RÉGION DE GENDARMERIE AUVERGNE – RHÔNE-ALPES

Bulletin d'information Entreprises

NOTRE ENGAGEMENT, VOTRE SÉCURITÉ

Semaines 17 & 18 - Avril 2020 – N° 3

ESCROQUERIES FINANCIÈRES
Bien réagir pour s'en prémunir

Apparues en 2005, les escroqueries aux faux ordres de virement ont touché plusieurs milliers d'entreprises pour un montant total supérieur à 700 millions d'euros.

Depuis le début de la crise du coronavirus, plus d'une soixantaine d'escroqueries liées à l'achat de matériels médicaux ou de protection ont été recensées en France, pour un préjudice estimé à plus de 11 millions d'euros.

De très nombreuses autres tentatives ont heureusement échoué. Si elles avaient réussi, elles auraient rapporté 40 millions d'euros supplémentaires à leurs auteurs *(1)*.

Faux ordre de virement : les 4 principales étapes

1 - Ingénierie sociale
Collecte d'informations pour connaître l'entreprise, ses dirigeants et salariés

2 - Contact
Demande par téléphone ou mail. Usurpation d'identité ou de fonction (*PDG, avocat, ...*).

3 - Relances incessantes
Mise sous pression du comptable « *urgence, confidentialité, situation sensible* ». Collaborateur invité à passer outre les procédures.

4 - Transfert d'argent
Argent viré sur un compte à l'étranger. Difficultés pour annuler l'opération.

CAS CONCRET : Un individu se présentant comme dirigeant d'une société de vente de produits médicaux contacte une PME pour lui proposer d'importantes quantités de matériels de protection contre le COVID-19 à des prix défiants toute concurrence.
Suite aux vérifications d'usage réalisées par le biais d'internet, le PDG constate que si la société existe bien, le nom du dirigeant lui, ne correspond pas. L'entreprise ne donne pas suite malgré de nombreuses relances.

MESURES DE PRÉVENTION / PROTECTION

- **Vérifier l'existence et l'application de procédures internes concernant virements et achats.**
- **Sensibiliser régulièrement les équipes financières et comptables ainsi que tout salarié exerçant une fonction «filtre»** (*secrétaire, assistante de direction, standardiste,...*).
- **Former les salariés au bon usage des moyens informatiques, aux dangers des réseaux sociaux ainsi qu'à la protection de l'information. Les responsabiliser par la mise en place de chartes.**
- **Ne pas rendre public l'organigramme de l'entreprise pour ne pas faciliter la collecte d'informations de l'escroc.**
- **Lorsqu'une demande de virement est faite hors du formalisme habituel, exiger une sollicitation écrite provenant d'une adresse mail professionnelle, ainsi qu'un numéro de téléphone fixe (et non portable) qui seront systématiquement vérifiés.**
- **Orienter l'interlocuteur vers la procédure régulière, et ne rien entreprendre sans l'aval de la hiérarchie.**
- **Ne communiquer aucun code confidentiel par téléphone, fax ou courriel.**

En cas de problème avéré ou de simple tentative : alerter immédiatement la banque pour bloquer les fonds.
Déposer rapidement plainte auprès du service de gendarmerie ou de police territorialement compétent.

Sécurité économique territoriale auvergne - rhône-alpes

Bureau renseignement – ***cellule sécurité économique***
36 boulevard de l'Ouest 69580 SATHONAY-CAMP - Tél. : 04.37.85.21.15
securite-economique-auvergnerhonealpes@gendarmerie.interieur.gouv.fr

(1) ***Source*** : la montagne du 28/04/2020

Bulletin d'information Entreprises N° 3

COURRIELS D'IMPOSTEURS (BEC)/ARNAQUES AU PRÉSIDENT (CEO)

La fraude CEO/BEC consiste à piéger un collaborateur habilité à effectuer les paiements de l'entreprise, le but étant qu'il paie une fausse facture/réalise un transfert non autorisé.

COMMENT CELA SE PASSE-T-IL ?

Par téléphone ou courriel, un fraudeur se fait passer pour un dirigeant de la société (par ex. CEO ou CFO).

Ils connaissent bien l'organisation.

Ils réclament un paiement urgent.

Leurs expressions courantes : "confidentialité", "la société vous fait confiance", "pour l'instant indisponible".

Sont souvent demandés des paiements internationaux vers des banques en dehors de l'Europe.

L'employé transfère les fonds vers un compte géré par le fraudeur.

Les instructions visant la procédure pourront être données plus tard, par courriel/un tiers.

Le collaborateur est invité à ne pas respecter les procédures d'autorisation prévues.

Ils font référence à une situation sensible (par ex. contrôle fiscal, fusion, acquisition).

Sites de référence

https://www.ssi.gouv.fr/
https://www.cybermalveillance.gouv.fr
https://www.ene.fr/
https://ma-solution-numerique.fr/

Formation à la cybersécurité

https://secnumacademie.gouv.fr/

Source : Europol