LA FRAUDE AUX PAIEMENTS ET LES ENTREPRISES

Comment reconnaître et prévenir la fraude ?

febelfin

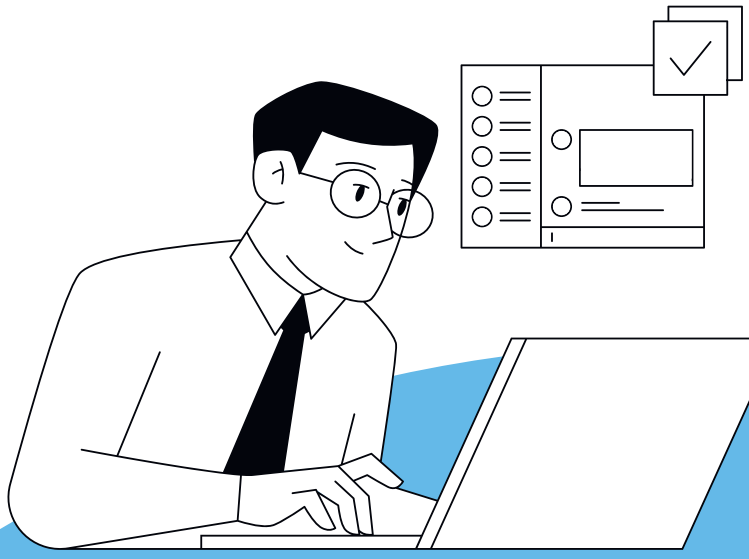
Les consommateur-rice-s, mais aussi les entreprises, sont de plus en plus souvent la cible de fraude aux paiements.

Il existe différents types de fraude aux paiements qui visent spécifiquement les entreprises et peuvent potentiellement entraîner de lourdes pertes financières. Il suffit de songer à la fraude au CEO, à la fraude à la facture, au phishing, etc.

Les banques investissent en permanence dans des systèmes de surveillance et de détection des fraudes mais, malheureusement, il n'est pas possible de détecter toutes les tentatives de fraude.

Cependant, en tant qu'entreprise, vous pouvez vous aussi prendre des dispositions pour améliorer la vigilance de votre personnel et mettre en place vos propres systèmes de sécurité. Car ce n'est qu'ensemble que nous pourrons arrêter les fraudeurs.

Dans la présente brochure, vous découvrirez 5 formes de fraude qui sont courantes dans les entreprises. Nous vous expliquons comment les fraudeurs tentent de tromper les gens et comment vous pouvez vous prémunir, vous-même ainsi que vos collaborateur-rice-s et votre entreprise. Dans cette publication, vous trouverez également des conseils utiles pour détecter ou – mieux encore – pour prévenir ces fraudes au sein de votre entreprise.



Formez vos collaborateur-rice-s financier-ère-s

Le personnel comptable constitue la première ligne de défense contre la fraude aux paiements. Ce sont ces personnes qui peuvent détecter les fraudes et empêcher les pertes financières. Nous vous recommandons de diffuser ce document en interne auprès de votre personnel. Encouragez les membres de la direction et tou-te-s les collaborateur-rice-s qui ont une procuration sur les comptes de l'entreprise à prendre connaissance de cette brochure.

FRAUDE À LA FACTURE

— Qu'est-ce que la fraude à la facture ?

Le nom le dit : dans le cas d'une fraude à la facture, les escrocs falsifient une facture. Ils commencent par intercepter une facture authentique, remplacent les coordonnées bancaires du bénéficiaire par les leurs et envoient la facture modifiée. Une entreprise peut recevoir une fausse facture ou envoyer elle-même une vraie facture qui est ensuite falsifiée.

— Comment fonctionne la fraude à la facture ?

Tout d'abord, les fraudeurs interceptent une facture. Cela peut se faire de plusieurs manières :

- Via le circuit postal : les fraudeurs dérobent les factures dans les boîtes aux lettres rouges de bpost ou dans les centres de tri.
- Ils les volent même dans les boîtes aux lettres des particuliers ou des entreprises.
- Ils pénètrent dans le système informatique d'un fournisseur et y interceptent les e-mails de facturation ou modifient le numéro de compte. Méfiez-vous donc également des factures que vous recevez par voie électronique.

