Recrudescence de fraudes – fatalité, phénomène de société ou nouveau risque pour le trésorier?

On a constaté ces derniers mois une augmentation inquiétante du nombre de tentatives de fraudes dont la célèbre « fraude au président ». Le phishing cible les grands groupes ainsi que les PME's, et plus spécifiquement les départements financiers. Qu'est-ce qui peut expliquer ces arnaques en tout genre ; comment les combattre efficacement ; état des lieux de la situation, sont les questions auxquelles nous tenterons de répondre. Un trésorier averti en valant deux, soyons sur nos gardes.

Pourquoi frauder plus aujourd'hui qu'hier?

Il est délicat d'oser prétendre qu'on fraude plus aujourd'hui qu'hier. Cependant, l'actualité semble nous l'indiquer. Pourquoi devons-nous faire face à cette menace nouvelle, alors ? Le contexte économique difficile, la crise financière globale et les traumatismes laissés depuis expliquent cette résurgence des fraudes. Le terreau est idéal pour générer ce type de tentatives. L'émergence de nouveaux moyens de paiement ouvre par ailleurs des brèches nouvelles, à tout le moins au début, des zones d'insécurité, d'ignorance et de failles possibles. Il n'en faut pas moins pour les petits génies informaticiens pour s'y engouffrer lorsque l'occasion se présente. Enfin ? Comme toujours hélas, le succès d'une fraude en appelle de nombreuses autres et la créativité n'est pas toujours affectée à la bonne cause, loin s'en faut. C'est donc ce contexte particulier et cette difficulté économique qui expliquent une situation nouvelle de risques accrus. Il faut en tenir compte et redoubler de vigilance. C'est souvent dans l'adversité que l'on peut se tester, s'améliorer ainsi que ses processus de contrôles internes et « vendre » des projets de sécurité, notamment informatique. Brandissez le spectre du risque de fraude et vous serez entendu de tout le « *C –level* », qui vous allouera des budgets pour la prévention.

L'habit ne fait pas le moine

La France et d'autres pays ont connu récemment une recrudescence de tentatives de fraudes dites « fraudes au président ». Ce type de fraude est une variante très particulière de *phishing* qui cible grands et petits groupes, sans distinction, et en particulier leurs départements financiers. Les fraudeurs multiplient les tentatives pour augmenter leurs chances de parvenir à chopper une victime. Statistiquement, cela fonctionne bien et tôt ou tard, une société plus négligente se fera prendre. Les services de police judiciaire des différents états de l'Union montrent que des millions d'euros ont été perdu. Ces techniques nécessitent patience, conviction, talent d'acteurs, génie informatique, recherches préalables

approfondies et une dose importante de culot. L'ensemble de ces éléments combinés pourrait faire des dégâts importants.

«*Security is the biggest challenge for businesses in adopting mobile technologies, cloud and the internet of things. Around 23% of companies surveyed said they have suffered a security breach in the past 12 months*" (source "The technology Industry Outlook Survey 2015" AFP – http://www.afponline.org/fraud/)

Ce type d'escroc est spécialisé (cas de la fraude au président) dans l'ingénierie sociale. Il passe au crible l'environnement de l'entreprise visée et son intimité, ainsi que celle de ses membres. Cela passe par la communication interne, les statuts officiels, les comptes bancaires, l'organigramme, les PV's d'Assemblées Générales, ou compte-rendu de comités divers. Bref, tout ce qui peut servir est collectionné et compilé pour mettre en place la souricière. Même si statistiquement, seules 1% des fraudes fonctionnaient, cela suffirait à pousser à l'institutionnaliser. Le succès et la pratique renforcera la crédibilité des scénarii.

L'idée est de capter la philosophie de l'entreprise, son langage et ses codes pour crédibiliser la fraude. L'idée de cette fraude au demeurant sommaire et idiote de simplicité réside dans la réussite à se faire passer pour le CEO d'une entreprise pour convaincre des employés d'agir à l'encontre des bonnes pratiques ou polices internes, à titre exceptionnel. Ils peuvent imiter voix, signature, mimiques, produire des faisceaux de présomption troublants qui donneront le confort à la victime (e.g. le numéro de portable du CEO s'affiche sur le display de l'employé, la voix du président est imitée à la perfection, il vous dit être là où on sait officiellement qu'il est, pour troubler l'interlocuteur, etc..). Le but est de faire valider un transfert de fonds urgent pour un bénéficiaire inconnu, en sachant que le CEO couvrira l'opération, à court terme avec la documentation requise. La base réside dans une pression psychologique venant du lien hiérarchique. Et hélas, parfois cela fonctionne et certains tombent dans le panneau.

