Cybercrime

L'arnaque au président ou escroquerie aux faux ordres de virement (FOVI)

21 janvier 2016

Les entreprises ne sont pas à l'abri des escroqueries. Depuis 2010, les escroqueries "la fraude au président" ou "au changement de RIB" ont fait de nombreuses victimes parmi les entreprises françaises. Pour s'en prémunir, retrouvez quelques conseils de prévention.

Depuis l'apparition de ce nouveau type d'escroquerie en 2010, plusieurs centaines de faits ou de tentatives ont été recensées pour un **préjudice global de 485 millions d'euros**. L'Office central de répression de la grande délinquance financière (OCRGDF), appelle les sociétés à la vigilance :

C'est un véritable fléau économique. Il faut être vigilant, la trêve des confiseurs est souvent synonyme de relâchement dans les sociétés et les escrocs en profitent.

En 5 ans **2.300 plaintes ont été déposées**, même si beaucoup d'entreprises n'osent pas par peur de mauvaise publicité.

FOVI?
Réalisée par téléphone ou par mail, l'escroquerie aux Faux Ordres de VIrement (FOVI) concerne les entreprises de toute taille et de tous les secteurs.
La "**Fraude au président**" consiste pour des escrocs à convaincre le collaborateur d'une entreprise d'effectuer en urgence un virement important à un tiers pour obéir à un prétendu ordre du dirigeant, sous prétexte d'une dette à régler, de provision de contrat ou autre.
Le "**Changement de RIB**" consiste pour les fraudeurs à envoyer un mail à un salarié du service de comptabilité ou trésorerie de l'entreprise en se faisant passer pour un fournisseur, et lui demander de diriger ses versements vers un autre compte bancaire appartenant aux escrocs.
Souvent situés à l'étranger, les escrocs collectent en amont un maximum de renseignements sur l'entreprise. Cette connaissance de l'entreprise associée à un ton persuasif et convaincant est la clé de réussite de l'arnaque. L'opération est alors lancée sur les personnes capables d'opérer les virements (services comptables, trésorerie, secrétariat...).

Quelques règles simples

Pour s'en prémunir, les entreprises peuvent mettre en place un ensemble de mesures simples de sécurité pour décourager les escrocs.

- **Rappeler à l'ensemble des collaborateurs** la nécessité d'avoir un usage prudent des réseaux sociaux privés et professionnels. Les alerter sur l'importance de ne pas y divulguer d'informations concernant le fonctionnement de l'entreprise.
- Sensibiliser **régulièrement l'ensemble des employés des services comptables, trésorerie, secrétariats, standards**, de ce type d'escroquerie. Prendre l'habitude d'en informer systématiquement les **remplaçants** sur ces postes.
- **Instaurer des procédures de vérifications** et de signatures multiples pour les paiements internationaux.
- Rompre la chaîne des mails pour les courriers se rapportant à des virements internationaux en **saisissant soi-même l'adresse habituelle du donneur d'ordre**.
- Maintenir à jour le système de sécurité informatique.
- Accentuer la vigilance sur les **périodes de congés scolaires**, les **jours fériés** et les **jours de paiement des loyers**.

Reconnaître les signes d'une attaque

- Une **demande de virement à l'international, non planifiée**, au caractère **urgent** et **confidentiel** : dans ce cas, contacter son interlocuteur habituel avec les coordonnées connues de la société.
- **Se méfier de tout changement de coordonnées téléphoniques ou mails**. Attention, la communication d'un nouveau numéro à l'indicatif français n'est pas une garantie.
- **Se méfier d'un contact direct d'un escroc se faisant passer pour un membre de la société ou un responsable qui va faire usage de flatterie ou de menace dans le but de manipuler son interlocuteur.**
- Pour asseoir sa crédibilité et usurper une fonction, l'escroc apportera une abondance de détails sur l'entreprise et son environnement : données personnelles concernant le chef d'entreprise, ses collaborateurs...

En cas de doute, prendre attache directement avec la personne au sein de la société, soit physiquement soit avec les coordonnées connues de l'entreprise.

Que faire en cas d'attaque ?

- Demander immédiatement à la banque le retour des fonds
- **Déposer une plainte** auprès des services de police et de gendarmerie, en apportant un maximum d'éléments.

Un dépôt de plainte rapide permet d'optimiser les chances de récupérer les fonds escroqués.