

FRAUDE AU PRÉSIDENT

La fraude au Président consiste à piéger un collaborateur habilité à effectuer les paiements de l'entreprise, le but étant qu'il paie une fausse facture ou réalise un transfert d'argent non autorisé.

COMMENT ÇA MARCHE ?

Par téléphone ou courriel, un fraudeur se fait passer pour un dirigeant de la société ou un directeur administratif et financier.

Les fraudeurs connaissent bien l'entreprise ciblée.

L'arnaqueur réclame un paiement urgent.

Les expressions courantes utilisées: «confidentialité», «la société vous fait confiance».



L'arnaqueur demande des paiements internationaux vers des banques en dehors de l'Europe.

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

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

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

COMMENT DÉTECTER L'ARNAQUE ?

➤ Contact direct d'un dirigeant avec lequel vous n'êtes normalement pas en contact

➤ Demande inhabituelle contraire aux procédures internes

➤ Demande de confidentialité absolue

➤ Menaces ou flatteries / promesses de récompense inhabituelles

QUE FAIRE EN CAS DE TENTATIVE D'ESCROQUERIE ?

SI VOUS ÊTES DIRIGEANT/E D'UNE SOCIÉTÉ

Soyez attentif/ve aux risques et assurez-vous que les collaborateurs soient conscients de ce type de risque.

Invitez votre personnel à la prudence concernant les demandes de paiement.

Prévoyez des protocoles internes pour les paiements.

Prévoyez une procédure pour vérifier l'authenticité des demandes de paiement reçues par courriel.

Ne dérogez jamais aux procédures que vous avez mises en place.

Contrôlez les informations publiées sur le site de votre société, limitez-les et soyez prudent/e vis-à-vis des médias sociaux.

Actualisez et améliorez la sécurité technique du process de validation d'un paiement.



Contactez toujours la police en cas de tentative de fraude, même si vous n'êtes pas tombé/e dans le piège.

SI VOUS ÊTES COLLABORATEUR

Appliquez strictement les procédures de sécurité prévues pour les paiements et les acquisitions. **Ne sautez aucune étape et résistez à la pression.**

Vérifiez toujours attentivement les adresses courriel lorsque vous traitez des informations sensibles / paiements.

En cas de doute sur un ordre de transfert, **consultez un collègue compétent.**

N'ouvrez jamais de liens / documents attachés douteux reçus par courriel. Soyez très vigilant/e lorsque vous vérifiez vos courriels privés sur un ordinateur de la société.

Limitez les informations et soyez attentif/ve en ce qui concerne les médias sociaux.

Ne partagez pas d'informations sur la hiérarchie dans l'entreprise, la sécurité ou les procédures.



Si vous recevez un courriel ou appel douteux, informez toujours votre service informatique.

ARNAQUES AUX FAUX PLACEMENTS

Les arnaques à l'investissement sont de faux placements présentés comme très rentables (actions, obligations, cryptomonnaies, métaux rares, investissements fonciers à l'étranger ou énergie alternative).

QUELS SONT LES SIGNES ?

- On vous promet un investissement sûr avec des gains rapides et importants.
- L'offre est limitée dans le temps.
- Vous recevez sans cesse un appel non sollicité.
- L'offre ne vaut que pour vous et vous ne devez pas la partager.



QUE FAIRE ?

- **Demandez toujours un conseil financier impartial** avant de payer ou d'investir.
- **Ne donnez pas suite aux appels importuns** visant des opportunités d'investissement.
- **Méfiez-vous** des promesses d'investissements soi-disant sûrs avec des gains très importants garantis.
- **Attention aux escroqueries à venir.** Si vous avez déjà répondu à une arnaque, les escrocs essaieront de vous cibler à nouveau ou de vendre vos informations à d'autres criminels.
- **Contactez la police** si vous avez des doutes.

FRAUDE AU RIB/IBAN

COMMENT CELA SE PASSE-T-IL ?



