COURRIELS D'IMPOSTEURS (BEC)/ARNAQUES AU PRÉSIDENT (CEO)

La fraude CEO/BEC consiste à piéger un collaborateur habilité à effectuer les paiements de l'entreprise, le but étant qu'il paie une fausse facture/réalise un transfert non autorisé.

COMMENT CELA SE PASSE-T-IL ?

Par téléphone ou courriel, un fraudeur se fait passer pour un dirigeant de la société (par ex. CEO ou CFO).

Ils connaissent bien l'organisation.

Ils réclament un paiement urgent.

Leurs expressions courantes : "confidentialité", "la société vous fait confiance", "pour l'instant indisponible".

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

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

Les instructions visant la procédure pourront être données plus tard, par courriel/un tiers.

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

Sont souvent demandés des paiements internationaux vers des banques en dehors de l'Europe.

QUELS SONT LES SIGNES ?

- Courriel/appel non sollicités
- Contact direct d'un dirigeant avec lequel vous n'êtes normalement pas en contact
- Demande de confidentialité absolue
- Pression et sentiment d'urgence
- Demande inhabituelle contraire aux procédures internes
- Menaces ou flatteries/promesses de récompense inhabituelles

QUE FAIRE ?

EN TANT QUE SOCIETE

Soyez attentif/ve aux risques et assurez-vous que les collaborateurs sont informés/conscients.

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.

Prévoyez des routines de notification pour contrer les fraudes.

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.

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

EN TANT QUE 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 pc 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 département IT.

#CyberScams

EUROPOL EC3 European Cybercrime Centre
EBF European Banking Federation
THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG Ministry of the Economy
SECURITY MADEIN.LU
BEE SECURE

ARNAQUES A L'INVESTISSEMENT

Les arnaques communes à l'investissement comprennent des opportunités de placement lucratives (actions, obligations, cryptomonnaies, métaux rares, investissements fonciers à l'étranger ou énergie alternative).

QUELS SONT LES SIGNES ?

- On vous garantit des gains rapides et un investissement sûr.
- 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.

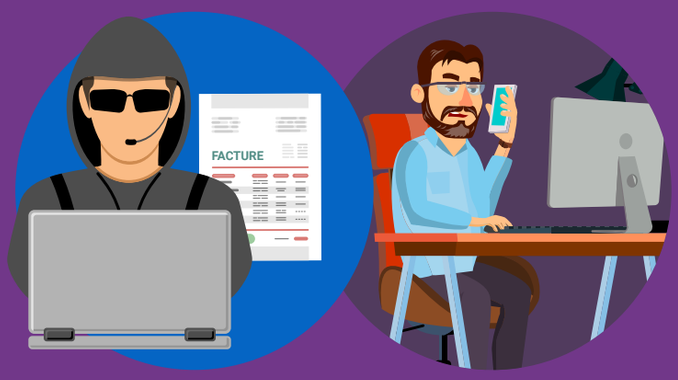
QUE FAIRE ?

- **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 sûrs, de gains importants et 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.

#CyberScams

EUROPOL EC3 European Cybercrime Centre
EBF European Banking Federation
THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG Ministry of the Economy
ABBL
SECURITY MADEIN.LU
BEE SECURE

FRAUDE A LA FACTURE



COMMENT CELA SE PASSE-T-IL ?

- Une entreprise est approchée par quelqu'un prétendant représenter un fournisseur (de service)/créancier.
- 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 ?

EN TANT QU'ENTREPRISE

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.

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

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

EN TANT QUE COLLABORATEUR

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.**

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

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 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 unique dédié.

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

#CyberScams

EUROPOL EC3 European Cybercrime Centre
EBF European Banking Federation
THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG Ministry of the Economy
ABBL
SECURITY MADEIN.LU
BEE SECURE

ARNAQUES AUX ACHATS EN LIGNE

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

QUE FAIRE ?

- **Passez** si possible **par des sites marchands nationaux,** vous vous en sortirez mieux en cas d'éventuels problèmes.
- **Faites des recherches** - Vérifiez les critiques avant d'acheter.
- **Utilisez une carte de crédit** -Vous aurez plus de chances de récupérer votre argent.
- **N'utilisez qu'un service de paiement sécurisé -** S'ils demandent un service de transfert d'argent ou un virement électronique, réfléchissez !
- Ne payez que via une **connexion internet sécurisée -** Evitez d'utiliser un wifi public ouvert ou gratuit.
- **Ne payez que via un dispositif sécurisé -** Tenez vos systèmes d'exploitation et logiciel de sécurisation à jour.

- Attention aux offres sensationnelles ou pour des produits miracles - **Ce qui l'air trop beau pour être vrai l'est sans doute !**
- 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. En l'absence de réponse, **contactez votre banque.**

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

#CyberScams

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG Ministry of the Economy · ABBL · SECURITY MADEIN.LU · BEE SECURE

COURRIELS D'HAMEÇONNAGE BANCAIRE

L'hameçonnage renvoie à des courriels de fraudeurs incitant 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.

reproduisent les logos, lay-outs et tons de vrais courriels.

vous invitent à télécharger un document attaché ou à cliquer sur un lien.

utilisent un langage qui évoque l'urgence.

QUE FAIRE ?

- **Gardez vos logiciels à jour,** et e.a. vos browser, antivirus et système d'exploitation.
- 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/téléchargez pas le document attaché,** retapez plutôt l'adresse correcte de votre banque dans votre browser.
- En cas de doute, **double-cliquez** sur votre site bancaire ou appelez votre banque.

Les cybercriminels escomptent que les gens sont occupés; au premier abord, ces faux courriels peuvent passer pour vrais.