"*3/4th of technology executives expect their company to spend 1 to 5 % of their revenue on IT security over the next 12 months*" " (source "The technology Industry Outlook Survey 2015" AFP – http://www.afponline.org/fraud/)

Comment débusquer les « faux présidents » et leur gang, comme dans « *Point break* »?

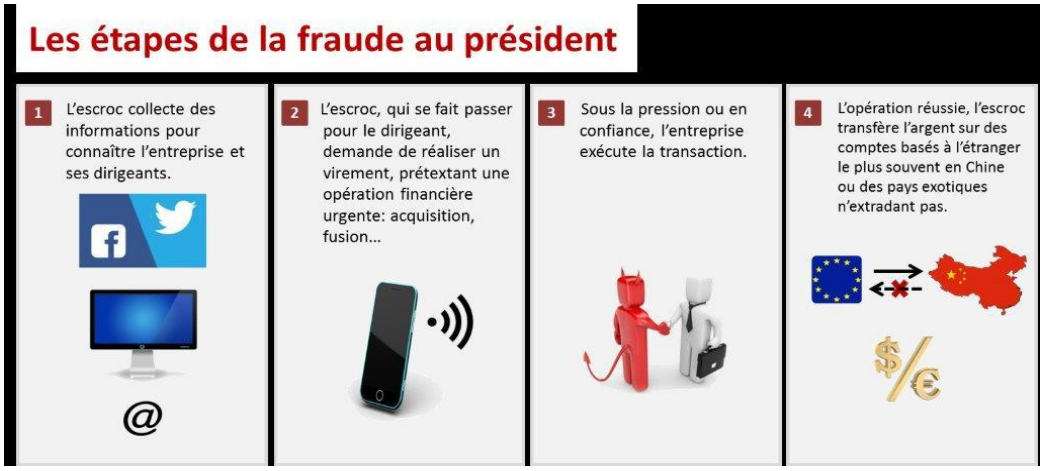
Afin de prévenir de telles attaques vicieuses, il est recommandables de (1) faire régulièrement suivre des formations de sensibilisation à la sécurité à son personnel et de s'assurer qu'ils connaissent ce type d'attaque. (2) L'information permet la prévention dans bien des cas. Il faut s'assurer que (3) le service comptable applique les procédures de vérification concernant les paiements, à la lettre et sans exceptions, surtout pour les paiements internationaux. On devrait même (4) insérer une clause dans les polices internes garantissant qu'un employé qui refuserait d'exécuter un ordre, fut-ce-t-il donné par le CEO/CFO, contraire aux procédures internes, ne pourra être en aucun cas licencié. Certains

CEO's délivrent des messages en ce sens et insistent pour que leur personnel n'accepte pas des instructions contraires aux règles et procédures internes. Cela peut rassurer le comptable et lui éviter la crise de panique, souvent mauvaise conseillère (et c'est bien là le but recherché par le fraudeur). Il est conseillé (5) de vérifier les signatures électroniques des virements bancaires et augmenter le niveau de sécurité et de contrôle autour de ces paiements. On n'est jamais trop prudent en matière de risques. Il n'est (6) pas inutile de vérifier les adresses courriels des interlocuteurs d'origine et les adresses « *reply-to* ». En cas de doutes ou d'e-mails suspects, l'employé devrait (7) contacter le département sécurité informatique de l'entreprise et transférer ces courriels douteux à qui de droit au département IT.

"*Payment fraud evolves as rapidly as payment sector is developing. As new payment methods are being introduced there are increasing criminal attempts. 62% of respondents reported their organizations were targets of payment frauds in 2014*". (source "The technology Industry Outlook Survey 2015" AFP – http://www.afponline.org/fraud/)

Lorsque le mal est fait, les conseils sont différents : tentez d'intercepter et de bloquer le paiement bancaire, si cela est encore possible, déposer plainte auprès de la police judiciaire locale, contacter votre département de sécurité informatique et votre auditeur interne. En matière de fraude, le facteur temps est capital. Le laisser passer est un risque énorme car il joue contre nous. Il faut traquer les comportements atypiques et les exceptions. Les procédures « sans papier » (« *paperless processes* ») doivent être privilégiées.

