Ecrit par Echo du Mardi le 13 février 2022

Saint-Valentin : attention aux cyber-arnaques

Avec la Saint-Valentin, les amoureux du monde entier s'efforceront de trouver la meilleure façon de témoigner leurs sentiments. Mais en parallèle, les cybercriminels sembleront également être gagnés par l'esprit de cette journée.

« Comme chaque année, le 14 février, les amoureux célèbreront l'amour à travers le monde,explique Hervé Liotaud, vice-président Europe de l'Ouest chez Sailpoint société spécialisée dans gestion des identités et des accès numérique. Mais ce ne sont pas les seuls pour qui ce jour sera une fête. Les cyber-criminels savent aussi en profiter. Arnaques sur les sites de rencontre, ransomwares, usurpation d'identité, piège au colis… Toutes les techniques seront bonnes pour atteindre leur cible. »

La Saint Valentin : proie des hackers

« En principe, il n'est pas surprenant que les cyber-criminels exploitent des évènements spéciaux tels que des vacances ou des fêtes. Une large cible d'attaque s'ouvre toujours pour des pirates lorsque de

Ecrit par Echo du Mardi le 13 février 2022

nombreuses personnes s'intéressent en même temps à un sujet particulier, et deviennent donc vulnérables. La bonne nouvelle est que les consommateurs ne sont pas sans défense contre ce type d'attaque. »

Des attaques ciblées

« Les précédentes Saint-Valentin ont été fortement marquées par le nombre d'attaques de 'credential stuffing' (vol d'identifiants pour accéder à d'autres comptes) sur les sites de rencontre, dans lesquels des comptes utilisateurs ont été compromis. Les criminels créent régulièrement de faux profils d'utilisateurs avec de faux messages romantiques afin de cibler des personnes seules puis les incitent à leur transférer de l'argent. Chaque année, nous voyons aussi se multiplier les faux sites en ligne proposant une fausse liste de cadeaux mais une escroquerie bien réelle. Cette méthode frauduleuse est particulièrement rentable. Or cette année, une grande part des achats de cadeaux s'effectuera en ligne, les sites marchands en ligne sont d'autant plus susceptibles d'être la cible des cyberattaques. »

Comment s'en protéger ?

« Il est évidemment possible d'appliquer des mesures de sécurité pour atténuer les menaces qui pèsent sur la Saint-Valentin pour protéger les utilisateurs et leurs identités digitales contre ces attaques :

Méfiance lors des achats en ligne : il est primordial de ne faire confiance qu'à des fournisseurs connus et vérifiés, et d'accorder une attention particulière à leur professionnalisme. Ceci inclut, par exemple, la vérification du nom de domaine du site – beaucoup d'acteurs malveillants créent des plates-formes usurpant des noms d'enseignes bien connus, mais ajoutent parfois à la fin « .fr.com » au lieu de simplement « .fr ». Pour s'assurer d'un site authentique, il faut éviter de cliquer directement sur un lien de promotion mais plutôt rechercher la boutique en ligne recherchée sur Google.

Des méthodes de paiement complexes doivent aussi éveiller l'attention : si le paiement doit obligatoirement être fait à l'avance, ceci peut remettre en question le sérieux du site. Des conditions générales de vente très mal traduites et une impossibilité d'impression doivent également alerter les consommateurs, et les inciter à ne pas acheter.

Concernant l'usage des sites de rencontres : les utilisateurs doivent limiter leurs visites à des sites reconnus, et toujours garder à l'esprit que les cyber-criminels les utilisent aussi. En conséquence, lors des communications avec d'autres utilisateurs, il est essentiel de s'assurer qu'ils possèdent un compte valide.

Les informations sensibles doivent rester secrètes : Il est également crucial d'éviter de partager des données personnelles et sensibles en ligne, telles que son adresse, des informations financières ou d'autres données d'identification personnelle. Ce sujet nécessite une attention particulière, car c'est précisément ce type d'informations qui vaut son pesant d'or pour les pirates – si un utilisateur sollicite explicitement ce genre de données, il s'agit d'un important signal d'alerte et toute communication doit être interrompue.

Savoir qui a accès à quoi : Dans le monde de l'entreprises si vous n'avez pas le contrôle ni la visibilité de savoir qui a accès à quoi au sein de votre système d'information …vous êtes en grand danger. Seule

Ecrit par Echo du Mardi le 13 février 2022

une solution de gestion de vos identités peut y remédier. »

« Cette année encore, la Saint Valentin promet d'être une occasion lucrative pour des cyber criminels qui exploiteront le désespoir des personnes seules, tout comme l'envie de faire plaisir des personnes en couple. Les menaces sont tout aussi importantes de part et d'autre. Toutefois, si les utilisateurs sont conscients des dangers et restent attentifs à certains points et signaux d'alerte qui révèlent de potentielles actions frauduleuses, ces attaques resteront vaines et les identités digitales seront saines et sauves. »