Gendarmerie de la Somme

Sécurité Economique et Protection des Entreprises

mardi 25 janvier 2022

ALERTE SECURITE ENTREPRISES

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

La gendarmerie nationale met en garde contre les arnaques au virement par mail

Nos enquêteurs ainsi que la section cybercriminalité du parquet de Paris appellent à la plus grande vigilance et déconseillent le **paiement de factures** qui seraient **adressées par mail** avant d'en avoir vérifié la **validité** auprès de l'émetteur.

S'agissant d'une escroquerie par **faux ordre de virement (*FOVI*)** commise après le piratage d'une adresse mail qui permettait de recueillir des informations détaillées, nos investigations ont abouti à la saisie de fichiers qui contenaient au final plus d'un millier d'adresses mail actives susceptibles d'avoir subi une escroquerie.

1ère tentative de fraude dans l'entreprise

Escroquerie au faux ordre de virements (*FOVI*) | C'est une technique qui consiste à contacter une entreprise et lui demander d'effectuer un **virement en urgence** d'une importante somme d'argent. Depuis plusieurs années, de nombreuses **entreprises** ont été **victimes** de cette arnaque. Véritable **fléau économique** apparu en 2010, ses chiffres ne cessent d'augmenter.

Comment s'en prémunir ?

Sensibiliser vos collaborateurs et cadres aux risques | En cas de réception de messages frauduleux d'**hameçonnage** (*phishing*) visant à leur dérober leurs **mots de passe** et en particulier si vos services de messagerie sont hébergés ou accessibles en externe ;

Communication mesurée | Les escrocs collectant en **amont** un maximum de **renseignements** sur l'entreprise victime à l'aide des réseaux sociaux, des vecteurs de communication de l'entreprise ou d'Internet, il y a lieu de ne pas diffuser d'**informations stratégiques** sur le site internet de l'entreprise et d'alerter votre personnel sur l'importance de ne pas divulguer des informations concernant l'entreprise sur les **réseaux sociaux** ;

Instaurer un protocole | concernant la **validation des virements bancaires** à plusieurs niveaux, connu uniquement des responsables (*banque*, *chef d'entreprise*, *comptable*). Créer des **mots d'authentification** pour réaliser ces virements et exclure les paiements de fin de semaine afin de pouvoir **réagir rapidement** auprès des banques en cas d'attaque avérée.

Comment réagir si vous êtes victime ?

Alerter votre banque | **identifier** immédiatement l'ensemble des **virements** exécutés, en instance ou à venir, à destination des coordonnées bancaires frauduleuses appartenant à l'escroc. **Alerter au plus vite** votre établissement bancaire de la transaction frauduleuse et **demander le retour des fonds**.

Préserver les traces | Conserver l'ensemble des **mails et numéros de téléphone** concernant les faits. Ces éléments seront très utiles aux enquêteurs.

Déposer plainte | Auprès de l'unité de **gendarmerie** ou de **police** territorialement compétente.