Qui se cache à l'autre bout du fil et une question-clé. Par exemple, il a été entendu : « - *Je suis votre CEO. Je vous fais confiance pour cette opération urgente et délicate. Gardez le secret jusqu'à l'annonce de l'opération d'acquisition, il y va de l'intérêt de l'entreprise*.(…) ». Usurper l'identité de quelqu'un n'est donc pas si difficile que cela n'y parait. L'escroc utilisera au mieux le ressort de la position de subordination hiérarchique pour asseoir sa tentative de fraude. Il est souvent un véritable manipulateur aguerri et persuasif (e.g. « - *c'est un ordre et je vous le donne (…) Cessez de discuter, on perd du temps (…) vous voulez perdre votre job ? (…)* »).



Scenario type

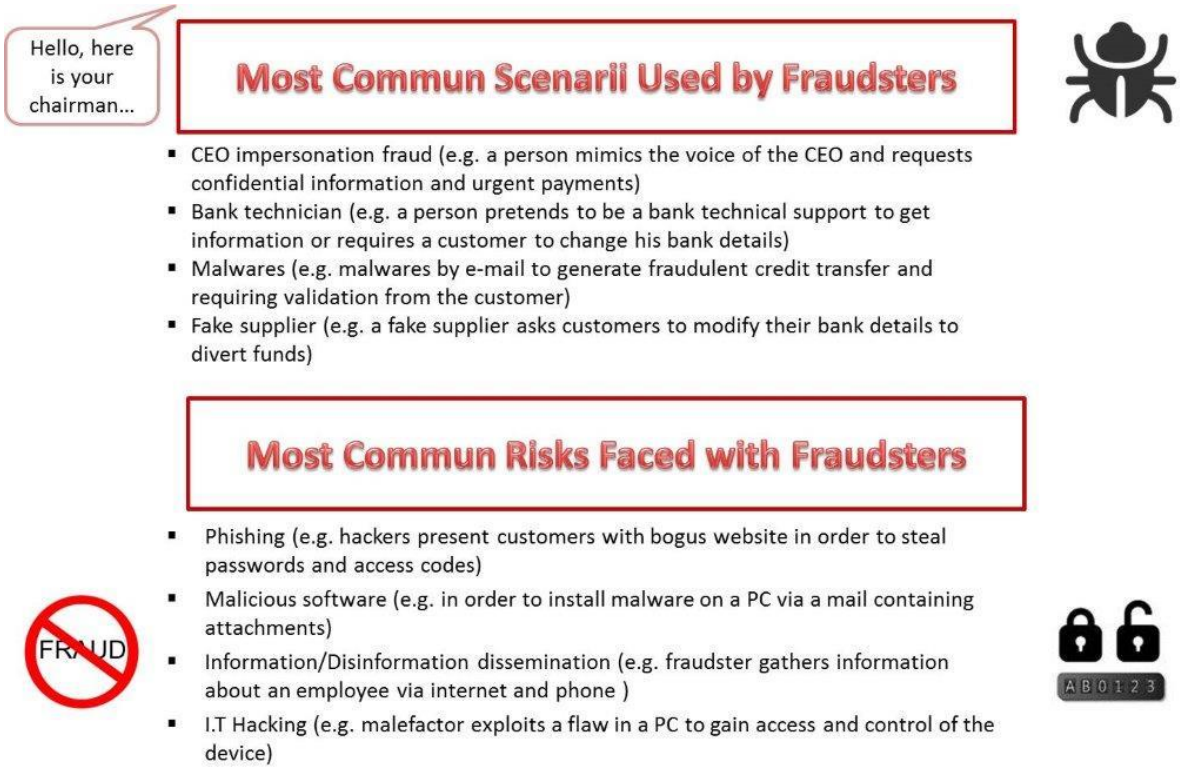
1. Prise de contact ;
2. Demande exceptionnelle et urgente ;
3. Force de persuasion ;
4. Ordre de virement manuel ;
5. Nouvelle tentative

Pour éviter ce risque, il faut s'en tenir aux procédures établies et résister à la tentation et à la pression. Faire preuve d'esprit critique, même si la pression et l'angoisse de l'appel du CEO pet vous la faire perdre. La pression est mauvaise conseillère, ne l'oubliez jamais ! Comme le disait très justement Bruno Lussato : « *l'amélioration des techniques de fraude est beaucoup moins coûteuse, en temps et en argent, que celle des moyens de prévention* ». Ce n'est donc pas parce que la prévention coûte cher qu'il faille s'en affranchir, au prétexte du coût et du principe « *cela n'arrive qu'aux autres* ».

