

Se protéger sur Internet - Arnaques aux envois de RIB par e-mail

Contexte

TL DR

“ Les boîtes des victimes sont discrètement piratées et les échanges de mails contenant un RIB [sont] détournés. Un phénomène qui prend de l'ampleur avec la crise économique et le télétravail.

Le Parisien - Site Internet - Vous envoyez vos coordonnées bancaires par mail ?

Attention à la nouvelle arnaque aux faux RIB

Les attaques aux faux ordres de virement et aux changements de RIB sont dans le *top 10* des cinquante principales arnaques touchant les professionnels.

Témoignages

“ Une administratrice d'une troupe de théâtre en région parisienne sollicite sa mairie afin d'obtenir une subvention de 4 000 €. Elle leur adresse donc un e-mail auquel elle joint son RIB. La mairie recevra bien le mail, mais le RIB aura été usurpé. Françoise ne recevra jamais sa subvention.

Le Parisien - Site Internet - Vous envoyez vos coordonnées bancaires par mail ?

Attention à la nouvelle arnaque aux faux RIB

“ Un arboriculteur dans la Sarthe pensait régler les 3 300 € pour la réparation d'une machine. Son virement ne créditera jamais son fournisseur. La facture était bonne, mais pas le RIB.

Que Choisir - Site Internet - Le faux RIB fait irruption dans les boîtes mail

Principe de l'arnaque

Le créancier transmet son relevé d'identité bancaire sur lequel figure son nom et ses coordonnées bancaires. Cependant, avant que le débiteur prenne connaissance du RIB, une tierce personne remplace les coordonnées bancaires par des coordonnées qui le rendent bénéficiaire du futur virement.

Les noms et adresse du bénéficiaire d'origine n'ont pas besoin d'être modifiés, seules les coordonnées bancaires sont nécessaires au virement, plus précisément le code IBAN (*International Bank Account Number : Numéro de compte en banque international*) et le code BIC (*Bank Identifier Code : Code d'identification de la banque*).

RIB : Relevé d'Identité Bancaire

Identifiant national de compte bancaire - RIB

Banque	Guichet	N° compte	Clé	Devise
00000	00000	00000000000	00	EUR

Domiciliation
NOM DE L'AGENCE DE RATTACHEMENT

Identifiant international de compte bancaire

IBAN (International Bank Account Number)						
FR00	0000	0000	0000	0000	0000	000

BIC (Bank Identifier Code)
XXXXFRXX

Domiciliation

NOM DE L'AGENCE DE RATTACHEMENT
ADRESSE DE LA BANQUE
CODE POSTALE ET VILLE

☎ 06 00 00 00 00

Titulaire du compte (Account Owner)

