eca
Experts & Consultants Associés

Lettre d'information

Août 2015

LA FRAUDE AU VIREMENT

Les fraudes par usurpation d'identité ont causé plus de 300 millions d'euros de préjudice en France. Avez-vous pris toutes les mesures pour protéger votre entreprise ?

LA FRAUDE AU VIREMENT EVOLUE

ALERTES

Protégez vos fichiers clients et fournisseurs : les commerçants et entreprises en général doivent sécuriser leurs fichiers clients et fournisseurs contre le vol de données, pour éviter en particulier la fraude monétique et la fraude au virement.

Attention aux changements de RIB : certains fraudeurs se faisant passer pour un fournisseur ou un bailleur, demandent à leur victime de modifier un compte bénéficiaire. Auditez vos procédures d'ajout et de modification de comptes tiers, en particulier en cas de compte domicilié à l'étranger.

Les faux ordres de virement classiques, supportant la signature usurpée du dirigeant, sont en déclin. Par ailleurs, les canaux électroniques bancaires sont de plus en plus sûrs.

Désormais, les escrocs agissent par **usurpation d'identité**. Ils s'attaquent au « maillon faible » : la personne responsable de réaliser les paiements dans l'entreprise. Ils amènent leur victime à envoyer de bonne foi un virement vers un **compte frauduleux à l'étranger**.

LES SCENARIOS DE FRAUDE LES PLUS COURAMMENT UTILISES PAR LES ESCROCS :

- **La fraude au Président** : Un faux dirigeant exige de sa victime qu'elle envoie un virement confidentiel et urgent.
- **Le technicien bancaire** : Un faux technicien bancaire « aide » sa victime à faire un virement de test.
- **Le faux fournisseur** : Un faux fournisseur demande à sa victime de modifier ses coordonnées bancaires.
- **La fraude au loyer** : Un faux bailleur demande à sa victime de modifier ses coordonnées bancaires.

L'ESCROQUERIE EST PRECEDEE D'UNE PHASE « D'INGENIERIE SOCIALE »

Pour mieux piéger leurs victimes, les fraudeurs collectent des informations sur l'entreprise sur les réseaux sociaux, par téléphone ou par piratage informatique : statuts, organigrammes, signatures, comptes bancaires …

TOUTES LES ENTREPRISES SONT CIBLEES

Toutes les entreprises sont ciblées : grands groupes, filiales en France ou à l'étranger, PME.

ATTENTION : CES FRAUDES SONT TRES DIFFICILES A DETECTER !

Les fraudeurs sont doués d'empathie et d'autorité naturelle. Ils imitent les voix, utilisent des outils de prise en main à distance d'ordinateur, le piratage d'email, le détournement de ligne téléphonique, etc.

SE PROTEGER

AVEZ-VOUS SENSIBILISE VOS EQUIPES AUX RISQUES DE FRAUDE ?

- **Sensibilisez régulièrement** aux risques de fraude les personnes pouvant préparer ou valider des paiements ou ajouter des comptes de tiers, etc.
- **Limitez la diffusion d'informations** par téléphone, par email et sur les réseaux sociaux, et sensibilisez les assistantes.

UNE PERSONNE SEULE PEUT-ELLE EXECUTER UN VIREMENT DANS VOTRE ENTREPRISE ?

Si oui, vous êtes en risque, surtout sur les **virements transfrontaliers**.
Protégez-vous grâce à la **double validation** des virements et/ ou des **listes fermées de comptes et/ou de pays**.

AVEZ-VOUS SECURISE L'AJOUT ET LA MODIFICATION DE COMPTES BENEFICIAIRES DANS VOS OUTILS ?

Sinon, assurez-vous d'avoir mis en place une procédure de **vérification d'identité du demandeur**, en particulier pour les comptes domiciliés à l'étranger.

FAITES-VOUS DE FREQUENTS RAPPROCHEMENTS DE VOS COMPTES ?

Ceci peut permettre de **détecter une fraude** et stopper les nouvelles tentatives des fraudeurs (qui récidivent tant qu'ils n'ont pas été démasqués).

ENVOYEZ-VOUS DES ORDRES OU DES VALIDATIONS PAPIER A VOTRE BANQUE ?

Ce canal est plus vulnérable aux fraudes. Supprimez autant que possible les ordres et les validations papier.

QUE FAIRE EN CAS DE FRAUDE ?

AU MOINDRE DOUTE

- **Vérifiez l'identité de votre interlocuteur** en contactant le cas échéant : votre hiérarchie, votre banque, votre fournisseur, votre bailleur, etc.
- **Utilisez les coordonnées sûres** en votre possession (adresse email, numéro de téléphone …), et pas celles que votre interlocuteur vous a communiquées.
- N'hésitez pas à contacter votre interlocuteur par **deux canaux différents** (par exemple en cas de modification d'un compte de fournisseur).

SI VOUS AVEZ DETECTE UNE FRAUDE EN COURS

- **Alertez immédiatement.**
- **Jouez le jeu et simulez** afin d'obtenir un maximum de renseignements (compte bancaire, pays et nom du bénéficiaire, etc.).
- Si votre interlocuteur vous demande de **vous connecter via internet à un système ou d'activer un lien**, ne le faites surtout pas.
- **Ne communiquez aucun code ou identifiant.**
- **Prévenez votre banque** qui vous aidera à porter plainte.

SI VOUS AVEZ ETE VICTIME D'UNE FRAUDE

- La rapidité est essentielle : **contactez votre banque le plus vite possible** afin de tenter de bloquer le virement ou de rappeler les fonds.
- **Alertez votre hiérarchie et déposez plainte auprès de la police**.