- Une entreprise est contactée par quelqu'un prétendant être un fournisseur.
- Il peut y avoir plusieurs approches combinées : téléphone, lettre, courriel, etc.
- L'escroc demande que les données bancaires (du bénéficiaire) pour le paiement des futures factures soient modifiées. Le nouveau numéro de compte donné est contrôlé par l'escroc.

QUE FAIRE ?

Assurez-vous que vos **collaborateurs soient informés et attentifs** à ce type de fraude et sachent s'en prémunir.

Prévoyez une **procédure pour vérifier** l'authenticité des demandes de paiement (par ex. contrôle de la réalité de la prestation, historique des relations avec le fournisseur...).

Vérifiez toutes les demandes supposées émaner de vos créanciers, surtout si vous êtes invité/e à modifier leurs données bancaires pour les paiements à venir.

N'utilisez pas les données de contact reprises dans les lettre/fax/courriel demandant des modifications. Réutilisez celles de **précédents messages**.

Prévoyez un **point de contact unique dédié** auprès des sociétés auxquelles vous faites des versements **réguliers**.

EN TANT QU'ENTREPRISE



Recommandez au chargé de paiement des factures de **toujours vérifier que celles-ci ne présentent pas d'irrégularités**.

Prévoyez plusieurs personnes pour valider un paiement important.

Surveillez les informations publiées sur le site de votre entreprise et évitez de parler de vos contrats et de vos fournisseurs. Veillez à ce que vos collaborateurs limitent les informations sur la société qu'ils partagent sur les réseaux sociaux.

Mettez en place des **formations sécurité** pour votre service financier et comptable.

EN TANT QUE COLLABORATEUR



Pour les paiements au-delà d'un certain seuil, **prévoyez une procédure pour confirmer** le numéro de compte et le bénéficiaire (par ex. une réunion avec la société).

Après le paiement d'une facture, **informez le destinataire** par courriel. Par sécurité, indiquez le nom de la banque du bénéficiaire et les quatre derniers chiffres du compte utilisé.

Limitez les informations sur votre employeur **que vous partagez** sur les médias sociaux.



Rapportez toujours à la police toute tentative de fraude, même si vous n'en avez pas été victime.

ARNAQUES AUX ACHATS EN LIGNE

Les transactions en ligne sont souvent intéressantes, mais attention aux arnaques.

QUE FAIRE ?

- **Privilégiez les sites marchands hébergés dans un pays de la communauté européenne** afin de bénéficier davantage de garanties et de recours en cas de litige.
- **Faites des recherches** - Vérifiez les avis clients avant d'acheter.
- **N'utilisez qu'un service de paiement sécurisé (3D Secure, wallets, carte de paiement virtuelle...)** - Vous aurez plus de chances de récupérer votre argent.
- **N'utilisez qu'un service de paiement sécurisé (3D Secure, wallets, carte de paiement virtuelle...)** - S'ils demandent un service de transfert d'argent ou un virement électronique, réfléchissez !
- **Ne payez que par une connexion internet sécurisée (https:// 🛡️)** - Evitez d'utiliser un wifi public ouvert ou gratuit.
- **N'utilisez qu'un dispositif sécurisé** - Tenez vos systèmes d'exploitation et logiciel de sécurisation à jour.
- **Attention aux offres sensationnelles ou pour des produits miracles - Méfiez-vous de ce qui a l'air trop beau pour être vrai (prix nettement inférieur à la valeur moyenne connue du produit par exemple).**
- **Un pop-up vous annonce que vous avez gagné un prix ? Attention, vous pourriez ne gagner qu'un logiciel malveillant.**
- **Le produit n'arrive pas ? Contactez le vendeur. La banque ne s'immiscera pas dans un litige commercial. Vérifiez sur votre compte bancaire le débit de l'opération et saisissez les organismes de traitement des litiges.**



Offre spéciale
SUPER OFFRE

70%



Rapportez toujours à la police toute tentative de fraude, même si vous n'en avez pas été victime.

