SOCIAL ENGINEERING, FRAUDE AU FAUX VIREMENT BANCAIRE

Qu'est-ce que le social engineering et la fraude au faux virement ?

Le social engineering, c'est l'art, la science de manipuler des personnes afin d'obtenir quelque chose d'elles sans qu'elles ne s'en rendent compte. On influence ou abuse de la confiance d'une personne pour obtenir un bien ou une information généralement à propos d'un système informatique (mot de passe, données sensibles). Il s'agit de la fameuse faille humaine.

La fraude au faux virement (FoVI) appelée aussi escroquerie au président consiste à faire payer une entreprise en se faisant passer pour la direction de la société ou un partenaire commercial. Mission des escrocs, mettre en place un transfert d'argent vers la banque de leur choix.

Voici un exemple récent pour illustrer ces propos :

« Des malfaiteurs ont par exemple frappé dans le Bas-Rhin, ou encore dans les Yvelines au préjudice d'un grossiste en matériel médical. La société francilienne pensait avoir affaire à son fournisseur régulier basé en Inde mais le RIB (relevé d'identité bancaire) de la facture avait été changé. Bilan : 13 000 euros perdus.

Des tentatives à plusieurs dizaines de millions d'euros ont également été recensées. Tout le territoire est concerné, mais aussi nos voisins européens francophones. Sont visés les pharmacies, hôpitaux, EHPAD, collectivités territoriales et tout les professionnels (grossistes et semi-grossistes) en matériel médical. Téléphones et courriels des usurpateurs apparaissent comme des numéros ou des adresses françaises. »

Comment se protéger contre le social engineering ?

On commence par ne pas laisser trop de traces sur Internet et d'en supprimer un maximum le cas échéant.

Le manipulateur adore les adresses e-mail que vous avez laissées par-ci par-là. Il cherche à identifier vos centres d'intérêt, vos loisirs, vos habitudes, vos amis. Il cherche de façon générale à créer une carte d'identité sur vous et plus vous donnez d'informations plus vous lui facilitez la tâche.

Les points suivants permettent de compliquer de manière considérable l'accès aux données sensibles :

- Se méfier des personnes extérieures à l'entreprise : plus l'entreprise est importante, plus il est facile pour les personnes tiers de s'infiltrer. Face à ce risque, il est important de rester vigilant et de ne pas se montrer trop ouverts.

- Informations par téléphone : il est conseillé de ne donner aucune information confidentielle par téléphone. Cela vaut avant tout pour les appels entrants et provenant de partenaires encore inconnus. Même les informations annexes peuvent aider les escrocs dans leurs démarches. Toute information quelle qu'elle soit présente un risque.

- Les emails provenant d'expéditeurs inconnus : si un expéditeur ne dévoile pas son identité, il est conseillé de faire attention. Les salariés d'une entreprise doivent dans tous les cas avertir leurs supérieurs hiérarchiques avant de répondre. Si la demande du message parait suspicieuse (effectuer un virement ou autre), il convient alors d'appeler l'expéditeur en question.

- Gare aux liens et aux pièces jointes dans les emails : il devient de plus en plus courant de recevoir des emails qui contiennent des liens vers des formulaires de saisie. Les escrocs utilisent ces techniques pour s'emparer de données de banque, des mots de passe voire des numéros clients. Pour le monde de l'entreprise, ce sont des pratiques courantes. En principe, les banques sérieuses, les boutiques en ligne ou les sociétés d'assurances n'exigent pas de leurs clients de telles informations. Il faut également prendre garde face aux pièces jointes. Il se peut que ces dernières présentent des programmes malveillants qui s'installeront en arrière-plan et qui s'empareront des données. Ce risque peut être minimisé en recommandant à vos salariés de n'ouvrir les emails qui ne proviennent que d'expéditeurs connus.

- Protection des données sur les réseaux sociaux : La préparation aux attaques d'ingénierie sociale doit se faire en amont. Au-delà du site Internet de l'entreprise, les réseaux sociaux présentent également une formidable source d'informations pour les escrocs du Net. En règle générale, il convient de demander aux salariés de configurer leurs profils pour qu'aucune information ne soit divulguée et de ne pas parler de leurs activités professionnelles sur ces plateformes.

En règle générale, la seule façon de se protéger est de s'armer de bon sens. Il est généralement utile de réfléchir sur les informations que l'on est amené à révéler, et à qui.