Ecoutez plutôt votre intuition et si la demande parait suspecte, il y a fort à parier qu'elle est illégitime. Vérifier la légitimité d'une demande, en effectuant un contre-appel vers un numéro référencé n'a jamais fait de mal. Adoptez les bons réflexes : limiter la diffusion d'informations sur les réseaux sociaux, elle peut vous desservir tôt ou tard. Mettez en place des procédures sécurisées basées sur le principe de quatre yeux et double contrôles, limitez les accès, sensibiliser votre collaborateurs et restez vigilent à toute demande inhabituelle. Les fraudes surviennent souvent en périodes de congé ou de sous-staffing.

Les techniques sont multi-canaux et tentent la pénétration par n'importe quelle porte d'accès (téléphone, fax, messagerie mail, web) afin de tromper les collaborateurs qui croient naïvement rendre service à leur supérieur hiérarchique en été zélé. Parmi les cibles mentionnées par les journaux français (à vérifier) on a parlé dans la presse de Michelin, Vallourec et d'Intermarché, notamment. Le syndicat des patrons français (i.e. MEDEF) a

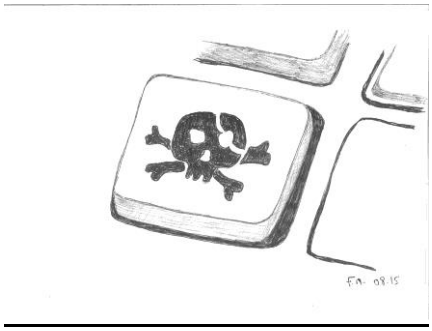
d'ailleurs initié un échange d'informations sur les fraudes avérées afin d'en partager les spécificités et s'en prémunir. Certains évoquent le chiffre d'une fraude qui a atteint à elle seule EUR 23 million sur un seul paiement. On a pu également lire que les fraudeurs seraient basés en Israël ou en Chine, très souvent, ou dans des pays qui n'extradent pas. Un nom a même été cité celui de Gilbert Chikil, pionnier français de l'arnaque et de l'escroquerie corporate. Cette fraude désormais classique est devenue la hantise des CEO's (e.g. « *Bonjour, c'est votre Président au téléphone, pourriez-vous exécuter un paiement confidentiel et urgent pour moi ? … Je compte sur vous ! …* ») en France, pays très attaqué par ce type d'escroquerie. Le caractère de bénédictin des fraudeurs et leur patience, alliée à leur ingéniosité permettent parfois atteindre leur cible. L'ensemble des artifices est tel qu'il peut donner l'illusion que la demande est bien réelle. Vous êtes honoré de vous voir confier cette mission stratégique et confidentielle au point d'en oublier l'élémentaire prudence.



<u>Se prémunir contre ce type de fraude</u>

Les cyber-attaques, en général, et les fraudes plus classiques, en particulier, requièrent un renforcement des procédures, des polices et des contrôles internes. Les services informatiques s'attèlent ces derniers mois à rappeler aux utilisateurs des ressources informatiques les mesures de sécurité fondamentales susceptibles de les protéger contre ce type d'attaques pernicieuses. Le hameçonnage/harponnage est une technique très répandue et dont les pirates abusent. Aux dires de *Trend Micro Research Paper*, 91% des attaques ciblées mettent en œuvre des courriels d'harponnage, ce qui porte à croire que cette méthode est celle privilégiée par les cyber-pirates pour s'infiltrer dans les réseaux afin d'y dérober de l'information ou les pirater de l'intérieur. Vous êtes ainsi invité à cliquer sur