Les fraudeurs modifient ensuite le numéro de compte du bénéficiaire.

- Souvent, ils scannent la facture originale et modifient les données (numéro de compte et parfois numéro de téléphone) du fournisseur/vendeur à l'aide d'un logiciel spécial.
- Ou bien ils joignent à la facture une lettre indiquant que le numéro de compte a été modifié. Parfois, ils apposent même sur l'enveloppe ou sur la facture elle-même un autocollant indiquant « Attention, numéro de compte modifié ».

Puis, ils envoient la facture modifiée.

Ils peuvent aussi rédiger des factures fictives.

CONSEILS POUR ÉVITER LA FRAUDE À LA FACTURE

- Comparez le numéro de compte figurant sur la facture avec celui se trouvant sur le bon de commande ou le site web officiel du vendeur ou du fournisseur.
- Soyez particulièrement vigilant-e si une facture indique un nouveau numéro de compte ou s'il y a un autocollant « Attention, numéro de compte modifié » sur l'enveloppe ou la facture proprement dite. Même s'il s'agit de la première facture que vous recevez d'un vendeur ou d'un fournisseur. Prenez le temps de vérifier le numéro de compte avant de procéder au paiement.
- Vous avez un doute ? Appelez l'entreprise en vous servant du numéro déjà repris dans votre base de données, et non du numéro figurant sur la facture (qui peut, elle aussi, avoir été falsifiée).
- Conservez les coordonnées et le numéro de compte bancaire de vos fournisseurs, même si vous payez par e-banking. Si vous recevez ensuite une nouvelle facture, vous pourrez facilement vérifier si le numéro de compte correspond aux données que vous avez enregistrées.
- Ne payez jamais une facture ou une note qui vous semble suspecte sans avoir vérifié que vous êtes bien client-e de cette entreprise ou que vous lui avez commandé quelque chose.

Vous recevez la facture par e-mail ? Alors vérifiez que l'adresse e-mail est bien correcte.

— J'ai malgré tout payé une fausse facture. Que faire ?

- Contactez au plus vite la banque de votre entreprise pour signaler la fraude. Votre banque demandera à la banque du bénéficiaire de rembourser l'argent. Cette banque essaiera également de bloquer le virement ou le compte afin que les retraits d'espèces par les fraudeurs ne soient plus possibles.
- Déposez une plainte auprès de la police.
- Signalez le cas sur le Point de contact (option « fausse facture »). Au terme de votre signalement, vous recevrez d'office des conseils sur les démarches que vous pouvez encore entreprendre et sur les personnes qui peuvent vous aider.

RÉAGISSEZ VITE.

Si vous détectez une fraude alors qu'un virement a déjà été effectué, prévenez immédiatement votre banque. Vous trouverez un aperçu de tous les points de contact sur le site https://cardstop.be/fr-be/home/quoi-bloquer/bloquer-votre-application-bancaire-ou-votre-compte-via-votre-banque.html

Si vous informez rapidement la banque, vous aurez plus de chances de récupérer l'argent volé. Il se peut également que vous deviez accomplir d'autres formalités auprès des autorités compétentes (dépôt de plainte auprès de la police...). Les experts des banques peuvent vous conseiller sur les démarches à accomplir.

FRAUDE AU CEO

— Qu'est-ce que la fraude au CEO ?

Dans le cas de la fraude au CEO, ou *social engineering*, les fraudeurs se font passer pour le CEO d'une entreprise (ou une personne de confiance interne ou externe) afin de manipuler un-e collaborateur-rice interne de cette entreprise pour qu'il/elle effectue une action (souvent un paiement) ou révèle des informations confidentielles.

— Comment fonctionne la fraude au CEO ?

