Fiche n°1

Précisions relatives aux tentatives d'escroquerie et renforcement de la vigilance de l'ordonnateur et du comptable

Des cas d'escroqueries ont déjà été rencontrés par des ordonnateurs et des comptables publics. Certaines fraudes ont été déjouées grâce à la vigilance des agents, mais d'autres n'ont pu être évitées. Il peut être considéré, à tort, que cela n'arrive qu'aux autres. Dans ce contexte, les actions de préventions régulières sont déterminantes.

I – Présentation générale de la fraude au président ou escroquerie aux faux ordres de virement (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 **ainsi que l'État, les établissements publics nationaux, les collectivités et établissements publics locaux ou les établissements publics de santé :**

Deux grands types d'escroquerie :

1) La "Fraude au président" consiste pour des escrocs à convaincre l'agent d'effectuer en urgence un virement important à un tiers pour obéir à un prétendu ordre de la hiérarchie, sous prétexte d'une facture à régler, de provision de contrat ou autres. L'escroc peut également se faire passer pour l'éditeur de logiciel de comptabilité, un responsable informatique souhaitant réaliser des tests à distance et réaliser des opérations frauduleuses sur le poste de l'agent.

2) Le "Changement de RIB", via usurpation d'identité, consiste pour les fraudeurs à envoyer un mail ou à téléphoner à un agent des services de l'ordonnateur ou du comptable en se faisant passer pour un fournisseur ou une société d'affacturage, et lui demander de diriger ses versements vers un autre compte bancaire appartenant aux escrocs.

Les escrocs collectent en amont un maximum de renseignements sur le fournisseur et l'administration et utilisent souvent des comptes bancaires domiciliés à l'étranger.

Cette connaissance des structures (nom des agents et salariés, leur fonction au sein de l'administration et de ses fournisseurs,…) et du contexte (exemple : existence d'un marché public de tel service de l'État avec tel fournisseur) associée à un ton persuasif et convaincant est la clé de réussite de l'escroquerie. L'opération est alors lancée sur les personnes ayant un rôle sur la chaîne de paiement et de virement (services de l'ordonnateur – service prescripteur, CSP, direction des finances mais également secrétariat, etc. - et du comptable public).

II - Reconnaître les signes d'une attaque : faits devant accroître la vigilance des agents :

1/ Un contact inhabituel dans la forme :

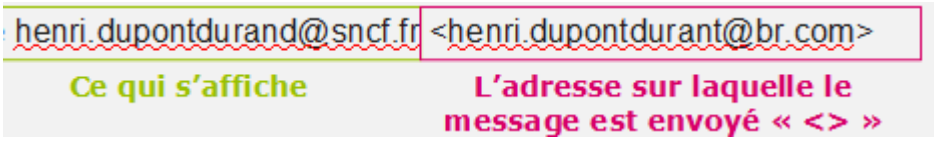
- L'agent est contacté par un correspondant inhabituel ;
- Pour asseoir sa crédibilité et usurper une fonction, l'escroc apportera une abondance de détails sur l'entreprise/l'administration et son environnement : données personnelles concernant l'ordonnateur, ses collaborateurs, le fournisseur et ses dirigeants… ;
- Contact direct d'un escroc (par courriel, par téléphone,…) se faisant passer pour un membre de la société ou un responsable qui va faire usage de flatteries ou de menaces dans le but de manipuler son interlocuteur.

2/ Une demande inhabituelle dans son contenu :

- Demande de virement à l'international (par courriel, par téléphone,…), non planifiée, au caractère urgent et confidentiel ;

- Demande de versement à un fournisseur national sur un compte bancaire domicilié à l'étranger ;
- Tout changement de coordonnées téléphoniques, électroniques et de coordonnées bancaires que ce soit du fournisseur, du factor ou du cessionnaire. Affiliation récente du fournisseur à une société d'affacturage. Attention, la communication d'un nouveau numéro à l'indicatif français ou de coordonnées bancaires domiciliées en France n'est pas une garantie ;
- La demande écrite ou orale de l'escroc comporte plusieurs incohérences, fautes d'orthographes et de syntaxe. Il peut s'agir d'incohérences de noms, de prénoms, d'une adresse de messagerie à la forme particulière (exemples : adresses décomposées en plusieurs parties entre "<>", l'adresse électronique du correspondant est composée de plusieurs sous adresses électroniques, adresse du destinataire affichée différente lorsque l'on répond au courriel…) ou approchant l'adresse de messagerie habituelle (exemple : pascal.durand@intérieur-gouv-fr au lieu de pascal.durand@intérieur.gouv.fr).

