esprit et à faire preuve de conscience sociale.

Il est déconseillé de valider l'authenticité de sites possiblement malicieux à partir de sites web génériques. Il est préférable de se référer à des sites gouvernementaux, de corps policiers ou spécialisés officiels. Google peut être d'une grande utilité pour faire certaines vérifications et fournir des informations, mais de grâce ne considérons pas tout ce que nous trouvons comme étant absolument valable, exact et vrai. Il faut savoir interpréter les résultats et vérifier la provenance de ces informations. Ce n'est pas parce que c'est sur Internet que c'est vrai!

Que faire si jamais nous croyons avoir été victimes d'une de ces supercheries?

- Porter une attention à tout changement sur notre ordinateur et téléphone intelligent et détecter tout comportement suspect ou inhabituel.
- Utiliser un logiciel antiviral ou de sécurité pour balayer le contenu de notre ordinateur ou téléphone intelligent pour détecter et éliminer des logiciels malveillants.
- Utiliser des logiciels plus spécialisés en fonction du type de logiciels malveillants auxquels nous sommes confrontés (virus, rançongiciel, trousse administrateur pirate, logiciel espion, cheval de Troie, ver informatique, etc.
- Réinstaller notre logiciel d'exploitation ou restaurer notre sauvegarde.
- Observer les communications réseau entre notre ordinateur et l'extérieur si nous possédons l'expertise pour interpréter ces informations.
- Contacter une entreprise spécialisée pour nous assister.

Tout comme dans le cas de la Covid 19, il vaut mieux prévenir que guérir! Faisons preuve d'une grande prudence télécommunicative!

SecurEcom Services-Conseils soutient les organisations dans la protection de leurs données, applications, infrastructure et aussi de leurs activités relatives à la cybersécurité en leur fournissant une expertise reconnue en gestion du risque.

Au cours des 20 dernières années, l'équipe aguerrie de SecurEcom composée d'experts de haut calibre en TI, en gestion du risque en TI et en cybersécurité, a accompagné une clientèle reconnue au Québec, au Canada et aux États-Unis.

Des entreprises réputées issues de divers secteurs dont les télécommunications, la finance, le transport, l'assurance, l'énergie, les technologies ainsi que de l'administration gouvernementale et publique ont eu recours aux services novateurs de SecurEcom dans leurs projets liés aux TI et à la cybersécurité et à la gestion du risque dans les TI.

N'hésitez pas à nous contacter : Alain Scherrer, associé principal

alain.scherrer@securecom.ca Tél. : 514 544-0442 poste 2320

Securecom.ca

Indik-dashboard.com