Sécurité, Banques et Entreprises

Prévention des risques et fraudes

ARKEA
BANQUE ENTREPRISES ET INSTITUTIONNELS

Une filiale du Crédit Mutuel Arkéa

Contexte

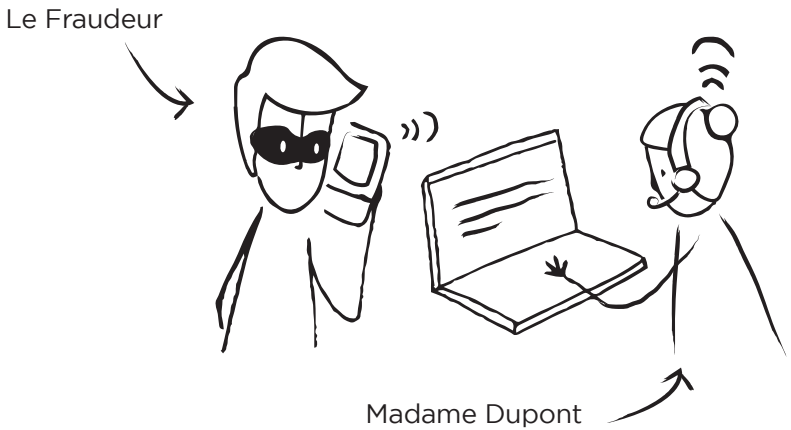
Les moyens modernes de communication et les systèmes informatiques actuels des entreprises ont fait naître de nouveaux modes de fraudes : escroqueries, abus de confiance, détournement d'actifs, usurpation d'identité... En 2020, plus de 7 entreprises sur 10 ont subit au moins une tentative de fraude.

Les fraudeurs usent d'artifices de plus en plus sophistiqués pour réunir les informations qui seront utilisées dans leurs scenarii. Le plus souvent, leur but est de provoquer un virement frauduleux à destination de l'international.

Les banques, premières entreprises visées par ce type de fraudes, ont pu constater un report important de ces tentatives vers les entreprises. Dans ce contexte, Arkéa Banque Entreprises et Institutionnels sensibilise et informe ses clients à travers la description des scenarii les plus employés par les fraudeurs et de quelques moyens pour limiter les risques d'exposition à celles-ci.

AVERTISSEMENT: Le présent document est un document établi uniquement à titre d'information et de sensibilisation aux risques de fraude. Ce document ne prétend en aucun cas à l'exhaustivité. Les scenarii décrits dans ce document ne constituent pas l'ensemble des risques auxquels sont exposées les entreprises. Les méthodes et moyens de prévention des risques présentés dans ce document (i) ne suffisent pas à eux seuls à une prévention efficace de l'ensemble des risques, (ii) ne représentent pas l'ensemble des moyens pouvant être mis en place et, (iii) en tout état de cause ne remplacent pas les procédures de contrôle et de sensibilisation que chaque entreprise se doit de développer en interne. Chaque société reste responsable de l'élaboration de sa propre cartographie des risques et d'identification des risques de fraude propres à son activité, ainsi que de la mise en place de ses procédures de prévention des risques de fraude.

Sommaire



La fraude au Président

Le fraudeur usurpe l'identité d'un des dirigeants de l'entreprise pour obtenir d'un collaborateur qu'il émette un virement urgent et confidentiel à destination de l'étranger. Dans certains cas, si la tentative échoue, le fraudeur pourra retenter sa chance en se faisant passer pour la police. La demande peut être formulée par téléphone ou par e-mail en falsifiant l'adresse de messagerie.

Madame Dupont en réfère à son responsable hiérarchique, Monsieur Leroy. Celui-ci s'assure que la transaction était frauduleuse auprès de sa direction et ne valide pas l'opération. Il prévient les autorités de la tentative de fraude.

Ce qui doit vous alerter :

- L'interlocuteur fait preuve d'autorité, d'assurance, de flatterie et/ou d'intimidation.
- Le virement demandé est inhabituel et à destination de l'étranger.
- La demande est urgente et intervient tardivement dans la journée ou à la veille d'un jour de congés.
- La demande de déroger aux procédures en place dans l'entreprise.

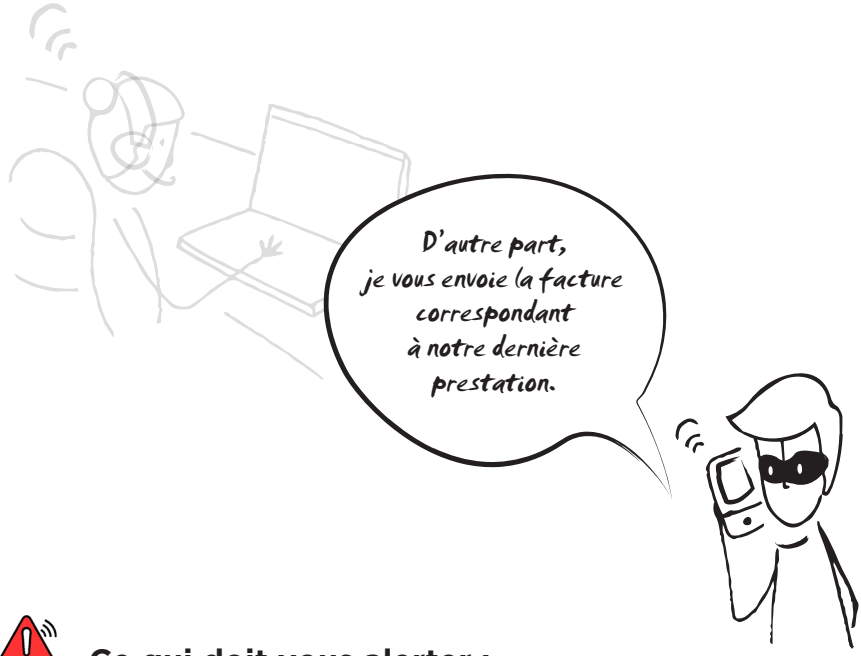
Quelques conseils

- Informez vos collaborateurs du risque de fraude.
- Sécurisez vos procédures d'ordre de virement en séparant les pouvoirs de rédaction d'ordres et de validation.
- Facilitez les échanges avec la hiérarchie.
- Demandez toujours confirmation de l'ordre reçu.

La fraude aux coordonnées bancaires

Le fraudeur simule le changement de coordonnées bancaires d'un client ou d'un fournisseur habituel de votre entreprise. Par e-mail, fax ou téléphone, il communique -avec toutes les habitudes graphiques habituelles de la société- un nouvel IBAN pour effectuer les paiements courants.

* Le nouveau destinataire des fonds peut parfois être une fausse société d'affacturage.



Ce qui doit vous alerter :

- Le demandeur n'est pas l'interlocuteur habituel de la société.
- Les coordonnées bancaires fournies peuvent être à l'étranger alors que le fournisseur n'y est pas domicilié.
- Le numéro de téléphone, de fax ou l'adresse e-mail ne correspondent pas avec les coordonnées habituelles de la société.
- L'éventuelle facture a un objet peu explicite.

Quelques conseils

- Informez vos collaborateurs du risque de fraude.
- Demandez toujours confirmation à votre interlocuteur habituel chez votre fournisseur du changement réel de coordonnées bancaires.
- Vérifiez la réalité de la prestation facturée auprès du responsable de la relation avec le fournisseur.

La Fraude au faux technicien

Le fraudeur usurpe l'identité d'un technicien informatique (de la banque par exemple) pour effectuer de faux tests dans le but de soutirer des identifiants de connexion ou provoquer des virements frauduleux. Il peut également procéder à l'installation de logiciels malveillants.

Scénario alternatif :

Le fraudeur se fait communiquer les identifiants de connexion et les mots de passe par son interlocuteur. Il a ensuite possibilité de réaliser lui-même les opérations.

Ce qui doit vous alerter :

- Vous n'avez pas sollicité d'aide informatique.
- L'interlocuteur demande de prendre la main sur votre poste.
- Un technicien n'envoie jamais de correctif via un lien dans un e-mail.

Quelques conseils

- Informez vos collaborateurs du risque de fraude.
- Demandez confirmation à votre chargé de clientèle que cette opération informatique est bien réelle.
- Ne communiquez jamais vos mots de passe ni vos identifiants de connexion.

Les autres types de fraudes

Les nouvelles technologies ouvrent de nouvelles possibilités de fraudes de plus en plus difficiles à détecter.

Mail-phishing

Vous recevez un e-mail, dans lequel il vous est demandé de « mettre à jour » ou de « confirmer suite à un incident technique » des données, notamment bancaires. Cette demande peut transiter par une invitation à se connecter en ligne par le biais d'un lien hypertexte sur un site falsifié ou un formulaire de saisie copie « conforme » du site original.

Virements SEPA

Sous le prétexte d'une mise à jour du paramétrage des nouveaux protocoles européens, un fraudeur se faisant passer pour un informaticien parvient à vous convaincre de vous connectersur un site dédié dont la page d'accueil affiche le logo de la société ciblée. Cette opération permet de prendre le contrôle de l'ordinateur à distance et d'émettre des virements.

Malware, spyware, ransomware

Un logiciel malveillant, s'installe à l'insu de l'utilisateur sur un ordinateur non protégé (ou mal protégé), lors de l'ouverture d'un e-mail frauduleux ou par téléchargement lors de la visite d'un site web. Ce virus permet au fraudeur d'avoir connaissance de (presque) tout ce qui se passe sur l'ordinateur contaminé et de prendre en otage les données dans le cas d'un ransomware.

Ces types de fraudes constituent un danger croissant car la qualité et la précision de ces contenus tendent à s'améliorer significativement : moins de fautes d'orthographe, une syntaxe qui progresse, des arnaques plus pertinentes, une imitation de la communication des sociétés de plus en plus crédible.

Que faire en cas de tentative de fraude ?

- Demander le blocage des fonds le plus vite possible auprès de votre banque.
- Déposer plainte auprès de la police locale.
- Aviser par téléphone la division économique et financière du Service Régional de Police Judiciaire et déposer plainte auprès de ce service. Le SRPJ s'organisera pour contacter la police locale en cas de virement à l'étranger afin de faciliter le gel des fonds et l'identification du titulaire du compte destinataire.
- Même en cas de tentative non réussie : relever les numéros et heures d'appel du fraudeur, garder les e-mails frauduleux, conserver les enregistrements des appels s'ils existent, demander l'extraction de la source (en-tête) de ces e-mails, déposer plainte directement au SRPJ.

Les 8 pratiques simples de la sécurité de vos opérations

En cas de contact téléphonique ou par e-mail par une personne que vous ne connaissez pas mais se présentant comme étant un collaborateur, un représentant (avocat) ou un fournisseur de votre société et/ou en cas de doute sur son origine :

- Vérifiez l'identité de votre interlocuteur en vérifiant son authenticité auprès de vos interlocuteurs habituels.
- Utilisez les coordonnées habituelles de votre répertoire (e-mail, fax, téléphone).
- Ne cliquez pas sur les liens internet contenus dans un courriel douteux.
- Vérifiez que vous êtes bien sur un site sécurisé « https ».
- Ne divulguez jamais vos identifiants ou vos mots de passe. Un technicien informatique de votre banque, des services de la direction générale des finances ou de tout autre organisme officiel n'aura jamais besoin de demander un mot de passe par courriel ou par téléphone.
- Ne communiquez pas les noms et coordonnées des collaborateurs ayant déposé leurs pouvoirs et signatures.
- Ne transmettez pas de données sensibles (solde de compte, mise à jour de données administratives, vérification des moyens de paiements, déblocage de carte).
- Au moindre doute, contactez votre interlocuteur habituel au sein d'Arkéa Banque Entreprises et Institutionnels.

ARKEA
BANQUE
ENTREPRISES ET
INSTITUTIONNELS

Améliorons ensemble notre sécurité en adoptant les bonnes pratiques !

Juillet 2021 - Quinze Mille