SÉCURITÉ ÉCONOMIQUE & PROTECTION DES ENTREPRISES

La Gendarmerie nationale, acteur de la politique publique d'intelligence économique

ALERTE SECURITE SECOPE 80 **entreprises**

CAMPAGNE DE FRAUDE SOUS CACHET DGFIP CONCERNANT UNE ENQUÊTE SEPA

Ce vendredi 04 septembre 2020, une entreprise samarienne a reçu un courriel frauduleux sous l'objet « **IMPORTANT : enquête SEPA** » avec un courrier en pièce jointe reprenant la signalétique, toutes les composantes d'un courrier DGFIP ainsi que l'identité réelle d'agents DGFIP.

Le seul indice de fraude du courrier réside dans l'adresse mail indiquée pour le renvoi des documents : en effet l'adresse spécifiée est « ODAC@dgfip-finances-gouv.**cloud** » alors que la fin d'une adresse DGFIP est toujours en « @dgfip.finances.gouv.**fr** ».

Cette campagne de fraude, basée sur la technique de **l'hameçonnage** (*technique consistant à récupérer des données personnelles sur internet*), vise à s'approprier frauduleusement les références bancaires et clients d'une entreprise afin d'organiser le détournement de virements bancaires auprès de ses clients, voir le détournement des coordonnées bancaires propres de l'entreprise ciblée.

NOS CONSEILS POUR PROTÉGER VOTRE ENTREPRISE

- **N'accordez jamais une confiance aveugle dans le nom de l'expéditeur d'un courriel** : l'usurpation d'adresse mail est une pratique très répandue qui permet au hacker de se faire passer pour une marque connue ou une connaissance. Cela n'est pas beaucoup plus compliqué que de mettre un faux nom d'expéditeur au verso d'une enveloppe ;
- **Ne répondez jamais à une demande d'informations confidentielles** : les demandes d'informations confidentielles (*mots de passe, code PIN, coordonnées bancaires, ...*), lorsqu'elles sont légitimes, ne sont jamais faites par courriel. En cas de doute, demandez à votre correspondant légitime de confirmer sa demande ;
- **Méfiez-vous des pièces jointes** : Elles peuvent contenir des virus ou des logiciels espion. Assurez-vous régulièrement que votre antivirus est activé et à jour. Si votre poste a un comportement anormal (*lenteur, écran blanc sporadique, ...*), faites-le contrôler ;
- **Passez votre souris au dessus des hyperliens** : en passant le curseur de souris au-dessus d'un lien proposé, vous pouvez repérer s'il pointe bien vers l'adresse du site annoncé dans le message. Si l'adresse est différente, soyez extrêmement méfiant, et évitez de cliquer dessus. De manière générale, il est préférable de saisir manuellement l'adresse dans le navigateur ;
- **Faites attention à la qualité du français ou de la langue pratiquée par votre interlocuteur** : dans la plupart des tentatives d'hameçonnage, notamment lorsqu'elles viennent de l'étranger et que le texte a été traduit par un logiciel, l'orthographe et la tournure des phrases sont d'un niveau très moyen, et les caractères accentués peuvent être mal retranscrits. Toutefois, on constate qu'un nombre croissant de ces tentatives emploie désormais un français très correct. Soyez donc le plus vigilant possible lors de la réception de courriels ;
- **Paramétrez correctement votre logiciel de messagerie** : un guide de paramétrage est disponible sur le site du CERT-FR (*Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques*), à cette adresse : *https://www.cert.ssi.gouv.fr/information/CERTA-2000-INF-002/*.

Sécurité Économique et Protection des Entreprises
Groupement de Gendarmerie Départementale de la Somme.

Nous contacter ggd80+secope@gendarmerie.interieur.gouv.fr

Gendarmerie de la Somme