

Identifier et reconnaître les tentatives de fraude aux entreprises

Rien ne remplacera jamais votre propre vigilance ni la pédagogie déployée auprès de vos employés.

Elles sont indispensables pour faire face à la créativité des fraudeurs pour dérober des données clients, usurper une identité ou mettre en place toutes sortes d'escroqueries et virements frauduleux. C'est le sens de ce guide qui recense les techniques les plus couramment utilisées,

afin de pouvoir les identifier et s'en prémunir.

Les banques, premières visées par ces tentatives de fraude, ont pu constater un report important de ces tentatives vers les entreprises, quelle que soit leur taille, y compris vers les TPE et PME.

Suivez le guide pour reconnaître et anticiper les tentatives de fraudes.



Depuis 2010, des centaines d'entreprises ont été victimes en France (ou dans leurs filiales Européennes) d'un préjudice qui se chiffre en centaines de millions d'euros.



La fraude au Président



OBJECTIF DU FRAUDEUR :

obtenir d'un collaborateur de l'entreprise qu'il effectue un **virement à destination de l'étranger**.

SON PROCESS : usurpation d'identité d'un dirigeant, de la police, de la répression des fraudes ou d'un organisme d'état (dans le cadre d'une enquête sur la tentative de fraude, si la première approche n'a pas fonctionné).

SES PRATIQUES : demande urgente intervenant souvent tardivement dans la journée, la veille d'un weekend ou d'un jour de congés (**caractère urgent et confidentiel, demande de discrétion**, force de persuasion et autorité de l'interlocuteur).

! Les escrocs sont tenaces, même en cas d'échec, ils renouvellent régulièrement leurs modes opératoires. S'ils décèlent que vous avez alerté la police, ils peuvent rappeler en prenant cette identité.

ICI VOTRE PRÉSIDENT, MONSIEUR PAUL...

... JE SAIS QUE JE PEUX COMPTER SUR VOTRE DISCRÉTION...

... EN URGENCE UN PAIEMENT PAR VIREMENT.

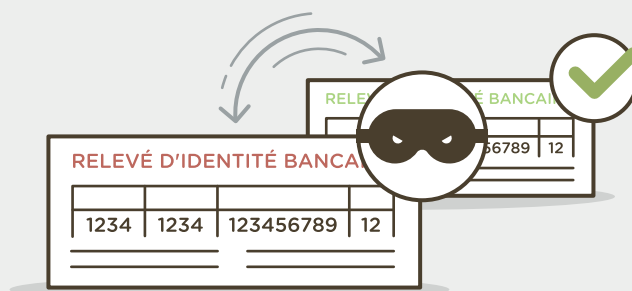


Comment prévenir ce type de fraude ?


- ✓ **Informez vos employés** sur ces risques et le respect de procédures internes strictes.
- ✓ Sécurisez vos procédures d'ordre de virement **en séparant la rédaction de l'ordre de sa validation**.
- ✓ Facilitez les échanges avec la hiérarchie.



La fraude aux coordonnées bancaires



JE VOUS APPELLE
POUR VOUS
SIGNALER QUE NOUS
AVONS CHANGÉ DE
BANQUE...

 Les escrocs se renseignent en amont pour collecter des données et informations sur les dirigeants (sur internet ou lors d'appels précédents sous de fausses identités).

OBJECTIF DU FRAUDEUR : obtenir d'un collaborateur de l'entreprise qu'il effectue un **changement de coordonnées bancaires** de l'un de vos fournisseurs.

SON PROCESS : usurpation d'identité d'un fournisseur habituel de votre entreprise, essentiellement par téléphone.

SES PRATIQUES : envoi d'un nouvel IBAN pour effectuer les paiements courants, en cohérence avec les procédures habituelles du fournisseur.



Comment prévenir ce type de fraude ?

- Demandez toujours la confirmation de tout changement auprès de **vos interlocuteurs habituels**.
- Vérifiez la **réalité de la prestation indiquée sur la facture** fournie auprès du collaborateur.
- Soyez très vigilant si les **nouvelles coordonnées bancaires** sont à **l'étranger** ou si les coordonnées mentionnées sont inhabituelles (e-mail, téléphone, fax...).



La fraude au faux technicien



OBJECTIF DU FRAUDEUR :

obtenir des identifiants de connexion, provoquer des virements frauduleux, installer des logiciels malveillants.

SON PROCESS : usurpation d'identité d'un technicien informatique de votre banque.

SES PRATIQUES :

arguments prétextes (anomalies relevées sur le compte, nécessité d'effectuer des tests de virements...)

! Un virement est irrévocable et ne peut être annulé, on ne vous demandera jamais d'effectuer un « virement test ».

JE VOUS ENVOIE PAR E-MAIL UN LIEN VOUS PERMETTANT DE TÉLÉCHARGER UN CORRECTIF...

... EFFECTUER QUELQUES VIREMENTS TESTS...

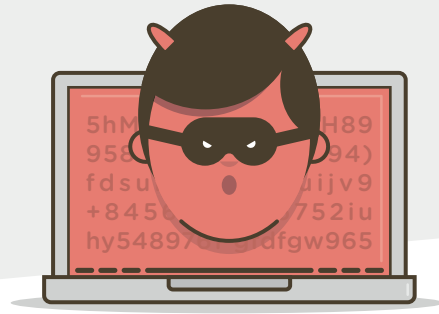


Comment prévenir ce type de fraude ?