- Les fraudeurs **commencent par recueillir des informations** sur les procédures de paiement internes d'une entreprise et sur ses collaborateur-rice-s habilité-e-s à effectuer des transactions de paiement importantes. Pour ce faire, ils les contactent par e-mail ou par téléphone et se font passer pour des auditeurs, des réviseurs d'entreprise ou des fonctionnaires d'un service public.

- Lorsque les fraudeurs disposent de suffisamment d'informations, ils **contactent un-e ou plusieurs collaborateur-rice-s responsables des paiements** (par exemple, la comptabilité) et se font passer pour le CEO. Pour ce faire, ils piratent généralement la mailbox du CEO ou créent une fausse adresse qui est presque semblable à l'adresse réelle du CEO. Ainsi, souvent, la différence avec l'adresse officielle tient à une seule lettre. Les fraudeurs concoctent une histoire dans laquelle une grosse somme d'argent doit être transférée de toute urgence et dans le plus grand secret.

- Parfois, les fraudeurs vont un peu plus loin en faisant intervenir un bureau de conseil ou un avocat (dont ils ont usurpé l'identité). Le bureau ou l'avocat confirme la transaction et répète que le paiement est urgent et secret.

- Les collaborateur-rice-s qui tombent dans le piège n'effectuent pas le paiement pour le véritable CEO mais – sans s'en rendre compte eux-mêmes – transfèrent d'importantes sommes d'argent vers les comptes de mules. De ces comptes, l'argent est ensuite redirigé vers le compte des fraudeurs.

CONSEILS POUR SE PRÉMUNIR CONTRE LA FRAUDE AU CEO

1. Vérifiez toujours le nom de domaine dans l'adresse électronique de l'expéditeur-rice.
2. Soyez vigilant-e en cas d'ordres « confidentiels » de transfert urgent de grosses sommes d'argent.
3. Si vous recevez une telle demande urgente, rappelez toujours le demandeur sur un numéro de téléphone que vous connaissez.
4. Ne laissez jamais une double signature aux mains d'une seule personne (cartes et codes PIN).
5. Prévoyez des étapes de contrôle suffisantes :
   - Convenez que les paiements – et surtout les paiements importants – ne seront pas seulement transmis par e-mail, mais seront aussi confirmés par un SMS, un message WhatsApp, par téléphone, etc.
   - Désignez une autre personne au sein de l'entreprise (pas le CEO) à laquelle les collaborateur-rice-s peuvent s'adresser en cas de demande confidentielle ou urgente. La personne désignée pourra alors vérifier avec le CEO si la demande est authentique. Remarque : personne en dehors de l'entreprise ne doit savoir qui est la personne désignée.

— Je suis tombé-e dans le piège. Que faire ?

- Contactez au plus vite la banque.
- Déposez une plainte auprès de la police.
- Informez le service informatique de votre entreprise si la mailbox du CEO a été piratée. Les fraudeurs ont probablement accès à de nombreuses informations grâce à cette mailbox. Les mots de passe devront être changés, par exemple.

PHISHING

— Qu'est-ce que le phishing ?

