GROUPEMENT COMMERCIAL
DU BAS-RHIN

Mars 2019

Données personnelles : "Mise en conformité RGPD", l'arnaque qui cible les petites entreprises

Des entreprises, en particulier des TPE, commerçants, artisans, reçoivent actuellement des courriers, emails ou des appels téléphoniques pour une « mise en conformité » avec le règlement européen sur la protection des données personnelles (RGPG).
Ces groupes très organisés se servent de l'entrée en application du RGPD pour soutirer de l'argent aux commerçants, artisans...

A la CNIL (Commission Informatique et Libertés) arrivent chaque jour plusieurs dizaines d'appels de personnes ciblées par ces escrocs qui se font passer pour l'Etat.
La CNIL et la DGCCRF mettent en garde les sociétés face à ces tentatives d'escroqueries et plusieurs recommandations sont à suivre pour se prémunir contre ces escroqueries :

- demander des informations sur l'identité de l'entreprise démarcheuse permettant de faire des vérifications sur internet ou auprès des syndicats de votre profession ;
- vous méfier de telles communications prenant les formes d'une information officielle émanant d'un service public ;
- lire attentivement les dispositions contractuelles ou pré-contractuelles ;
- prendre le temps de la réflexion et de l'analyse de l'offre ;
- diffuser ces conseils de vigilance auprès de vos services et des personnels qui sont appelés à traiter ce type de courrier dans l'entreprise ;
- **ne payer aucune somme d'argent au motif qu'elle stopperait une éventuelle action contentieuse.**

Si vous vous estimez lésé, vous pouvez vous adresser à la direction départementale de la protection des populations (DDPP) de votre département de résidence.

BAS-RHIN - **DDPP :** Cité administrative Gaujot - 14 rue du maréchal Juin - CS50016 - 67084 Strasbourg cedex
Courriel : ddpp@bas-rhin.gouv.fr Tél. : 03 88 88 86 00 fax : 03 88 88 86 01

Pour rappel, les entreprises de moins de 5 salariés sont protégées par les dispositions du code de la consommation pour les contrats conclus hors établissement.

Source CNIL

Comment se prémunir contre le phishing ?

source Bercy Infos

Cybersécurité

Usagers du web, vos données sont précieuses et les pirates le savent. C'est pourquoi ils redoublent d'imagination pour tenter de vous les soutirer. L'un de ces moyens est le phishing. Qu'est-ce que c'est et comment s'en prémunir ? Comment signaler facilement une tentative d'hameçonnage ?

© *Fotolia*

Qu'est-ce que le phishing ou hameçonnage ou filoutage ?

Selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI) : « le phishing ou hameçonnage vise à obtenir du destinataire d'un courriel d'apparence légitime qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion à des services financiers, afin de lui dérober de l'argent ».

Il s'agit de l'un des principaux vecteurs de la cybercriminalité. Ce type de pratique peut être également utilisé dans des attaques plus ciblées pour essayer d'obtenir d'un employé ses identifiants d'accès aux réseaux professionnels auxquels il a accès.
Pour renforcer sa crédibilité, le courriel frauduleux n'hésitera pas à utiliser logos et chartes graphiques des administrations ou entreprises les plus connues. Le contenu du message repose en général sur deux stratégies :

- soit il vous est reproché de ne toujours pas avoir réglé une certaine somme d'argent (factures, impôts, électricité...) et on vous enjoint à le faire sous peine de pénalités de retard voire de saisine de la justice ;
- soit on vous signale une erreur d'ordre financier en votre faveur (impôts, banque...) et on vous invite à suivre des indications pour vous faire rembourser.

D'autres méthodes existent (fax en attente, cadeaux...). Restez vigilant !

Comment vous protéger contre le phishing ?

- Si un courriel vous semble douteux, ne cliquez pas sur les pièces jointes ou sur les liens qu'il contient ! Connectez-vous en saisissant l'adresse officielle dans la barre d'adresses de votre navigateur.
- Si vous réglez un achat en ligne et que vous devez donc fournir des informations relatives à votre carte bancaire, vérifiez que vous le faites sur un site web sécurisé dont l'adresse commence par « https ».
- Ne communiquez jamais d'informations confidentielles par mail. Aucun site web fiable ne vous le redemandera !
- Vérifiez que votre antivirus est à jour pour maximiser sa protection contre les programmes malveillants.
- Utilisez le filtre contre le filoutage du navigateur internet : la plupart des navigateurs existants proposent une fonctionnalité d'avertissement contre le filoutage. Leurs principes peuvent être différents (liste noire, liste blanche, mot clé, etc.) ces fonctions aident à maintenir votre vigilance.
- Utilisez un logiciel de filtre anti-pourriel ou les fonctionnalités de classement automatique en tant que spam de votre boite de réception : même si ces filtrages ne sont pas exhaustifs, ils permettent de réduire le nombre de ces courriels.

Signalez l'abus d'utilisation d'informations personnelles aux autorités compétentes

- Si vous pensez avoir été victime d'une escroquerie ou d'une tentative d'escroquerie par phishing signalez-le sur https://www.signal-spam.fr/

Signal Spam résulte d'un partenariat public-privé. Il donne la possibilité aux internautes de signaler tout ce qu'ils considèrent être un spam dans leur messagerie afin de l'assigner ensuite à l'autorité publique ou au professionnel qui saura agir pour lutter contre le spam signalé.