

Fraude au virement et arnaque au président

Un email pressant, un RIB modifié, et des dizaines de milliers d'euros envolés. Les contre-mesures.

9 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/fraude-au-virement

Pas besoin de pirater un serveur pour dévaliser une entreprise : il suffit de convaincre la comptabilité de faire un virement. Usurpation du dirigeant, faux fournisseur, faux changement de RIB — ces fraudes « à l'humain » coûtent des milliards chaque année.

1. Les scénarios classiques

- L'arnaque au président : un email urgent et confidentiel « du dirigeant » exige un virement immédiat
- Le faux fournisseur : « nos coordonnées bancaires ont changé, merci de mettre à jour le RIB »
- Le faux technicien ou la fausse banque qui demande un « virement test »
- La compromission d'une vraie boîte email d'un partenaire, rendant la demande crédible

2. Les contre-mesures organisationnelles

La parade est avant tout procédurale : aucune urgence, aussi pressante soit-elle, ne doit court-circuiter les vérifications.

- Tout changement de RIB se vérifie par téléphone, au numéro déjà connu (jamais celui de l'email)
- Double validation obligatoire au-delà d'un montant défini
- Aucun virement déclenché sur la seule base d'un email ou d'un appel, même « du patron »
- Sensibiliser explicitement la comptabilité et l'accueil, cibles prioritaires

3. Si le virement est parti

- Appeler immédiatement votre banque pour demander le rappel des fonds — chaque minute compte
- Déposer plainte sans délai
- Prévenir le vrai fournisseur si son identité a été usurpée
- Analyser la messagerie : la fraude découle souvent d'une boîte email compromise

4. Pourquoi ça marche : les ressorts psychologiques

Ces fraudes n'exploitent aucune faille technique — elles exploitent des réflexes humains parfaitement normaux :

- L'autorité : on ne fait pas répéter le président, on exécute
- L'urgence : « avant midi, c'est impératif » court-circuite la réflexion
- La confidentialité : « n'en parlez à personne, opération sensible » isole la victime de ceux qui auraient tiqué

- L'habitude : le faux fournisseur imite un processus routinier — la mise à jour d'un RIB n'alerte personne
- La flatterie : « je compte sur vous, vous êtes la seule personne de confiance » verrouille l'engagement

CAS CONCRET

Scénario type : vendredi 16 h 45, la comptable reçoit un email « du dirigeant » (en déplacement, injoignable) : acquisition confidentielle, virement de 48 000 € à faire avant la fermeture des banques, « je vous fais confiance ». Tous les ressorts y sont — autorité, urgence, secret, flatterie. La seule parade qui tient à 16 h 45 un vendredi : la procédure qui interdit ce virement sans double validation, quoi qu'il arrive.

L'essentiel à retenir

- 01 Instaurer la vérification téléphonique systématique des changements de RIB
- 02 Mettre en place la double validation des virements importants
- 03 Écrire noir sur blanc qu'aucune urgence ne court-circuite ces règles
- 04 Sensibiliser la comptabilité et l'accueil aux scénarios d'usurpation
- 05 Protéger les messageries par double authentification
- 06 Afficher le numéro d'urgence de la banque en cas de fraude

Questions fréquentes

Combien de temps a-t-on pour rappeler un virement frauduleux ?

Très peu : les fonds sont souvent dispersés en quelques heures vers d'autres comptes, parfois à l'étranger. Appelez la banque dans la minute où la fraude est découverte pour demander le rappel (recall) — les chances de récupération chutent drastiquement après 24-48 h. D'où l'importance du numéro d'urgence de la banque affiché et connu.

La banque doit-elle rembourser un virement frauduleux ?

Rarement : un virement que vous avez vous-même autorisé, même sous manipulation, n'engage généralement pas la responsabilité de la banque. C'est différent d'un paiement non autorisé (carte piratée). Certaines assurances cyber ou fraude couvrent ce risque — vérifiez votre contrat, c'est une option souvent séparée.

Le dirigeant est réellement pressé parfois. Comment éviter de bloquer le vrai business ?

La procédure doit prévoir le cas : une validation express reste possible, mais toujours par un second canal (le dirigeant confirme de vive voix ou via un canal interne authentifié). Ce qui est interdit n'est pas la rapidité — c'est le virement déclenché sur la foi d'un seul message. Un vrai dirigeant comprend la règle : elle protège son argent.

Nos fournisseurs peuvent-ils être le maillon faible ?

Oui, et c'est le cas le plus vicieux : leur boîte email compromise envoie de vraies factures avec un RIB modifié, dans une conversation existante. La parade est chez vous : tout changement de coordonnées bancaires, même venant d'un contact habituel, se vérifie par téléphone au numéro que VOUS connaissez. Prévenez aussi vos clients que vos propres coordonnées ne changeront jamais par simple email.

Pour aller plus loin

Cybermalveillance.gouv.fr — faux ordres de virement — www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/faux-ordres-de-virement-fovi-escroquerie

Police nationale — signaler une escroquerie (THESEE) — www.service-public.fr/particuliers/vosdroits/N31138

Un doute, une urgence, un incident ?

Cyberionis évalue votre exposition, prépare vos défenses et vous épaula pour réagir vite en cas d'attaque.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr