Atradius

Les Fraudes

Les bons réflexes à adopter en cas de tentative de fraude

Nous nous trouvons actuellement face à une recrudescence des actes de fraudes visant les entreprises. Selon PWC, 47% des entreprises dans le monde ont été victime d'une fraude entre 2019-2020 et ce taux atteint les 53% en France. Comment les déceler ? Comment réagir ? Ce document vous permettra de les identifier, ainsi que de connaître les bons réflexes à adopter en cas de tentative de fraude à l'encontre de votre entreprise.

Les différentes fraudes

Il existe différents types de **fraudes externes** (le fraudeur est un individu ou une organisation extérieurs à l'entreprise). Plusieurs fraudes peuvent se manifester simultanément. Par exemple, un fraudeur peut usurper l'identité de l'un de vos collaborateurs dans le but de soutirer des données (usurpation d'identité et phishing).

Le phishing

C'est une technique utilisée par des escrocs, afin de collecter des données telles que des mots de passe, des codes d'accès, des codes PIN, des codes de carte de crédit, des numéros de comptes bancaires, ou encore diverses informations sur une entreprise (cocontractants, organisation...).

Le fraudeur va donc soit contacter la victime par téléphone, soit envoyer un message (SMS, WhatsApp...) ou un email dans le but d'obtenir des informations concrètes telles que des coordonnées bancaires. Le fraudeur agira sûrement sous couvert d'anonymat ou en donnant de fausses informations sur lui-même. Il pourra par exemple se faire passer pour un conseiller bancaire, un notaire, un avocat, **l'un de vos collaborateurs, l'un de vos clients,** une personne du département IT de **l'un de vos prestataires ou encore pour un cocontractant** afin de crédibiliser son intervention. Il est également possible, dans le cadre du phishing, que vous soyez invités à appeler un numéro surtaxé, à cliquer sur un lien ou encore à ouvrir une pièce jointe contenant un virus.

Mise en situation de phishing :

Vous recevez un appel d'un numéro masqué:

- « Bonjour, je travaille pour la banque, je vous contacte afin d'effectuer une vérification d'opération sur l'un de vos comptes. »

Vous demandez à la personne son nom ainsi que la banque pour laquelle il travaille, la personne vous répond:

- « La vérification est urgente, j'ai besoin que vous me transmettiez immédiatement votre numéro de compte ainsi que votre numéro de carte bancaire car une opération suspecte est actuellement détectée. »

ou

« Je suis de l'IT, il y a un virus informatique sur votre pc. Donnez-moi votre login, mot de passe pour que je puisse le mettre en urgence en quarantaine. »

L'usurpation d'identité

Cette fraude consiste en l'utilisation de données, propres à identifier une personne, par un individu dans le but de nuire à la réputation, de réaliser des opérations financières, des achats ou encore de commettre des actes répréhensibles au nom de cette personne.

Les usurpateurs peuvent voler des données via le piratage ou encore se faire passer pour un organisme privé ou public connu afin de vous encourager à transmettre vos données. Le fraudeur peut également usurper l'identité d'un collaborateur (ex : membre de la Direction), d'un avocat.... Le fraudeur peut également usurper l'identité de votre entreprise auprès de particuliers ou d'autres entreprises afin de leur proposer de faux services et ainsi leur soutirer de l'argent ou des données.

Mise en situation :

Vous recevez un mail expédié par l'adresse mail suivante « francisK@gmail.com » signé de votre supérieur hiérarchique vous demandant de façon totalement confidentielle d'effectuer un paiement sur un compte à l'étranger afin de conclure un contrat gardé secret :

« Bonjour Henri,
Je vous contacte car je vous ai sélectionné au sein de l'entreprise pour effectuer un paiement urgent à mon nom permettant de conclure un contrat gardé secret. Je vous demande de faire preuve de discrétion de par la nature confidentielle de l'opération.
Pouvez-vous me contacter au plus vite ?
Merci. »

« Bonjour Ingrid,
Êtes-vous disponible? Il y a un paiement urgent que vous devez effectuer en mon nom. Faites-moi savoir si vous pouvez le gérer maintenant afin que je puisse vous envoyer les détails.
Cordialement,
Nom prénom »

« Monsieur,
Je suis M xxxx de la Sté X du bureau de Brest, je vous propose cette prestation, si vous effectuez ce jour un virement sur le compte en banque RIB XXXX. »

Fabrication et usage de faux documents

Cette fraude consiste en la fabrication d'un faux document, en la modification frauduleuse d'un document existant ou encore en l'imitation d'une signature. Il s'agit d'un faux document qui est utilisé dans le but d'obtenir un droit et ce même si le faux document n'a pas été conçu par le fraudeur.

La fabrication et l'usage de faux peuvent se présenter dans certains cas particuliers. Le fraudeur peut créer et/ou utiliser un faux document dans le but de vous tromper, ou de tromper un particulier, une banque, un factor, vos clients et d'obtenir des données, de l'argent, des facilités bancaires, des marchandises, des services.

Les fraudeurs peuvent falsifier de multiples documents et ainsi utiliser **par exemple** :

- Un faux contrat
- Une fausse facture
- Une fausse commande
- Faux comptes sociaux

Mises en situation :

Les fraudeurs prennent contact avec des particuliers afin de leur vendre des services qu'en réalité votre société ne propose pas (ex : prêt, ...).
Les fraudeurs vont crédibiliser leur offre grâce aux faux documents (faux contrats, faux RIB, faux courriels) et, ainsi soutirer de l'argent aux victimes.

La fraude au factor

La fraude au factor se déroule en deux étapes, une étape de repérage puis une phase de passage à l'action pour le/les fraudeurs.

La période de repérage va permettre aux escrocs de récolter un maximum d'informations et de données sur l'entreprise (organigramme, base de données des clients, signature du dirigeant, signature du directeur financier). Les fraudeurs vont, afin de recueillir ces informations, contacter directement l'entreprise et se faire passer pour une agence de marketing, par exemple. Le fraudeur va également contacter les clients de la future victime afin de récupérer des doubles de factures pour pouvoir utiliser les mentions y étant présentes ainsi que l'en-tête du document. Les fraudeurs vont, enfin, se procurer une adresse mail dont le nom de domaine se rapproche de celui des adresses mails de la victime.

Une fois la phase de repérage terminée, les fraudeurs passent à l'action, généralement durant les périodes de congés ou lors d'un pic d'activité de l'entreprise. Les escrocs vont alors envoyer un faux courrier, néanmoins très similaire aux originaux, aux clients de l'entreprise afin de leur signaler que l'entreprise a mis en place un partenariat avec une société d'affacturage et qu'il convient donc désormais de régler leurs factures directement au factor. Les escrocs transmettent également un RIB d'un compte leur appartenant afin de recevoir les fonds.

Fraude au crédit

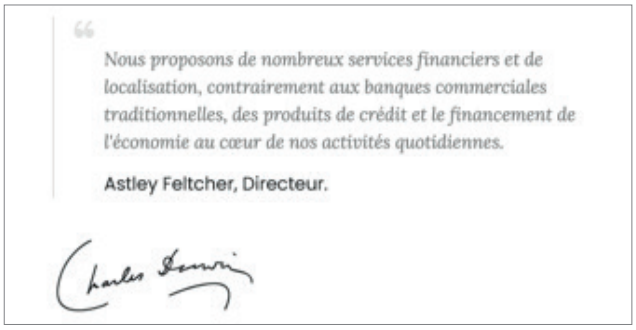
Cette technique de fraude consiste à attirer une victime par le biais de publicité pour un crédit afin que celle-ci contracte un faux crédit à des conditions avantageuses.

La victime de la fraude au crédit est contactée par des escrocs usurpant l'identité d'un tiers et proposant des crédits au nom de ce tiers. Cet acte peut être crédibilisé par la fabrication d'un faux contrat de prêt par exemple. Une fois l'argent (faux frais de souscription, d'assurance emprunteur) soutiré à la victime, le fraudeur disparaît.

Sociétés clonées

Cette fraude consiste dans l'usurpation de l'identité d'une société (en utilisant le nom de celle-ci, voire d'autres informations de celle-ci) afin de faire croire aux victimes qu'elle est en mesure d'octroyer un crédit ou d'autres types de produits/services financiers.

Certains fraudeurs reproduisent à l'identique un site internet d'entreprise déjà existant, voire créent leur propre site afin d'attirer les personnes. Voici quelques **exemples** des incohérences que l'on peut trouver sur ces sites internet frauduleux :



Signature au nom de Charles Darwin alors que le Directeur se nomme Astley Feltcher

Le logo Airbus présent sur ce site n'est pas celui d'Airbus.

La fraude au fournisseur

L'escroc usurpe l'identité d'un fournisseur d'une entreprise et contacte le client afin de lui faire croire que ses coordonnées bancaires ont changé. Le fraudeur transmet ses propres coordonnées bancaires afin de recevoir le paiement de l'entreprise initialement destiné au fournisseur.

Le fraudeur aura préalablement récolté quantité d'informations et de données sur le fournisseur afin d'usurper au mieux l'identité de celui-ci. Les escrocs peuvent également créer une adresse mail plus ou moins similaire à celle du fournisseur (ex : société-X@consultant.com, société-X@consultant.fr) afin de donner plus de crédibilité à leur acte.

Mise en situation :

Une personne va se faire passer pour un client et vous demander de lui adresser votre dernière facture car elle ne l'a pas reçue. Vous lui transmettez. Le fraudeur va ensuite copier vos factures tout en modifiant vos coordonnées bancaires pour détourner le paiement de vos factures sur son compte en adressant les fausses factures de l'entreprise à plusieurs de vos clients en signalant un changement de RIB.

Il est donc nécessaire de rester vigilant quant aux vols de factures, d'informations et de données.

Vous pouvez également être victime d'une telle fraude dans l'hypothèse où l'un de vos fournisseurs verrait son identité usurpée.

« Bonjour, je travaille pour votre fournisseur XXX, nous vous signalons que nous changeons d'établissement bancaire. Nous vous transmettons donc notre nouveau RIB sur lequel effectuer vos paiements. »

La fraude au technicien

Dans le cadre de cette fraude, l'escroc se fait passer pour un technicien bancaire ou du service informatique. Il prétexte un dysfonctionnement ou encore des « tests » dans le but de récupérer des codes d'accès et de validation bancaires afin d'effectuer des paiements à son profit ou encore des codes d'accès aux ordinateurs.

Mise en situation :

« Bonjour, notre SSII propose de nouveaux logiciels qui vont faciliter votre travail au quotidien. Réponse du collaborateur : Nous sommes déjà en phase d'installation d'un nouveau logiciel. Quel est son nom ?

Réponse du collaborateur : XYZ. ... »

Quelques jours après, un nouvel appel a lieu vers un

autre collaborateur. « Bonjour, je travaille au service informatique sur le projet XYZ, j'ai besoin de vos codes d'accès pour tester le nouveau logiciel, XYZ. »

Autres fraudes

Boiler Room

Il s'agit d'une fraude au cours de laquelle l'escroc contacte un investisseur, sans y avoir été invité, afin de lui proposer une opération censée être financièrement intéressante. La victime recevra alors, en contrepartie de son apport, des produits financiers sans valeur.

Recovery Room

La fraude dite Recovery Room vise uniquement les investisseurs ayant déjà été victimes d'une arnaque. Les fraudeurs prennent contact avec la victime afin de lui proposer de l'aide en vue de récupérer les sommes qu'elle a précédemment perdues en raison d'une arnaque moyennant le versement d'une somme d'argent (double fraude).

Le vol d'informations

Le vol d'informations est préalable à toute fraude (factures, base de données des clients, numéros de comptes bancaires, signatures, organigramme...).

Les fraudeurs utilisent divers moyens pour parvenir à voler des informations et des données :

- Intrusion dans le système d'information de l'entreprise
- Usurpation d'identité (comptable, commissaire aux comptes, inspecteur des impôts, banque, clients...)

Pour vous protéger contre le vol de données :

- Méfiez-vous de toute personne qui cherche à obtenir des factures ou des informations.
- Vérifiez l'identité de l'interlocuteur en le contactant pour être sûr de ses coordonnées.
- Ne répondez pas au mail en cas de doute, contactez votre interlocuteur habituel directement par téléphone.
- N'utilisez pas le numéro de téléphone indiqué dans le mail, passez par le standard figurant dans les Pages Jaunes.
- Si un inconnu douteux vous appelle, prétextez être occupé, prenez ses coordonnées et vérifiez-les.
- Vérifiez les adresses mails de vos interlocuteurs.

Par exemple : Imaginons que l'adresse de votre interlocuteur habituel soit « jean.piano@clavier-piano.com ».
Il est possible que vous receviez des mails des adresses frauduleuses suivantes :
« jean.piano@piano.com » (nom de domaine différent)
« jean.piano@clavierpiano.com » (nom de domaine proche de l'original, un seul caractère diffère)

Prévenir ces fraudes

Ainsi, afin de prévenir ces fraudes, il est important de sécuriser au maximum les données personnelles :

- Choisir un mot de passe sécurisé et le mettre à jour
- Ne jamais partager vos mots de passe
- N'inscrivez pas votre adresse mail principale sur un site internet dont vous n'êtes pas certain de la fiabilité
- Détruisez tout document contenant des informations confidentielles avant de le jeter
- Pensez à verrouiller votre ordinateur lorsque vous quittez votre poste de travail

L'objectif est d'éviter que vous ne soyez victime d'une fraude, mais également d'éviter qu'un fraudeur ne duplique vos documents ou ne puisse contacter vos clients.

La prévention est la première étape dans la lutte contre les fraudes et nécessite de faire preuve de vigilance au quotidien que ce soit au travail ou en dehors.

Détecter la fraude et Réagir

Si vous soupçonnez une fraude (appel, mail, document douteux...) :
Si la communication se fait par messagerie (mail, whatsapp, SMS...) :

- Vérifier le numéro d'envoi ou l'adresse mail utilisée (l'adresse mail peut révéler la fraude).
- Analyser le message en profondeur afin de déceler des fraudes (fautes d'orthographe, syntaxe).
- Pour vérifier si l'identité d'un collaborateur a été usurpée, vous pouvez analyser la façon dont est rédigé le message et le comparer aux autres mails reçus de ce collaborateur (tutoiement ou vouvoiement habituel entre vous, style rédactionnel, signature en fin de mail...).
- N'ouvrez pas les pièces jointes et ne cliquez sur aucun lien (vérifiez les préalablement en passant la souris dessus).

Dans le cas où vous recevez un appel dont vous soupçonnez le caractère frauduleux :

- Ne dévoilez aucune information demandée par l'interlocuteur.
- Demandez à la personne de s'identifier.

En cas de doute sur un site internet, il est nécessaire d'analyser la véracité des éléments y figurant afin de déceler une potentielle fraude.

Atradius

159, rue Anatole France
CS50118
92596 Levallois Perret Cedex
Tel : +33 (1) 41 05 84 84
info.fr@atradius.com
www.atradius.fr