Comment déjouer les tentatives de fraude ?

La fraude au faux fournisseur : 48 % des tentatives

Se faire passer pour un fournisseur pour demander à « son » client un changement de coordonnées bancaires est la fraude externe la plus répandue.

Jean-Pierre travaille au service comptable d'une centrale d'achat alimentaire. Un jour, il reçoit un courriel d'un gros fournisseur, une coopérative agricole, qui lui indique un changement de coordonnées bancaires et un changement de numéro de téléphone. Le courriel est signé par son interlocuteur habituel, M. Jean, le directeur administratif de la coopérative. Jean-Pierre compose le nouveau numéro. On lui indique que M. Jean est en déplacement et on lui confirme le changement de numéro de compte. Au cours des 6 mois suivants, Jean-Pierre met en paiement trois factures pour un total de 230 000 €.
Un jour, M. Jean appelle Jean-Pierre car il n'a pas été payé. Ensemble, ils découvrent la fraude.

Comment se protéger ?

En cas de demande de changement de coordonnées bancaires d'un fournisseur, il faut, surtout si le nouveau compte est à l'étranger :
– contacter directement le fournisseur en question sans utiliser les coordonnées présentées dans le courriel ou le courrier papier ;
– mettre en place un système de double validation pour tout changement de ce type.

Comment réagir ?

Si un virement vient d'être effectué, sans attendre, il convient :
– d'alerter sa banque pour bloquer le paiement ;
– de saisir les autorités ;
– de prévenir le fournisseur.

Une variante : les escrocs ne manquent pas d'imagination ! Certains d'entre eux n'hésitent pas à contacter les entreprises en se faisant passer pour l'administration. Le motif : obtenir une copie des factures impayées de leurs clients à des fins prétendument statistiques. En réalité, grâce à ces factures, ils n'ont plus qu'à contacter les clients « en retard » en se faisant passer pour une société de recouvrement et à les faire payer.

La fraude au président : 38 % des tentatives

Même si elle émane de sa hiérarchie, une demande de paiement pressante et inhabituelle doit éveiller l'attention.

Directeur financier de la filiale néerlandaise d'un groupe

français de cinéma, Edwin reçoit, un jour de mars 2018, un courriel venant de la direction générale française. Dans ce courriel, il est question de l'acquisition d'une société à Dubaï. Une opération qui doit être menée avec discrétion et rapidité au risque d'être compromise et qui nécessite que la filiale néerlandaise procède à une avance de fonds. Par prudence, Edwin en informe Derje, sa directrice. Puis, tous deux persuadés du caractère légitime de la demande, ils ordonnent plusieurs virements. La fraude ne sera détectée que quelques semaines plus tard. Au total, 19,2 M€ auront été détournés.

Comment se protéger ?

La fraude au président est un cas typique d'abus de confiance. Elle s'appuie sur la connaissance que les fraudeurs ont de l'entreprise cible, sur la mise en place d'un scénario crédible et sur leur capacité à contrôler psychologiquement la personne qui, malgré elle, va devenir leur complice. Pour limiter ce risque de fraude, il faut :
– assurer la confidentialité des organigrammes (au moins en extraire le nom et les coordonnées des responsables financiers et comptables) ;
– limiter la communication de l'entreprise autour de ses partenariats et de ses grands projets ;
– sensibiliser les salariés en leur présentant la mécanique de cette fraude ;
– rappeler aux salariés qu'ils doivent systématiquement mettre en place une procédure de validation permettant de s'assurer de l'identité du demandeur et du caractère légitime de la demande (par exemple, contacter directement le chef d'entreprise, un cadre, le cabinet d'expertise comptable, même s'ils sont en vacances) quand la demande est insolite et/ou formulée par un interlocuteur inconnu faisant preuve d'insistance (flatterie, intimidation) ;
– mettre en place un protocole de double signature ou un principe de supervision pour tout virement supérieur à 1 000

€.

Comment réagir ?

Si le virement vient d'être effectué, il n'est peut-être pas trop tard. Les banques disposent, en effet, d'une possibilité de rappel des fonds durant les premières heures qui suivent l'ordre. Sans attendre, il convient :
– d'alerter sa banque (y compris en dehors des heures d'ouverture, via son numéro d'urgence) ;
– de saisir les autorités (la police dispose de services spécialisés).

Attention : mettre la pression sur sa victime et l'isoler est la base de toute escroquerie. Aussi, pour rompre cette emprise, le réflexe doit consister, en cas de doute, même léger, à toujours en parler à un tiers.

Les cyber-fraudes : 29 % des tentatives

Les courriels inhabituels invitant à télécharger des pièces jointes ou à renseigner des mots de passe doivent finir dans la corbeille.

Cadre administratif dans une société de transport de marchandises, Gilles est en télétravail depuis le début du confinement. Comme tous ses collègues dans le même cas, il passe plusieurs heures par jour à participer à des visioconférences. Et d'ailleurs, il vient de recevoir un courriel aux couleurs de Zoom. L'outil de visioconférence lui indique qu'il peut, pendant 48 heures, visionner l'enregistrement de la dernière réunion de direction. Une réunion à laquelle il n'a pas pu assister. Il se connecte, via ce courriel, sur une page d'accueil où ses code et mot de

passe Microsoft lui sont demandés. Il ne s’en étonne pas et les renseigne. Or il n’accédera jamais à l’enregistrement de la conférence mais apprendra, quelques jours plus tard, que le serveur de son entreprise a été victime d’une attaque de rançongiciel qui a bloqué son fonctionnement pendant une semaine.

Comment se protéger ?

Le phishing (tentative d’extorsion de mots de passe ou de coordonnées bancaires via des mails ou des interfaces Web imitant ceux d’une entreprise ou d’une administration) et les rançongiciels (logiciels cryptant les données et réclamant une rançon pour les libérer) se répandent comme tous les logiciels malveillants. Dès lors, il convient :
– de mettre à jour les antivirus et systèmes d’exploitation ;
– de ne jamais ouvrir les pièces jointes des courriels douteux (inhabituels, expéditeurs inconnus, style impersonnel, texte mal traduit…) ;
– d’effectuer une sauvegarde quotidienne des données stockées sur des supports déconnectés du réseau.

Comment réagir ?

Dès qu’une machine est touchée, immédiatement, il faut :
– la déconnecter du réseau ;
– alerter les services techniques (internes ou externes à l’entreprise) ;
– porter plainte ;
– ne pas payer la rançon demandée (rançongiciel).