PRENOM NOM
ADRESSE DU TITULAIRE
CODE POSTALE ET VILLE

Mode opératoire

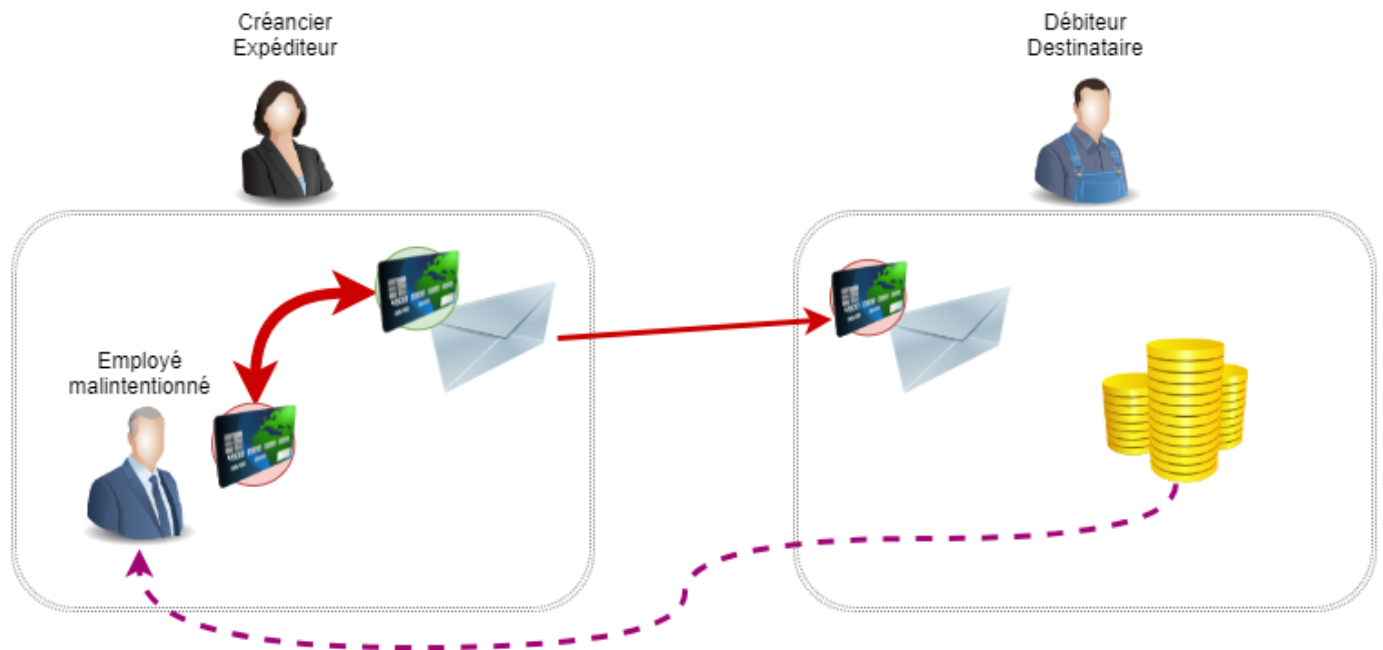
Malveillance interne

Une personne malintentionnée employée par le créancier pourrait se connecter à la messagerie de son entreprise afin de substituer le RIB original par un RIB dont il sera le bénéficiaire.

Cette procédure nécessite que l'employé ait accès à la messagerie de l'entreprise soit :

- sous un identifiant général,
- sous l'identifiant de la direction,
- ou un identifiant du service comptable.

L'identifiant désigne ici le couple « identifiant et mot de passe » du service de messagerie.



Hormis la substitution lors de l'envoi des e-mails, un employé ayant accès au serveur de stockage des données de l'entreprise pourrait substituer le RIB original par un autre dont il sera bénéficiaire.

Cybermalveillance

Côté expéditeur

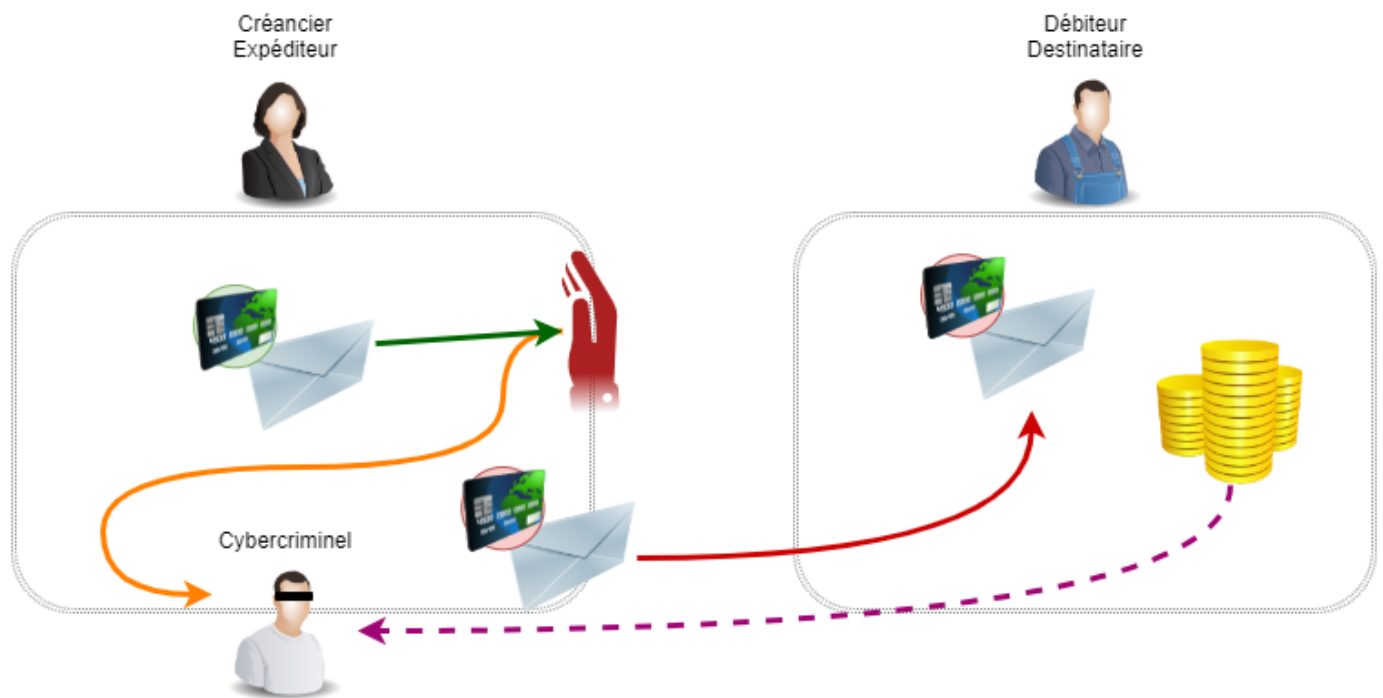
Un cybercriminel a infiltré le serveur de messagerie de l'expéditeur. Les messages contenant certains mots seront filtrés, comme :

- « RIB »,
- « Relevé d'identité bancaire »,
- « facture »...

Ce filtre aura deux fonctions :

- empêcher l'e-mail d'origine de partir ;
- informer le cybercriminel.

Ensuite, le cybercriminel substitue le RIB du créancier par le sien et transmet l'e-mail modifié au débiteur directement depuis la messagerie de l'expéditeur.



Cette approche est la plus technique à mettre en place, mais elle est aussi la plus difficile à déceler.

Côté destinataire

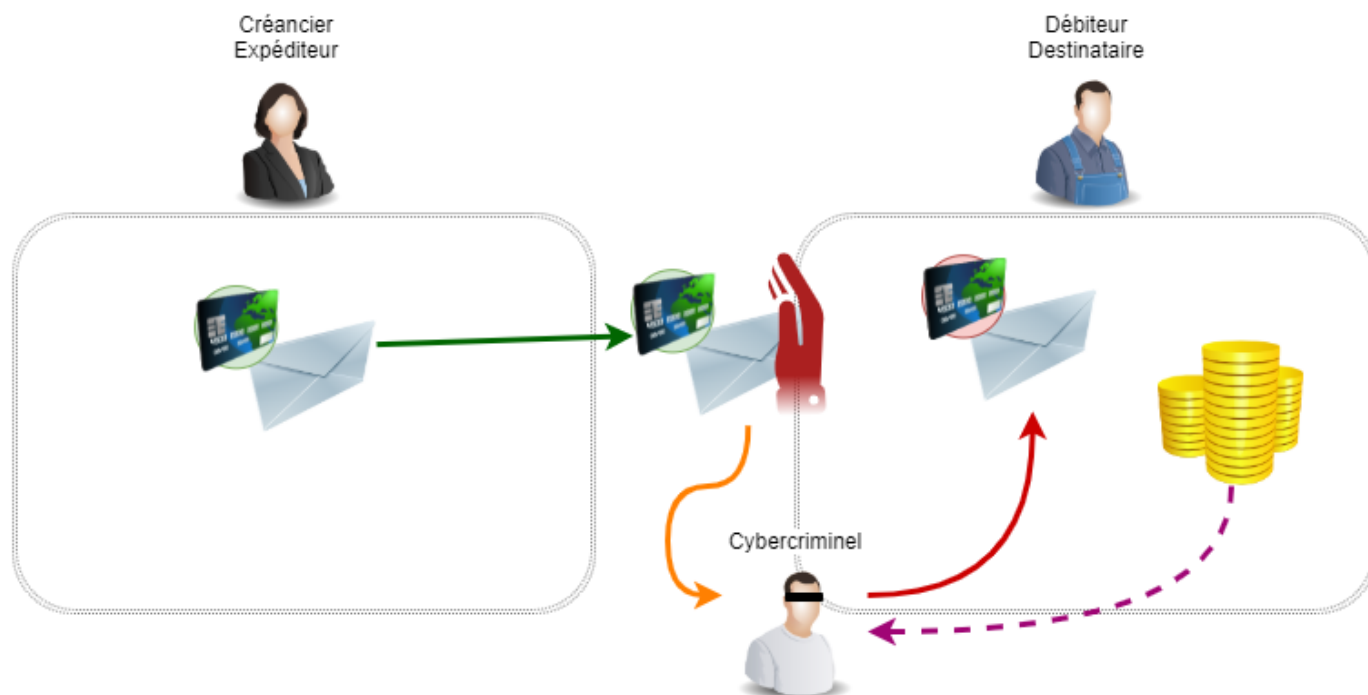
Un cybercriminel a infiltré la messagerie du destinataire. Les messages contenant certains mots seront filtrés, par exemple :

- « RIB »,
- « Relevé d'identité bancaire »,
- « facture »...

Ce filtre aura deux fonctions :

- empêcher d'être lu par le destinataire d'origine ;
- être transféré au cybercriminel.

Ensuite, le cybercriminel substitue le RIB du créancier par le sien, désactive le filtre et transmet l'e-mail modifié au débiteur.



Pour être plus crédible, le cybercriminel crée une adresse de messagerie proche de l'expéditeur d'origine. Par exemple :

- « ent.durand@gmail.com » **devient** « ent.durant@gmail.com »
- « jacques.durand@orange.fr » devient « jacques.durand@outlook.com »
- « contact@ent.durand.com » **devient** « contact.durand@orange.fr »

Cette approche est relativement simple à mettre en place. Le cybercriminel a besoin de disposer des identifiant et mot de passe de la messagerie internet du destinataire.

La finalité

Quel que soit le mode opératoire, la finalité reste la même : le compte bancaire de la personne malintentionnée est crédité et non celui du créancier. Le cybercriminel aura pris les dispositions afin de ne pas être identifiée (avec notamment un compte bancaire domicilié dans un pays étranger).

L'argent détourné est rapidement transféré, voire le compte bancaire frauduleux clôturé rendant impossible tout rappel de fond. Les chances de récupérer l'argent dérobé sont quasiment nulles.

“ Pour information

Les assurances ne couvrent pas ce désagrément, estimant qu'il s'agit d'un acte volontaire suite à une erreur de l'utilisateur, une négligence.

Précautions à prendre

Contexte de la **requête**

Tout comme dans l'arnaque au « faux président » ou « au prêt d'argent », il ne faut pas céder au chantage émotionnel et à l'urgence.

Le mail frauduleux peut faire mention de la nécessité de faire le virement au plus vite. Ce caractère d'urgence peut être accentué par un message expliquant que l'entreprise traverse des difficultés suite à un mauvais concours de circonstances. Sans ce règlement dans les meilleurs délais, l'entreprise devra, par exemple, se séparer de salariés.

Simple vérification du RIB

Une simple vérification du relevé d'identité bancaire peut mettre en déroute l'arnaque :

“ Votre plombier a rarement une banque basée aux îles Caïman.

Jean-Jacques Latour – Responsable de l'expertise en cybersécurité à
Cybermalveillance.gouv.fr

Cette information se retrouve notamment dans le code BIC : xxxxFRxx.

Double vérification du RIB

Ce conseil peut sembler contraignant à l'air de la communication dite asynchrone (la discussion n'est pas directe mais lorsque les interlocuteurs sont disposés à répondre). Cependant, elle reste la première étape pour déceler avec certitude une tentative d'arnaque :

- Procéder à une double vérification des coordonnées bancaires par un autre moyen de communication, idéalement un échange téléphonique.

Double authentification de sa messagerie Internet

Le double authentification permet de s'assurer qu'une nouvelle connexion à son service de messagerie est bien volontaire.

Cette vérification peut se faire sous plusieurs formes :

- Envoi d'un code temporaire par SMS ;
- Authentification à deux facteurs (« **2FA** »).

Outre le fait d'en avoir connaissance, la configuration de cette sécurité nécessite une aisance relative avec les outils numériques. Comme beaucoup de mesures de sécurité, la double authentification n'a pas pour vocation à faciliter le quotidien de l'utilisateur, mais bel et bien de dissuader les personnes malintentionnées : la sécurité numérique passe souvent par une contrainte additionnelle.

“ Analogie

Nous fermons la porte de nos maisons à clef lorsque nous nous absentons. Cette contrainte est devenue un automatisme afin de sécuriser nos biens domestiques.

Gestion des mots de passe

Comme tout mot de passe, il est vivement conseillé d'utiliser un mot de passe dit « robuste ». Il s'agit d'un mot de passe :

- relativement long (au moins une dizaine de caractères),
- comportant des caractères variés (lettres minuscules, majuscules, nombres, caractères spéciaux),
- n'ayant pas de logique particulière (base commune suivi de caractères variants suivant le site),
- unique (ne pas réutiliser ses mots de passes).

“ Analogie

Les clefs de notre quotidien en plus d'être toutes différentes (maison, voiture, boîtes aux lettres, etc.) sont également complexes, voire non-reproductibles.

L'utilisation d'un gestionnaire de mots de passe est recommandé. Cependant, son usage nécessite une période d'apprentissage qui peut dissuader les utilisateurs.

Peines encourues

Pour information, le cybercriminel encoure de nombreuses peines :

- Poursuites pour escroquerie :
 - cinq années de prison,
 - 375 000 € d'amende ;
- Usurpation d'identité :
 - un an de prison,
 - 15 000 € d'amende ;
- Accès frauduleux à un système de traitement de données :
 - deux ans de prison
 - 60 000 € d'amende.



Révision #6

Créé 8 octobre 2021 00:13:02 par Mickaël G.

Mis à jour 9 décembre 2021 21:57:13 par Mickaël G.