Exemple : lors d'une réponse à un courriel d'un escroc cherchant à se faire passer pour un employé de la sncf :



La demande peut être trompeuse du fait de sa "qualité" avec utilisation du logo du fournisseur ou affichage d'un faux numéro sur le poste téléphonique de l'agent ;

- La demande écrite ou orale de l'escroc, les nouvelles coordonnées bancaires, présentent des incohérences avec les pièces justificatives de la dépense (facture, acte d'engagement, acte de cession). Les écarts peuvent porter notamment sur les adresses du fournisseur (ou du factor, du cessionnaire), les références SIRET, la dénomination de l'entreprise.

III – Comment déjouer la fraude

- Ne pas céder à la pression de l'interlocuteur souhaitant un paiement rapide ;
- En référer, au moindre doute, immédiatement à sa hiérarchie ;
- Porter un regard critique sur les demandes urgentes ou la transmission de nouvelles coordonnées à tous les niveaux de la chaîne de la dépense (des services prescripteurs au comptable) ;
- Contacter son interlocuteur habituel avec les coordonnées déjà connues de la société (= procédure de contre-appel) en cas de moindre doute sur des nouvelles coordonnées téléphoniques, électroniques ou bancaires. Ne pas contacter le fournisseur à partir des coordonnées téléphoniques, électroniques fournies par le potentiel escroc ;
- Rompre la chaîne pour les courriers/courriels douteux en saisissant soi-même l'adresse (physique, électronique) habituelle du donneur d'ordre, voire en le contactant directement à son numéro de téléphone usuel.

IV - Quelques règles simples de vigilance pour se prémunir de l'escroquerie :

- Ne pas divulguer à l'extérieur (dont réseaux sociaux) et à un contact inconnu d'informations concernant le fonctionnement de l'administration et de ses fournisseurs : organigrammes, adresses électroniques et documents ou images comportant la signature des acteurs-clés, des procédures internes… Dans le cadre professionnel, divulguer ces informations avec prudence en les restreignant au strict nécessaire ;
- Avoir un usage prudent des réseaux sociaux privés et professionnels ;
- Informer/Sensibiliser régulièrement l'ensemble des agents des services financiers, comptabilités, trésoreries, secrétariats, standards, de ce type d'escroquerie. Prendre l'habitude d'en informer systématiquement les remplaçants sur ces postes ;
- Instaurer des procédures de vérifications pour les paiements internationaux ;

- Accentuer la vigilance sur les périodes de congés et de forte charge de travail ;
- Diffuser à l'ensemble de la chaîne de traitement des dépenses (service prescripteur, CSP, services financiers, comptable…) les alertes et communications transmises par les fournisseurs indiquant faire l'objet d'escroquerie.

V – Réagir vite en cas de réalisation de l'escroquerie

- L'ordonnateur doit immédiatement en informer le comptable. D'une manière générale en cas de fraude suspecte ou avérée, les ordonnateurs et le comptable public doivent échanger leurs informations sans tarder ;
- Identifier l'ensemble des paiements déjà réalisés, à venir, ou en instance pour effectuer les rejets et blocages nécessaires. Identifier immédiatement les virements exécutés, les mandats de paiement ou les demandes de paiement en instance ou à venir utilisant les coordonnées bancaires frauduleuses (travaux nécessitant le cas échéant une collaboration entre l'ordonnateur et le comptable).
- Demander immédiatement le blocage des coordonnées bancaires frauduleuses dans les applications métiers.
- Si le paiement n'est pas encore intervenu, le comptable doit immédiatement suspendre le mandat de paiement/la demande de paiement concerné et/ou bloquer la mise en paiement pour analyser la situation ;
- Renforcer les actions de sensibilisation de l'ensemble des acteurs de la chaîne afin d'éviter que le cas ne se reproduise.