

Alerte

ESCROQUERIE AU R.I.B

Une société asiatique se faisant passer pour un fournisseur contacte une entreprise et l'informe par courriel de son changement de domiciliation bancaire. Une facture et un relevé d'identité bancaire mentionnant les nouvelles coordonnées y sont joints.

Confiant l'entreprise victime effectue immédiatement 2 virements pour un montant supérieur à 20000€. Les dirigeants ne s'aperçoivent de l'escroquerie que quelques temps après. Lors des vérifications, ils constatent que l'adresse mail utilisée diffère légèrement de celle habituellement employée par le fournisseur.

DE QUOI PARLE T-ON ?

L'escroquerie au « faux RIB » ou plus exactement au « changement de domiciliation bancaire » connaît un certain essor.

Variante de l'escroquerie dite « au faux président », cette arnaque est la plus simple à réaliser.

Elle ne nécessite aucune connaissance en informatique et peu de recherches d'informations par le biais de l'ingénierie sociale.

Pour y parvenir, la création de fausses adresses mail, de fausses factures à entête de fournisseurs bien réels et l'adjonction d'un RIB suffisent.

Relevé d'Identité Bancaire

Code Banque	Code Guichet	Numéro de compte	Clé RIB	Domiciliation
12345	12345	1234567891A	12	Banque-ville-agence

IBAN FR00 1234 5123 4512 3456 7891 A12

BIC ABCDEFGH

Titulaire Monsieur ou Madame Jean NEAJE

SPECIMEN

QUE FAIRE ?

En amont :

- Mettre en œuvre des procédures écrites strictes concernant les virements.
- Contrôler et limiter la diffusion d'informations concernant l'entreprise. A ce titre, éviter la mise en ligne de l'organigramme de la société pour ne pas faciliter le travail des escrocs. De même, ne communiquer aucune information sensible (factures, baux, etc.) par téléphone, fax ou mail sans avoir formellement identifié le demandeur.
- Sensibiliser régulièrement les salariés et ce quel que soit le niveau de responsabilité exercé. De même, les responsabiliser en adoptant une charte d'utilisation des moyens informatiques, d'internet et des réseaux sociaux.

Lors de la réception de courriels :

- Ne jamais se contenter des seules informations affichées. Ne pas répondre à un mail en utilisant la fonction «répondre» de la messagerie. La victime risquerait alors de ne pas s'apercevoir qu'elle a affaire à une fausse adresse.
- Contacter immédiatement et systématiquement par téléphone le fournisseur en utilisant de préférence un téléphone portable, le serveur téléphonique ayant peut être été piraté par l'escroc en vue de rediriger les contre-appels de sécurité.
- La mise en place d'une veille régulière permettra d'anticiper et de s'adapter aux nouvelles menaces.