- ✓ **Ne donnez pas l'accès à distance à votre poste de travail.** Le faux technicien pourrait alors installer des logiciels espions et récupérer toutes les données enregistrées sur votre poste, et ceci sans que vous le voyiez.
- ✓ **Aucun technicien de la banque ne contactera un client pour faire une mise à jour sur le poste d'un client.**
- ✓ **Ne diffusez pas d'informations (organigramme...) sur les personnes habilitées à réaliser des virements.**



Le ransomware



! Ce type d'attaque progresse de façon exponentielle, que ce soit auprès des particuliers ou des entreprises, et cible sans distinction tous les systèmes d'exploitation, y compris les mobiles.



OBJECTIF DU FRAUDEUR : obtenir une rançon en échange du déverrouillage de fichiers chiffrés sur votre poste ou votre serveur.

SON PROCESS : exécution du chiffrement de tous vos fichiers via un lien ou une pièce jointe dans un e-mail, et/ou en exploitant une faille de sécurité non corrigée d'un logiciel.

SES PRATIQUES : e-mail contrefait aux couleurs d'une entreprise connue (phishing) avec un lien vers un fichier exécutable (pour télécharger une facture par exemple), menace d'effacer vos données ou de les rendre publiques si une rançon (en bitcoins) n'est pas payée dans un délai très court (souvent jusqu'à 96 heures).

Comment prévenir ce type de fraude ?

- ✓ Effectuez des sauvegardes régulières de vos données.
- ✓ Installez un logiciel anti-virus et le maintenir à jour vous permet de vous protéger des ransomwares existants les plus courants.
- ✓ Au moindre doute sur l'expéditeur du mail, ne cliquez jamais sur une pièce jointe.
- ✓ Activez les mises à jours importantes de sécurité pour une installation automatique sur votre système d'exploitation et vos logiciels, afin qu'elles soient installées dès la publication (correction de failles de sécurité).



Spam, phishing, spyware...



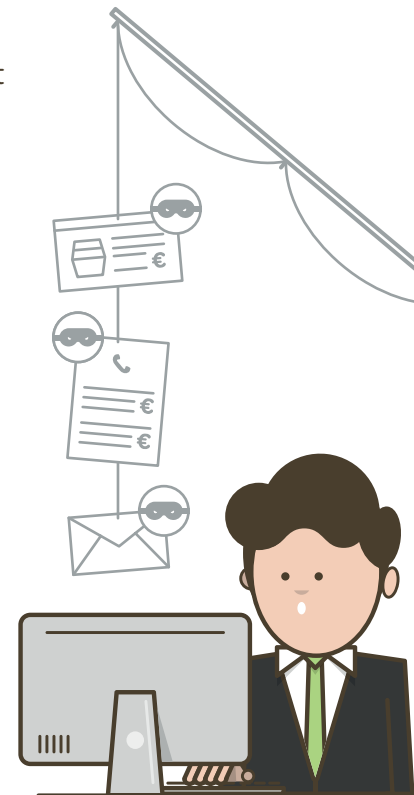
OBJECTIF DU FRAUDEUR : obtenir des données de connexion ou des données clients.

SON PROCESS : lien ou PJ frauduleuse dans un e-mail imitant celui d'une société, déclenchant l'installation d'un **logiciel espion**.

SES PRATIQUES : e-mail contrefait à la charte d'une société cliente, utilisation des failles de sécurité sur vos logiciels, utilisation de données/adresses e-mail récupérées en amont (qui masque la véritable adresse de l'expéditeur). L'objet du message peut prendre la forme de nombreux

prétextes (facture, mise à jour d'un logiciel, virement en attente, virement ou opération frauduleuse remontée par votre banque...

! Les e-mails contrefaits comportent de moins en moins de fautes d'orthographe et sont de plus en plus difficiles à identifier.



Comment prévenir ce type de fraude ?

- ✓ N'ouvrez pas et ne conservez pas de messages non sollicités, avec des pièces jointes d'origine inconnue.
- ✓ Activez un pare-feu et un logiciel anti-virus complet (et à jour) sur tous les postes de votre entreprise.
- ✓ Effectuez des sauvegardes régulières de vos données.
- ✓ Mettez régulièrement à jour vos logiciels, limitant ainsi les risques d'exploitation des failles de sécurité et d'intrusion.
- ✓ Restreignez l'installation de logiciels à une procédure strictement encadrée.

Vous pensez avoir été **victime** de fraude ?



En cas de fraude ou de tentative de fraude, contactez rapidement votre banque et la police (OCRGDF) :

Crédit Mutuel de Bretagne :

<https://www.cmb.fr>

Informez au plus vite votre conseiller
en cas de fraude.

**OCRGDF (Office Central pour la
Répression de la Grande Délinquance
Financière) :**

ocrgdf-sec.dcpjaef@interieur.gouv.fr
T : 01 40 97 43 20

Informations & conseils :

**ANSSI - Agence Nationale
de la Sécurité des systèmes
d'informations :**

<http://www.ssi.gouv.fr/entreprise>
[http://www.ssi.gouv.fr/guide/guide-
dhygiene-informatique/](http://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/)

**Site d'aide contre les attaques
de type RansomWare,
mis en place par Interpol
et plusieurs solutions d'anti-virus :**

<https://nomoreransom.org>

Le service **Info Escroquerie**, composé de policiers et de gendarmes
peut également vous conseiller et vous orienter, au :

0 805 805 817

Service &
appel gratuits



Pour en savoir plus, rendez-vous sur :
<https://www.cmb.fr/securite>