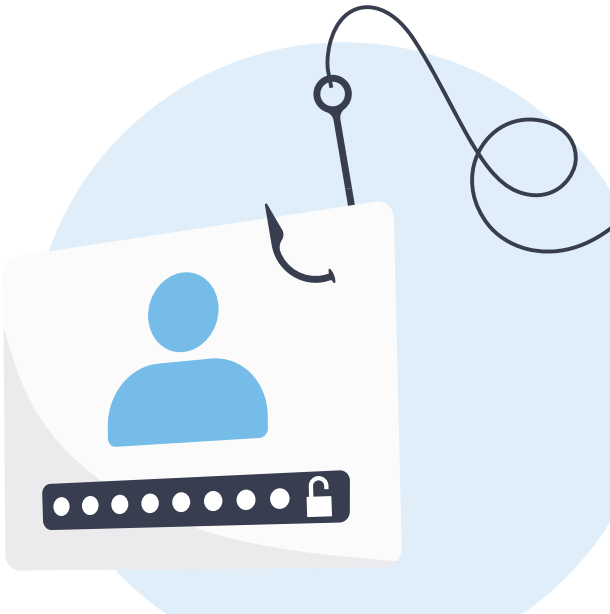
Le phishing est une technique par le biais de laquelle les escrocs tentent de pêcher vos codes personnels, qui donnent accès à votre environnement bancaire en ligne. Le contenu des messages de phishing peut varier considérablement. Il peut s'agir d'un faux message (e-mail, WhatsApp, SMS, etc.) de votre banque vous incitant à renouveler votre carte bancaire, de votre opérateur de téléphonie concernant un problème de paiement de votre abonnement, du SPF Finances vous promettant une prime, etc. Cependant, ce message contient toujours un lien vers un faux site web. Si vous cliquez dessus et entrez les coordonnées bancaires et le code secret de votre entreprise sur le faux site, vous ouvrirez aux fraudeurs l'accès aux comptes de votre entreprise.

CONSEILS POUR PROTÉGER VOTRE ENTREPRISE CONTRE LE PHISHING

- Ne communiquez jamais les codes pour l'internet banking (codes générés par le lecteur de carte) par e-mail, médias sociaux, SMS ou téléphone. Les codes bancaires en ligne de l'entreprise sont aussi secrets que le code PIN de votre propre carte bancaire !
- Ne passez jamais par un lien pour vous rendre sur le site de paiement ou l'application mobile de la banque de votre entreprise. Et retenez que la banque ne vous demandera jamais de codes via un lien.
- Tapez toujours vous-même l'adresse du site de la banque de votre entreprise dans votre navigateur. Vous pouvez également enregistrer cette adresse (URL) dans la liste des favoris de votre navigateur. Ou ouvrir vous-même l'application mobile de la banque.
- En cas de doute, il vaut mieux vous interrompre sans attendre. Si vous avez reçu un message un peu étrange et que vous ne savez pas ce qui s'est passé, choisissez la sécurité et arrêtez tout.
- Regardez le module gratuit « Surfer sans soucis » appelé « Regarde où tu vas! » sur le site safeonweb.be.

— Vous êtes malgré tout tombé-e dans le piège ?

- Contactez au plus vite la banque de votre entreprise. Grâce à des numéros spéciaux dédiés à la fraude, celle-ci peut être jointe 24 heures sur 24 et 7 jours sur 7 pour signaler une fraude en ligne. Vous trouverez un aperçu de tous les points de contact sur https:/cardstop.be/fr-be/home/quoi-bloquer/bloquer-votre-application-bancaire-ou-votre-compte-via-votre-banque.html
- Une fois que vous avez transmis les données de votre carte, prévenez Card Stop (www.cardstop.be ou 078 170 170).
- Changez vos codes.
- Déposez une plainte auprès de la police.



LA FRAUDE AU COMPTE À SÉCURITÉ RENFORCÉE

Une autre forme de fraude se développe au sein des entreprises, il s'agit de la fraude au compte à sécurité renforcée. Un-e expéditeur-rice qui semble digne de confiance (par ex. un secrétariat social, la banque, la poste, un opérateur de téléphonie, etc.) appelle l'entreprise ou l'indépendant-e pour l'avertir que des transactions bancaires suspectes sont en cours sur le compte de l'entreprise. Le dommage peut être évité si l'on agit « rapidement » et que l'on transfère les fonds sur un « compte à sécurité renforcée ». A posteriori, il s'avérera que ce « compte de sécurité » n'existait pas et le chef d'entreprise se retrouvera avec une grosse perte financière...

La fraude au compte à sécurité renforcée est généralement opérée en deux temps. Le fraudeur envoie tout d'abord un message de phishing pour obtenir accès au compte bancaire de l'entreprise ou de l'indépendant-e. Il appelle ensuite un-e collaborateur-rice de l'entreprise ou l'indépendant-e et le ou la convainc de transférer l'argent du compte vers un compte dit « à sécurité renforcée ».