COURRIELS D'HAMEÇONNAGE BANCAIRE

Les courriels d'hameçonnage bancaire sont des courriels d'escrocs qui incitent les destinataires à partager leurs données personnelles, financières ou de sécurité.

COMMENT CELA SE PASSE-T-IL ?

Ces courriels :

peuvent **ressembler** aux correspondances envoyées par les banques (ex. logo, trame et discours identiques à de vrais courriels).



QUE FAIRE ?

- **Gardez vos logiciels et votre antivirus à jour.**
- Malgré l'urgence décrite, **prenez le temps d'examiner attentivement** la demande.
- Soyez très **vigilant/e** si un courriel «bancaire» vous invite à communiquer une information sensible (ex. votre mot de passe de compte en ligne).
- **Vérifiez attentivement le courriel** : comparez l'adresse avec de précédents messages authentiques de votre banque. Contrôlez les fautes d'orthographe/de grammaire.
- **Ne répondez pas à un courriel suspect**, renvoyez-le plutôt à votre banque en tapant l'adresse vous-même.
- **Ne cliquez pas sur le lien « télécharger le document attaché ».**
- En cas de doute, **connectez-vous à votre site bancaire ou appelez votre banque.**
- N'agissez jamais dans la précipitation.



Les cybercriminels comptent sur le fait que les gens sont pressés ; au premier abord, ces faux courriels peuvent sembler vrais.



Les cybercriminels investissent de plus en plus les terminaux mobiles tablette et smartphone. Veillez à la mise à jour de leurs logiciels notamment de sécurité.

#CyberScams



ESCROQUERIE SENTIMENTALE

Les escrocs choisissent leurs victimes sur des sites de rencontre, mais aussi via les médias sociaux ou par courriel.



QUELS SONT LES SIGNES ?



QUE FAIRE ?

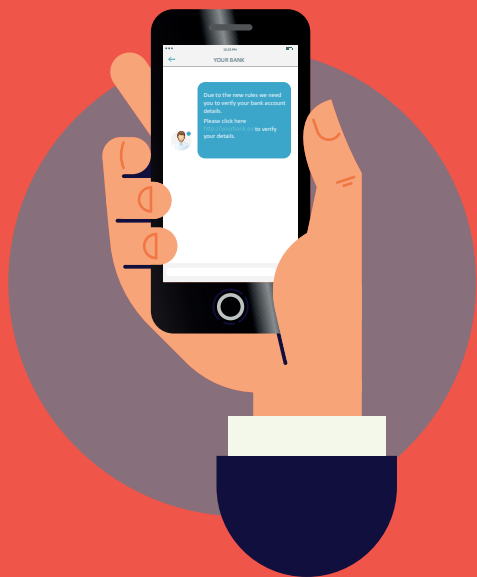
- **Soyez très prudent/e** quant aux données personnelles que vous partagez sur les réseaux sociaux / sites de rencontre.
- **Pensez toujours aux risques.** Les escrocs sont présents sur les sites les plus réputés.
- **Ne vous précipitez pas** et posez des questions.
- **Vérifiez** que la photo ou le profil n'est pas utilisé sur d'autres sites.
- **Soyez attentif/ve** aux fautes d'orthographe/grammaire, à leurs contradictions et excuses, par ex. la panne de caméra.
- **Ne partagez pas** d'informations qui pourraient vous amener à subir du chantage.
- Si vous acceptez une rencontre de visu, dites à vos **amis/famille** où vous allez.
- **Méfiez-vous des demandes de fonds.** N'envoyez jamais ni argent, ni données de carte de crédit, de compte en ligne, de copies de documents personnels.
- **Ne leur versez jamais de paiement initial.**
- **Ne transférez pas** d'argent pour un tiers : le blanchiment d'argent est un délit pénal.

VOUS ETES VICTIME ?

Ne soyez pas gêné/e : allez porter plainte !
Stoppez immédiatement tout contact.
Conservez tous les échanges, comme les « Chats ».
Déposez plainte auprès de la police.
Informez le site sur lequel l'escroc vous a abordé/e.
Si vous avez fourni vos données de compte, contactez votre banque.

