Ingénierie sociale (escroquerie au président)

Le terme d'« ingénierie sociale » (en anglais « social engineering ») désigne l'art de manipuler des personnes afin de contourner des dispositifs de sécurité. L'ingénierie sociale est basée sur l'utilisation de la force de persuasion et l'exploitation de la crédulité en se faisant passer pour une personne de la société, par exemple un administrateur, voire le directeur lui-même (notamment en utilisant des adresses e-mails quasi identiques dans la syntaxe). D'autres intervenants externes peuvent entrer dans le schéma de cette escroquerie, à savoir un soi-disant avocat ou notaire par exemple.

Il s'agit d'une technique qui consiste au final à obtenir la confiance du lésé, afin de lui demander d'opérer certains versements d'argent, par exemple sur des comptes bancaires en Israël, Chine ou Angleterre.

D'une manière générale, la méthode d'ingénierie sociale se déroule selon le schéma suivant :

- **Une phase d'approche**, par e-mail ou par téléphone, pour mettre l'utilisateur en confiance (en se faisant passer pour une personne de sa hiérarchie, de son entourage commercial, un client, un fournisseur, un avocat, un notaire, etc.)
- **Une mise sous pression**, afin de le déstabiliser et de s'assurer de la rapidité de sa réaction (par exemple pour un prétexte de sécurité, de discrétion, une situation d'urgence, un besoin de liquidités, une affaire à saisir sans délai)
- **Une diversion**, c'est-à-dire une phrase ou une situation permettant de rassurer l'employé pour éviter qu'il se focalise sur la mise sous pression (par exemple des remerciements, des compliments, une phrase rassurante ou, dans le cas d'un courrier électronique, une redirection vers le site web de l'entreprise)

Recommandations

- Informer et sensibiliser les employés concernés, les RH et la comptabilité de l'entreprise.
- Ne jamais utiliser le bouton «répondre» des courriels, mais systématiquement en rédiger un nouveau, l'adresse électronique des auteurs étant une «contrefaçon» visuellement proche de l'original.
- Prendre contact téléphoniquement ou «de visu» avec le directeur.
- Ne jamais agir dans l'urgence (sous la pression de tierces personnes).
- Ne pas contrevenir aux règles usuelles de sécurité interne à l'entreprise (sous le prétexte de l'urgence et de la confidentialité).

Les liens utiles :

Police neuchâteloise
www.ne.ch/police

Prévention suisse de la criminalité
www.skppsc.ch

Site de la confédération suisse
www.melani.admin.ch
www.cybercrime.admin.ch

Numéros d'urgence :

Police : 117

Pompiers : 118

Ambulance : 144

Contact :

Rue des Poudrières 14
CP 96, 2006 Neuchâtel

- Tél. **032 889 9000**
- Fax **032 722 0296**

police.neuchateloise@ne.ch

police NEUCHÂTELOISE

Arn@ques

Internet

La police neuchâteloise

sensibilise les usagers d'internet

Une mise en garde de votre police NEUCHÂTELOISE

Arn@ques sur Internet

Quelques conseils de la police neuchâteloise sur différentes arn@ques

Les conseils de votre police :

- **Se méfier des trop bonnes affaires.**

  Il convient de rester attentif lorsque les prix sont particulièrement en dessous du marché.

- **Toujours se renseigner.**

  Evaluation du vendeur/acheteur, vérifier l'existence d'une société, utiliser les moteurs de recherche.

- **Rester vigilant lorsque, pour une transaction en Suisse, votre interlocuteur est à l'étranger.**

  Les adresses e-mail, les coordonnées de la personne, les numéros de téléphone, le contenu du courriel sont autant de signes qui permettent de le déterminer.

- **Refuser de payer par le biais de sociétés de transfert d'espèces.**

  Ce type de paiement peu fiable est fréquemment utilisé par les escrocs.

- **Ne jamais transmettre votre mot de passe, votre identifiant ou vos coordonnées bancaires.**

  Les fournisseurs d'adresses e-mail, les réseaux sociaux, les plates-formes d'échanges commerciaux, les banques et autres services de paiement reconnus ne vous demanderont jamais votre mot de passe ou autre information personnelle/privée.

- **Définir un mot de passe sûr.**

- **Supprimer les courriels suspects.**

  Effacer les e-mails dont l'expéditeur n'est pas connu et/ou dont l'objet est douteux, ceci sans même l'ouvrir.

