Gendarmerie de la Somme

Sécurité Economique et Protection des Entreprises

vendredi 16 juillet 2021

ALERTE SECURITE ENTREPRISES

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

Le mercredi 07 juillet 2021, une entreprise implantée dans le département de la Somme est la cible d'une escroquerie dite au **faux ordre de virement international** (FOVI).

A l'issue d'un premier contact téléphonique, l'escroc usurpe l'identité électronique d'un dirigeant puis adresse un courriel frauduleux au directeur financier concernant une opération confidentielle de rachat.

La vigilance du directeur financier permet d'annihiler la tentative.

L'escroquerie au faux ordre de virement internationale

But recherché | Escroquerie financière réalisée en usurpant l'identité d'un dirigeant, d'un fournisseur ou d'un employé visant à faire verser de l'argent sur un compte bancaire détenu par les cybercriminels.

Une attaque préparée en amont | Les escrocs collectent en amont un maximum de renseignements sur l'entreprise victime à l'aide des réseaux sociaux, des vecteurs de communication de l'entreprise, d'Internet, mais aussi en utilisant des virus informatiques (chevaux de Troie).

Mode opératoire | Cette escroquerie est réalisée grâce à des méthodes très élaborées qui reposent essentiellement sur la manipulation d'interlocuteurs (chef comptable, secrétaire direction, ...) susceptibles de déclencher des ordres de virements dans un cadre habituel ou à la suite de négociations imprévues. De plus, pour asseoir sa crédibilité et usurper une fonction, l'escroc apportera des détails précis sur l'entreprise et son PDG.

Mesures préventives

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 | Ne pas diffuser d'informations stratégiques sur le site internet de l'entreprise et alerter votre personnel sur l'importance de ne pas divulguer sur les réseaux sociaux des informations concernant l'entreprise ;

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.

Que faire 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 demandez le retour des fonds.

Préserver les traces | Conservez 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.