— Comment cela fonctionne-t-il ?

La fraude au compte à sécurité renforcée débute souvent par un message de phishing (hameçonnage) que le cybercriminel envoie par e-mail, SMS, Whatsapp ou via les médias sociaux. Ce message contient un lien qui mène vers un site factice. Les escrocs utilisent ensuite ce site web pour récupérer des informations personnelles, comme des données de contact voire des codes permettant de se connecter aux services bancaires en ligne.

Une fois ces informations en leur possession, les escrocs peuvent entamer leurs opérations frauduleuses : ils appellent l'entreprise ou l'indépendant-e et se font passer pour un-e collaborateur-rice de la banque. Ils expliquent alors que des transactions suspectes ont été effectuées sur le compte.

Souvent aussi, ils passent l'étape de l'envoi d'un message de phishing et appellent simplement l'entreprise ou l'indépendant-e en usant de beaucoup de persuasion. Ils sont prêts à tout pour gagner la confiance de leur interlocuteur-rice.

Les escrocs proposent alors de transférer l'argent vers un compte sécurisé, le fameux « compte à sécurité renforcée ». Mais ce type de compte n'existe absolument pas. Et si le ou la collaborateur-rice de l'entreprise ou l'indépendant-e transfère effectivement de l'argent sur ce faux « compte à sécurité renforcée », l'argent se retrouvera sur le compte d'une mule financière, d'où il sera retransféré à toute vitesse pour aboutir sur le compte des cybercriminels.
Un autre scénario consiste pour le fraudeur à faire croire à la personne ciblée qu'elle confirme l'« annulation de virements frauduleux », alors même qu'elle sera justement en train de signer les virements frauduleux.

CONSEILS POUR PROTÉGER VOTRE ENTREPRISE

- Ne communiquez jamais les informations personnelles et/ou les codes bancaires de l'entreprise (numéro de compte, code PIN, code réponse) par e-mail, SMS, appel téléphonique, message sur les réseaux sociaux ou WhatsApp. Ni une banque – ni aucune autre organisation - ne vous adressera jamais une telle demande par téléphone, e-mail, SMS ou via les médias sociaux
- La banque ne vous conseillera pas non plus de transférer l'argent de l'entreprise sur le compte d'un tiers. Le compte à sécurité renforcée, ça n'existe pas !
- La banque ne vous demandera pas davantage d'installer un logiciel (AnyDesk, TeamViewer) permettant de prendre le contrôle à distance de votre ordinateur.
- Si vous avez reçu un message ou un appel bizarre et que vous doutez de son authenticité, ne prenez pas de risque et n'y donnez pas suite. Ne vous laissez pas influencer et convaincre d'agir « vite ». Vous voulez plus d'informations ? Appelez la banque vous-même. En effet, les escrocs ne peuvent pas intercepter cet appel, mais ils peuvent « usurper » un numéro de la banque et vous appeler eux-mêmes avec ce numéro.

— Vous êtes malgré tout tombé-e dans le piège ?

- Contactez au plus vite la banque de votre entreprise. Elle est joignable 24 heures sur 24, 7 jours sur 7, via des numéros spéciaux pour signaler les fraudes en ligne. Vous trouverez un aperçu de tous les points de contact sur https://cardstop.be/fr-be/home/quoi-bloquer/bloquer-votre-application-bancaire-ou-votre-compte-via-votre-banque.html
- Prévenez Card Stop (078 170 170).
- Déposez une plainte auprès de la police.

LA FRAUDE AU FAUX SUPPORT TECHNIQUE BANCAIRE

— Qu'est-ce que la fraude au faux support technique bancaire ?

Dans ce type de fraude, les entreprises sont appelées par des escrocs qui se font passer pour des collaborateurs-rices de banque. Ils/elles convainquent les entrepreneur-e-s de les laisser prendre le contrôle à distance de leur ordinateur et leur demandent leurs codes personnels. C'est ainsi que les escrocs parviennent à dérober d'importantes sommes d'argent. Ce type de fraude est en augmentation et peut entraîner des pertes financières considérables en peu de temps.