TENTATIVE DE VOL DE DONNÉES PERSONNELLES (« PHISHING » / « HAMEÇONNAGE »)

L'hameçonnage par texto est une tentative d'appropriation de données personnelles (financières ou de sécurité) par des escrocs.



COMMENT CELA SE PASSE-T-IL ?

Le texto vous demandera de cliquer sur un lien ou d'appeler un numéro pour « vérifier », ou « actualiser » ou « réactiver » votre compte bancaire... mais le lien aboutit à un faux site bancaire ou l'appel vous met en relation avec l'escroc prétendant être une banque qui captera vos données confidentielles ou tentera de vous faire réaliser des opérations à son profit.

COMMENT SE PRÉMUNIR D'UN TEXTO FRAUDULEUX?

- **Ne cliquez pas sur des liens, documents attachés ou images** que vous recevez dans des textos non sollicités sans avoir d'abord vérifié l'expéditeur.
- **Ne vous pressez pas.** Prenez votre temps et faites les vérifications appropriées avant de répondre.
- **Ne répondez jamais à un texto** vous demandant votre code PIN ou votre mot de passe de banque en ligne ou toutes autres données de sécurité.
- Si vous pensez avoir répondu à un texto d'hameçonnage et avoir fourni vos données bancaires, **contactez votre banque immédiatement.**

FAUX SITES BANCAIRES

Les courriels d'hameçonnage contiennent classiquement des liens vers un faux site bancaire où vous sont demandées vos informations financières et personnelles.



COMMENT DÉTECTER L'ARNAQUE ?

Les faux sites bancaires ressemblent aux sites originaux. Ces sites affichent souvent une fenêtre pop-up vous demandant d'entrer vos identifiants bancaires. Les vraies banques n'utilisent pas de telles fenêtres.

Caractéristiques de ces sites :

Urgence : les sites officiels n'afficheront jamais de tels messages.



Fenêtres pop-up : en général utilisées pour rassembler des informations sensibles sur vous. Ne cliquez pas sur celles-ci et n'y indiquez pas vos données personnelles.

Design raté : méfiez-vous des sites présentant des anomalies graphiques ou des fautes de grammaire/d'orthographe.

QUE FAIRE EN CAS DE TENTATIVE D'ESCROQUERIE ?



Ne cliquez jamais dans les courriels sur des liens menant au site de votre banque.



Tapez toujours le lien vous-même ou utilisez un lien existant stocké dans vos « favoris ».



Utilisez un navigateur internet permettant de **bloquer les fenêtres pop-up**.



Si un fait important requiert vraiment votre attention, votre banque vous en avertit lorsque vous **accédez à votre compte en ligne**.

HAMEÇONNAGE PAR TÉLÉPHONE

L'hameçonnage vocal est une fraude téléphonique au cours de laquelle le fraudeur s'efforce d'obtenir de sa victime des données personnelles, financières ou de sécurité, voire un transfert d'argent.

QUE FAIRE EN CAS DE TENTATIVE D'ESCROQUERIE ?

- **Méfiez-vous** des appels téléphoniques non sollicités.
- **Notez le numéro de l'appelant** et dites-lui que vous allez le rappeler.
- **Cherchez le numéro de l'entreprise concernée** et appelez-la avec ce numéro.
- **Ne appelez pas l'escroc en utilisant un numéro de téléphone qu'il vous a donné** (il pourrait s'agir d'un faux numéro).
- Les escrocs peuvent avoir accès facilement à vos données personnelles par les médias sociaux par exemple. **N'accordez pas de crédit à un appelant** parce qu'il dispose des informations vous concernant.
- **Ne communiquez pas** vos codes de carte de crédit / débit ou mot de passe de banque en ligne. Votre banque ne vous demandera jamais ces informations.
- **Ne transférez pas d'argent** vers un autre compte à la demande de l'appelant. Votre banque ne vous demandera jamais d'agir de la sorte.
- Si vous pensez avoir affaire à un appel suspect, informez-en votre banque.