#CyberScams

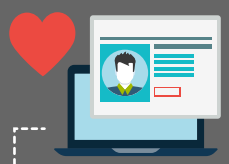
Attention quand vous utilisez un dispositif mobile : un téléphone ou une tablette peuvent avoir plus de mal à détecter une tentative d'hameçonnage.

EUROPOL EC3 European Cybercrime Centre
EBF European Banking Federation
THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG Ministry of the Economy
ABBL
SECURITY MADE IN.LU
BEE SECURE

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 ?



Un nouveau contact en ligne exprime des sentiments forts à votre égard et veut vous parler en privé.

Leurs messages sont souvent mal rédigés et vagues.

Leur profil en ligne ne cadre pas avec ce qu'ils vous racontent.

Il se pourrait qu'ils vous demandent des photos ou vidéos intimes.

€ € €

Ils gagnent votre confiance puis vous demandent de l'argent, des cadeaux ou vos n° de compte / données de carte de crédit.

Si vous n'envoyez pas l'argent, ils peuvent tenter le chantage. Si vous cédez, ils exigeront toujours plus.

ETES-VOUS VICTIME ?

Ne soyez pas gêné/e !
Stoppez immédiatement tout contact.
Si possible, 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.

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.
- **Enquêtez** sur la photo et le profil de la personne pour voir s'ils n'ont pas été utilisés ailleurs.
- **Soyez attentif/ve** aux fautes d'orthographe/grammaire, à leurs contradictions et excuses, par ex. la panne de caméra.
- **Ne partagez pas** d'infos/images compromettantes ouvrant la porte au 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.
- **Evitez** de leur verser un paiement initial.
- **Ne transférez pas** d'argent pour un tiers : le blanchiment d'argent est un délit pénal.

#CyberScams

EUROPOL EC3 European Cybercrime Centre
EBF European Banking Federation
THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG Ministry of the Economy
ABBL
SECURITY MADEIN.LU
BEE SECURE

TEXTO D'HAMEÇONNAGE BANCAIRE

L'hameçonnage par texto (smishing: SMS + phishing) est une tentative par des escrocs de s'approprier des données personnelles, financières ou de sécurité par texto.

COMMENT CELA SE PASSE-T-IL ?

Le texto vous demandera typiquement de cliquer sur un lien/d'appeler un numéro pour "vérifier", "actualiser" ou "réactiver" votre compte. Mais… le lien aboutit à un faux site et l'appel vous mène chez l'escroc prétendant être la vraie société.

QUE FAIRE ?

- **Ne cliquez pas sur des liens, documents attachés ou images** que vous recevez dans des textos non sollicités sans en 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.**

#CyberScams

EUROPOL EC3 European Cybercrime Centre
EBF European Banking Federation
THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG Ministry of the Economy
ABBL
SECURITY MADE IN.LU
BEE SECURE

FAUX SITES BANCAIRES

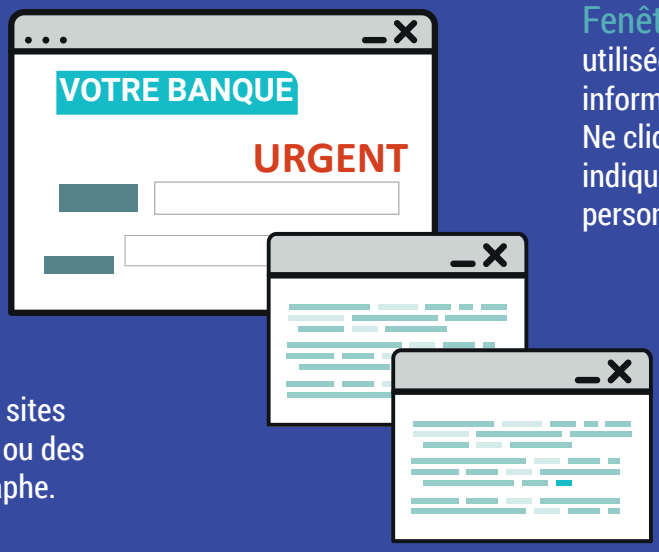
Les courriels d'hameçonnage contiennent classiquement des liens vers un faux site bancaire où vous sont demandées vos informations financières et personnelles.

QUELS SONT LES SIGNES ?

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 designs boîteux ou des fautes de grammaire/d'orthographe.

QUE FAIRE ?

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

Tapez toujours le lien vous-même ou utiisez un lien existant stocké dans vos"favoris".

Utilisez un browser 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.**

#CyberScams

EUROPOL EC3 European Cybercrime Centre
EBF European Banking Federation
THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG Ministry of the Economy
ABBL
SECURITY MADEIN.LU
BEE SECURE

HAMEÇONNAGE BANCAIRE VOCAL

L'hameçonnage vocal (vishing: voice + phishing) 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 ?

- **Méfiez-vous** des appels téléphoniques non sollicités.
- **Notez le numéro de l'appellant** et dites-lui que vous allez le rappeler.
- Afin de valider l'identité de l'appellant, **cherchez le numéro de téléphone de l'organisation** et contactez-le directement.
- **Ne validez pas l'appellant en utilisant le numéro de téléphone qu'il vous a donné** (il pourrait s'agir d'un numéro fantôme ou faux).
- Les escrocs peuvent trouver vos informations de base en ligne (par ex. médias sociaux). Un appellant n'est pas de bonne foi juste parce qu'il dispose de ces données.
- **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'appellant. Votre banque ne vous demandera jamais d'agir de la sorte.
- Si vous pensez avoir affaire à un appel suspect, informez-en votre banque.

#CyberScams

EUROPOL EC3 European Cybercrime Centre
EBF European Banking Federation
THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of the Economy
ABBL
SECURITY MADEIN.LU
BEE SECURE