jeudi 18 février 2021

ALERTE SECURITE ENTREPRISES

Contact : *ggd80+secope@gendarmerie.interieur.gouv.fr*

L'hameçonnage (ou « phishing » en anglais)

Dans la Somme | Les campagnes d'hameçonnage sont nombreuses et leurs auteurs ne manquent pas d'imagination pour peaufiner les détails et faire illusion. Chaque jour, de multiples entreprises et administrations samariennes sont la cible de hackers.

Modus operandi | Technique utilisée par des fraudeurs pour **obtenir des renseignements personnels** dans le but de perpétrer une **usurpation d'identité**. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance (*banque*, *administration*, *site commercial*,...) afin de lui **soutirer des renseignements personnels** (*mot de passe*, *numéro de carte de crédit*, *numéro ou photocopie de la carte d'identité*, *date de naissance*, *etc*). Le plus souvent, un hyperlien fourni dans le message renvoie vers une **copie exacte d'un site internet**, réalisée dans l'optique de faire croire à la victime qu'elle se trouve sur le site internet officiel où elle pensait se connecter. La victime va ainsi **saisir ses codes personnels** qui seront récupérés par celui qui a créé le faux site. L'escroc aura ainsi accès aux données personnelles de la victime (*comptes*, *mots de passe*, *données bancaires*...) et pourra en faire un **usage frauduleux**. L'attaque, qui est le plus souvent réalisée par **courrier électronique**, peut également être dirigée par **téléphone**, **réseaux sociaux** ou **SMS**.

Mesures préventives

Ne vous fiez pas à l'adresse de messagerie source | Une adresse de messagerie provenant d'un ami, de votre entreprise, ou d'une administration **peut facilement être usurpée**. Seule une investigation poussée permet de confirmer ou non la source d'un courrier électronique. Si ce message semble provenir d'un ami (*par exemple pour récupérer l'accès à son compte*), **contactez-le sur un autre canal pour vous assurer qu'il s'agit bien de lui !**

Ne communiquez jamais d'informations sensibles par messagerie ou téléphone | Aucune administration ou société commerciale sérieuse ne vous demandera vos **données bancaires** ou vos **mots de passe** par message électronique ou par téléphone.

Positionnez le curseur de votre souris sur l'hyperlien (*sans cliquer*) | Cela affichera l'adresse vers laquelle il pointe réellement et vous permettra d'en **vérifier la vraisemblance**. Parfois, **un seul caractère peut changer dans l'adresse du site pour vous tromper**. Au moindre doute, ne fournissez aucune information, fermez la page correspondante et allez sur le site de l'organisme en question par un lien que vous aurez vous-même créé.

Utilisez des mots de passe différents et complexes pour chaque site et application | Afin d'éviter que **le vol d'un de vos mots de passe ne compromette tous vos comptes personnels**. Vous pouvez également utiliser des **coffres forts numériques** de type « *KeePass* » pour stocker de manière sécurisée vos différents mots de passe.

S'il s'agit de votre compte de messagerie professionnel | Transférez le message au **service informatique** et au **responsable de la sécurité des systèmes d'information** de votre entreprise pour vérification. Attendez leur réponse avant de supprimer le courrier électronique.

D'une manière générale | Restez **vigilant** quand vous recevez un mail qui vous **demande une action urgente.**

Que faire si vous êtes victime d'hameçonnage ?

Moyens de paiement | **Faites opposition** immédiatement si vous constatez des **débits frauduleux**.

Conservez les preuves | Et en particulier, le **message d'hameçonnage reçu**.

Changer rapidement vos mots de passe | **Changez-le immédiatement** sur le site ou service concerné, ainsi que sur tous les autres sites ou services sur lesquels vous utilisiez ce mot de passe **compromis**.

Déposez plainte | Auprès de votre brigade de gendarmerie ou commissariat territorialement compétent(e).