Les 7 cyber menaces les plus exploitées chaque jour | Le Net Expert Informatique

	Les 7 cyber menaces les plus exploitées chaque jour

Les cyber-attaques qui frappent les Etats ou les grandes entreprises ont beau être celles qui font le plus régulièrement l'actualité, les cybercriminels usent tout autant de techniques d'escroqueries plus basiques mais tout aussi efficaces, ciblant les individus. La plupart des gens n'étant pas assez informés sur les cyber menaces ou ne suivant pas les mesures de cybersécurité classiques, restent la proie des hackers via des failles pourtant très connues, et exposent leur entreprise à des attaques beaucoup plus importantes.

Il vous qui se reconnaîtraient – ou l'un de leurs collègues ou amis – dans l'un des 7 profils décrit ci-dessous, il est encore temps de perfectionner vos compétences en matière de cybersécurité !

J'ai tendance à cliquer très (trop) rapidement

Un clic peut être suffisant pour être infecté par un virus ou pour être redirigé vers un site web malicieux. Les hackers sont très bons pour créer des contenus destinés à leurrer les utilisateurs et les inviter à cliquer. Ce contenu piégé peut être un message important – parvenant venir d'une personne ou d'une société que vous connaissez bien et en laquelle vous avez confiance – technique que l'on appelle le spear phishing. Il peut aussi simplement s'agir d'un spam, d'une publicité proposant une promotion trop belle pour être vraie ou encore d'une fausse enquête vous demandant de donner certaines informations personnelles.
Aussi, avant de cliquer, une bonne précaution à prendre est de survoler le lien hypertexte avec sa souris pour voir apparaître l'URL de destination et ainsi vérifier sa légitimité. Les liens de phishing incluent toujours une petite erreur dans l'écriture du lien qui va donc mener vers un site factice ou infecter votre PC avec un malware. Deuxième précaution : portez plus d'attention aux comportements inhabituels. Une entreprise connue ne demande jamais des mots de passe et autres informations sensibles et n'envoie pas d'mails comportant des fautes d'orthographe ou des images de mauvaise qualité, etc. En d'autres termes, au moindre doute, ne cliquez pas !

J'ignore toujours les demandes de mises à jour

Les fournisseurs de solutions de sécurité investissent en permanence pour renforcer la sécurité de leurs produits face aux cyber-attaques et publient des patchs et mises à jour pour résoudre chaque problème rencontré. Toutefois, si ces mises à jours ne sont pas installées par les utilisateurs eux-mêmes, ceux-ci resteront vulnérables aux attaques. Les navigateurs web sont le meilleur exemple d'outils utilisés au quotidien et pouvant facilement être exploités par les hackers. Lorsque l'on sait que seulement 10% des utilisateurs d'Internet Explorer utilisent la dernière version du navigateur, il est évident que les failles à exploiter pour les hackers sont nombreuses.

Je suis friand de Free Wi-Fi

Les espaces de Free Wi-Fi vous ont permis d'être plus connectés ou encore d'éviter les frais de connexion exorbitants lorsque vous sommes à l'étranger. Ces connexions étant ouvertes à tout le monde et en continu, il est très facile pour les hackers d'intercepter les données qui transitent via le Wi-Fi. Utiliser le Wi-Fi gratuit, c'est bien, mais il est clairement recommandé de ne pas consulter son compte en banque ou encore réaliser des achats en ligne avec sa carte d'identité lorsque l'on est connecté via un réseau Wi-Fi public. Dès lors que vous utilisez régulièrement un réseau de Wi-Fi public pour travailler, vous devez être en mesure de vous connecter à un VPN pour renforcer la sécurité de votre connexion.

J'utilise des applications gratuites

Si vous êtes fan des dernières applications, jeux ou gadgets, vous devez savoir que certaines applications gratuites peuvent être infectées par des malwares. Celles-ci permettent aux hackers de collecter vos données à des fins malveillantes, sans que cela ne vous soit jamais notifié. Aussi, il est recommandé de télécharger des apps issues de sources connues.

J'utilise le même mot de passe pour tous mes comptes en ligne

Les hackers savent pertinemment que la plupart des gens réutilisent les mêmes mots de passe pour plusieurs sites. Ils sont ainsi décoder un mot de passe sur un site peu sécurisé et essayer d'utiliser ce même mot de passe sur des sites de vente très connus ou des réseaux sociaux sur lesquels vous pourriez avoir un compte, jusqu'à ce qu'ils trouvent des informations personnelles, financières ou même liées à votre entreprise. Le meilleur moyen de se prémunir de ce type de risques est d'utiliser des mots de passe compliqués et personnalisés pour chaque site web. Il existe de nombreux conseils en ligne pour savoir comment créer des mots de passe fort et facilement mémorisables.

Je ne verrouille jamais ma session

Le moyen le plus facile de dérober des données de valeur ou de pénétrer dans la vie privée d'une personne est d'accéder physiquement à son ordinateur non verrouillé puis de copier ses données ou de se connecter aux sites sur lesquels le mot de passe est enregistré et dont l'accès se fait automatiquement. Cela ne nécessite aucune compétence technique et, même si la personne ayat intentionnée est repérée par une caméra, cela ne permet absolument pas de la tenir pour responsable, en partant de la faille. Le conseil ici est évident, ne jamais laisser sa session ouverte sur son PC lorsque l'on s'absente.

Je partage énormément (trop) en ligne

Quel est le nom de jeune fille de votre mère ? Le nom de votre premier animal de compagnie ? Le nom de votre première école ? Ce sont autant de questions de sécurité qui vous permettent de récupérer votre mot de passe oublié, et il serait bien dommage que quelqu'un puisse retrouver ces informations sur votre profil FacebOok. Si vous êtes accro aux réseaux sociaux, mais que vous souhaitez vous protéger ainsi que votre entreprise des nombreuses menaces en ligne, vous pourriez commencer par restreindre l'accès à vos publications, à vos amis uniquement. Faites un nouveau tour sur votre profil et réexaminez vos posts.

De la même manière, informez-vous sur les termes et conditions des sites que vous fréquentez régulièrement dans la mesure ou certains d'entre eux pourraient déclarer collecter vos données et les utiliser pour de la publicité voire même les partager avec des sociétés tierces.

La cybersécurité commence avec vous !

Aussi évoqué que soit la technologie, ce que l'utilisateur fait reste la plus grande partie de l'équation à résoudre. Les sites web que vous utilisez et l'entreprise pour laquelle vous travaillez peuvent faire le maximum pour assurer la protection de vos données, ils restent toutefois dépendants de vos actes. L'humain est le maillon faible de la sécurité, et pour changer cela nous devons tous prendre nos responsabilités et jouer notre rôle. Les bonnes pratiques de cybersécurité qui commencent à la maison, avec nos données et terminaux personnels, peuvent être facilement étendues à nos vies professionnelles.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Formateur n°93 84 03041 84

Expert Informatique assermenté et Formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plaît ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.globalsecuritymag.fr/Christophe-Jolly-Cisco-France-Les,20150728,54749.html
Par Christophe Jolly, Cisco France