mercredi 29 septembre 2021

ALERTE SECURITE ENTREPRISES

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

Depuis le début de l'année, la section *Sécurité Économique et Protection des Entreprises* du groupement de gendarmerie départementale de la Somme observe une recrudescence de **mails frauduleux usurpant l'appellation de la Gendarmerie, de la Police, d'Europol ou d'Interpol** et reprochant une prétendue infraction.

Il s'agit d'une escroquerie ancienne et connue des cyber gendarmes. Ces derniers temps, ceux-ci observent un retour en force de ces campagnes de mails frauduleux, où la victime reçoit un mail usurpant l'appellation d'un service judiciaire, et lui reprochant une infraction. Le message provient d'un prétendu commissaire divisionnaire, chef de la Brigade de protection des mineurs. Ce message indique, qu'après enquête de la « *Cyber-infiltration* », l'internaute s'est rendu coupable de différentes infractions sur des mineurs : **pédopornographie, pédophilie, exhibitionnisme, cyber pornographie, trafic sexuel**.

L'objectif des escrocs est de **dérober de l'argent** en utilisant différents ressorts.

Faut-il avoir peur de ces messages ?

La réponse est simple : NON | Car il s'agit d'une simple arnaque qui vise à escroquer des victimes crédules en leur faisant peur avec de **fausses accusations**.

Un message anxiogène | Sur fond de faits reprochés d'une **grande gravité** (pédopornographie, pédophilie…).

Se réclamant de diverses forces de l'ordre | Les **forces de sécurité intérieure** ne vous contactent jamais directement par e-mail, ne vous demandent pas d'argent et ne vous invitent jamais à transmettre vos informations (identités, données bancaires) ou à effectuer un quelconque virement.

Une usurpation détectable | Nous vous rappelons qu'un mail se prévalant d'un service de la gendarmerie et ne se terminant pas par « ***gendarmerie.interieur.gouv.fr*** » est forcément un mail frauduleux.

Que faire si vous recevez ce type de message ?

Ne paniquez pas | En effet, vous n'avez sans doute rien de réellement compromettant à vous reprocher. Par ailleurs, la consultation de sites pornographiques, dans le respect de la loi, n'est pas répréhensible.

Ne cliquez sur aucun lien | Si vous êtes invité à cliquer dans ces e-mails, déplacez-les dans les spams ou supprimez ces e-mails sans en tenir compte.

Ne répondez pas | Cela montrerait aux cybercriminels que votre adresse de messagerie est « *valide* » et que vous portez de l'intérêt au message d'escroquerie qu'ils vous ont envoyé.

Signalez la tentative d'escroquerie | Ces e-mails ont pour but de voler vos identités, vos données bancaires ou vous soutirer de l'argent. Vous pouvez signaler ces e-mails frauduleux à l'adresse suivante : *https://www.signal-spam.fr/*.

Et si vous avez donné suite à l'arnaque et avez payé ?

Rassemblez les preuves | Conservez le message reçu, les échanges avec l'escroc ainsi que toute autre information que vous avez pu collecter et qui pourra vous servir pour déposer plainte auprès des autorités.

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

Contactez votre banque | Pour essayer de vous faire rembourser. Certaines banques exigeront la preuve du dépôt de plainte pour instruire votre demande.