— Comment fonctionne cette fraude ?

En général, l'entrepreneur-e reçoit un appel téléphonique d'un-e prétendu-e collaborateur-rice (du service des fraudes) de sa banque l'avertissant que des transactions suspectes viennent d'être détectées sur le compte de l'entreprise. L'escroc convainc l'entrepreneur-e de l'urgence de la situation et lui donne des conseils pour éviter le pire.

Une fois la victime mise en confiance, on lui demande de transférer de l'argent sur des « comptes sécurisés » (qui n'existent pas) ou d'annuler des virements frauduleux (qui n'existent pas non plus) avec le/la prétendu-e « collaborateur-rice de banque ».

Les escrocs demandent également l'installation d'un logiciel (AnyDesk, TeamViewer...) qui permet au/à la « collaborateur-rice de banque » d'aider l'entrepreneur-e. L'escroc a ainsi le contrôle total de l'ordinateur ou du smartphone de la victime. Il/elle détermine ce que l'entrepreneur-e peut voir et ce qu'il/elle ne peut pas voir et peut donc effectuer des opérations bancaires en ligne et effectuer des virements à partir des comptes professionnels et privés de la victime au nom de l'entreprise. L'entrepreneur-e signe ces virements, pensant qu'ils vont sécuriser ses comptes ou que cela permet de les annuler.

CONSEILS POUR VOUS PROTÉGER ET PROTÉGER VOTRE ENTREPRISE

1. Si vous recevez un appel d'un-e « collaborateur-rice de banque » vous demandant d'installer un logiciel afin qu'il/elle puisse prendre le contrôle de votre ordinateur, n'exécutez pas ses instructions et mettez fin à l'appel.
2. Vous pouvez également décider, en tant qu'entreprise, que vos collaborateur-rice-s ne peuvent pas installer de logiciels.
3. Prenez les mesures nécessaires : informez vos collègues, ami-e-s ou collaborateur-rice-s afin qu'ils/elles puissent mieux se prémunir contre cette forme d'escroquerie.

— Vous êtes quand même tombé-e dans le piège ?

- Contactez au plus vite la banque de votre entreprise. Elle est joignable 24 heures sur 24, 7 jours sur 7, via des numéros spéciaux pour signaler les fraudes en ligne. Vous trouverez un aperçu de tous les points de contact sur https://cardstop.be/fr-be/home/quoi-bloquer/bloquer-votre-application-bancaire-ou-votre-compte-via-votre-banque.html
- Prévenez Card Stop (078 170 170).
- Déposez une plainte auprès de la police.

Encore quelques bonnes pratiques sur les paiements en ligne dans une entreprise :

— Bonne gestion de la double signature

La double signature est un moyen de prévenir la fraude. La personne qui appose la deuxième signature n'est pas liée à la transaction et remarquera la fraude plus facilement.

— Utilisation judicieuse des procurations sur les comptes

Chaque mandataire devrait avoir son propre accès aux comptes de l'entreprise. En effet, lorsqu'il/elle partage avec quelqu'un d'autre un accès électronique aux comptes de l'entreprise, il/elle ne partage pas seulement ses procurations mais donne également accès à ses comptes privés. Avoir son propre accès est plus sûr non seulement pour l'entreprise mais aussi pour le ou la collaborateur-rice, qui ne peut ainsi effectuer que les transactions liées à ses procurations.

POUR CONCLURE

Toute entreprise peut être victime de fraude. La fraude peut prendre de nombreuses formes, mais heureusement, de nombreuses dispositions peuvent être prises pour en préserver votre entreprise et ses collaborateur-rice-s. Il est toujours essentiel de rester vigilant-e et de prendre les mesures appropriées pour tenir les fraudeurs à l'écart.

Boulevard du Roi Albert II 19, 1210 Bruxelles

www.febelfin.be