un cyber-courriels envoyé à des millions de gens, victimes potentielles, afin de les inciter à cliquer sur un lien associé à un site malveillant, à ouvrir une pièce jointe infectée ou contaminée ou pour simplement obtenir des informations intéressantes pour une attaque ultérieure. Ces messages donnent l'impression de venir d'une source digne de confiance telle votre banque ou entreprise de transport ou même d'une connaissance ou pire un collègue. Les messages peuvent être personnalisés et l'on parle alors d' « harponnage », en lisant des comptes LinkedIn ou Facebook de victimes innocentes. L'apparente véracité et crédibilité des messages troublent plus d'un destinataire. Et si tel est le cas, le piège est tendu. Il semble que 66% des cyber-attaques réussies l'aient été par des harponnages. Même si les techniques de défense sont toujours plus sophistiquées, à l'instar du dopage, le fraudeur a souvent une longueur d'avance sur le gendarme. Il faut donc toujours être méfiant à l'égard de ce qui n'a pas été sollicité. Il faut se méfier comme de la peste de demande d'informations complémentaires à annexer. La destination URL du lien est souvent différente de celle indiquée dans le courriel, c'est le premier signe d'harponnage. C'est la pêche au « gros » et ils font feu de tout bois dans l'espoir d'en cueillir l'un ou l'autre, trop peu prudents. Le pire est que ça marche très bien. Par exemple, il existe des procédures obligatoires pour confirmer des numéros de comptes bancaires de fournisseurs. Les opérations de fusion et acquisitions, par leur caractère exceptionnel, sont des pièges parfaits pour qui sait y faire. On n'est jamais trop précautionneux dans ce genre de situation. Un trésorier averti en vaut deux, n'est-ce pas ? Il existe des mesures simples et efficaces : utiliser des instructions standards pour les paiements (i.e. *Standard Settlement Instructions*), avoir une visibilité complète sur tous les comptes bancaires via un système efficient, utiliser la signature digitale et même y ajouter des clés comme le 3SKey de SWIFT par exemple, améliorer la sécurité des données et du « cloud » avec de solides « SLA's » (*Service Level Agreements*) signés par vos fournisseurs, par des tests réguliers d'intrusion, en renforçant considérablement les mots de passe et leur rotation obligatoire (même si cela gêne l'utilisateurs lambda), en supprimant immédiatement les pouvoirs de signature des personnes licenciées ou quittant la société, en élaborant des polices claires, exhaustives et communiquées à tous, en organisant des ateliers de prévention, etc… Comme le disait le poète libanais Gibran Khalil Gibran : « *Si vous révélez vos secrets au vent, vous ne devriez pas blâmer le vent de les avoir révélés aux arbres* » (à méditer). Le succès passe forcément par la prévention et la parfaite communication. Il faudrait que les trésoriers et leurs associations se fédèrent pour aider à lutter contre la fraude, fléau des temps modernes.



Rôles des banques et des associations de trésoriers

Banques et association de trésoriers, toutes deux, doivent aider leurs clients et membres/adhérents en communiquant clairement et régulièrement sur le sujet de la fraude. Certaines banques sont très actives et on ne peut que s'en féliciter. Les associations de trésoriers elles aussi par le pouvoir fédérateur et leur réseau doivent contribuer à recommander les bonnes pratiques de préventions, comme celles décrites dans les illustrations jointes à cet article. Comme les comportements frauduleux ont cette faiblesse d'être très répétitifs et systématiques, les expliquer ouvertement permettrait de prévenir certains risques. Un petit exemple vaut plus qu'un long discours, si nous voulions paraphraser Napoléon. Nos associations devraient même montrer par des vidéos ou enregistrements, le genre de fraude auxquelles on est exposé bien malgré soi. Cela devrait même faire part de cours de trésorerie de base et des bonnes pratiques que nous essayons de disséminer à notre communauté de membres. Puissions-nous faire d'incidents malheureux avérés des exemples de ce qu'il ne faudrait pas faire. La fraude ne devrait pas être un sujet tabou, même pour les victimes.

Conclusions :

Nous ne pouvons donc qu'encourager les trésoriers et leurs associations à collaborer pour prévenir les risques et partager les expériences, aussi mauvaises soient-elles. Dans l'adversité, on apprend les uns des autres. La fraude reste un sujet très sensible, dont on préfère ne pas parler et qu'on règle, en général, en famille, à l'écart des regards indiscrets. C'est là le tort qui fait que beaucoup ne soupçonnent pas la triste réalité. Certaines banques, notamment BNP Paribas ou d'autres ont compris que c'était aussi leur intérêt que de lutter contre la fraude. Les banques sont aussi des victimes et leurs clients pourraient le leur faire payer cher, même si parfois cela le serait reproché à tort. En cas de problème, on cherche toujours les coupables ailleurs que chez soi, c'est humain. Jamais un CFO ne vous reprochera trop de zèle et trop de prévention. Par contre, toute erreur se paiera cash et pour un trésorier, c'est un comble ! Nous aimerions dire comme Sophocle (propos d'Œdipe à Colone) qu' « *un bien acquis par fraude ne profite jamais longtemps* ». Cependant, cela serait une maigre consolation pour la victime et il est fort à parier que jamais vous ne reverrez les fonds détournés.

«*La fraude est l'hommage que la force rend à la raison* ». (Charles P. Curtis)

François Masquelier, Chairman of ATEL