- **Mettre à jour et sécuriser vos équipements informatiques.**

  Garder toujours à l'esprit qu'Internet et les sites de communication/réseaux sociaux (MSN, Facebook, Twitter, etc.) sont publics et accessibles à n'importe qui de façon pratiquement anonyme.

- **Ne pas se laisser filmer par webcam dans des situations compromettantes.**

- **Ne pas donner suite à des sollicitations spontanées.**

  Loteries, héritages, propositions d'achats, etc.

Les escroqueries fréquentes :

Passeurs d'argent

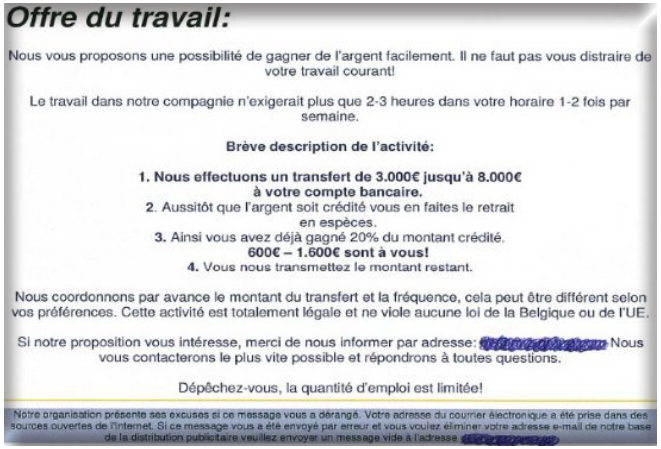
Une activité qui est illégale (en anglais money mule).

Cette escroquerie se présente sous la forme d'e-mails offrant des jobs de «gestionnaire commercial», «assistant-trader», etc., assortis de perspectives de rémunération des plus attractives. Hormis la rémunération promise, la prestation à fournir à elle seule devrait déjà éveiller les soupçons, à savoir mettre son compte bancaire ou postal à disposition pour recevoir de l'argent et retirer cette somme le même jour pour l'envoyer à divers destinataires à l'étranger, via des sociétés de transfert d'espèces. Si ce type d'offre de travail d'appoint existe réellement, il faut tout de même savoir que l'activité en question est illégale. En effet, la personne qui la pratique devient «passeur d'argent» puisqu'elle blanchit de l'argent provenant de divers délits (généralement du phishing, à savoir le piratage de comptes bancaires/postaux par Internet).

Recommandations

- Ne pas répondre à de tels courriels.
- Supprimer les e-mails immédiatement.

Exemple d'annonce :



Offre du travail:

Nous vous proposons une possibilité de gagner de l'argent facilement. Il ne faut pas vous distraire de votre travail courant!

Le travail dans notre compagnie n'exigerait plus que 2-3 heures dans votre horaire 1-2 fois par semaine.

Brève description de l'activité:

1. Nous effectuons un transfert de 3.000€ jusqu'à 8.000€ à votre compte bancaire.
2. Aussitôt que l'argent soit crédité vous en faites le retrait en espèces.
3. Ainsi vous avez déjà gagné 20% du montant crédité. **600€ – 1.600€ sont à vous!**
4. Vous nous transmettez le montant restant.

Nous coordonnons par avance le montant du transfert et la fréquence, cela peut être différent selon vos préférences. Cette activité est totalement légale et ne viole aucune loi de la Belgique ou de l'UE.

Si notre proposition vous intéresse, merci de nous informer par adresse: [redacted] Nous vous contacterons le plus vite possible et répondrons à toutes questions.

Dépêchez-vous, la quantité d'emploi est limitée!

Notre organisation présente ses excuses si ce message vous a dérangé. Votre adresse du courrier électronique a été prise dans des sources ouvertes de l'Internet. Si ce message vous a été envoyé par erreur et vous voulez éliminer votre adresse e-mail de notre base de la distribution publicitaire veuillez envoyer un message vide à l'adresse [redacted]

Sextorsion

Les victimes, généralement de sexe masculin, sont contactées sur divers réseaux sociaux par des femmes inconnues. Suite à ce premier échange, ces dernières proposent de continuer la conversation sur une plate-forme de vidéocommunication de type Skype. Elles se déshabillent devant la caméra et demandent à leurs victimes de s'adonner à des actes sexuels, également devant la caméra. Les cybercriminels qui se dissimulent derrière le profil de la jeune femme enregistrent tout et se servent ensuite de ces images pour faire chanter la victime. Ils exigent une certaine somme d'argent, à virer par le biais d'une société de transfert d'espèces, sans quoi ils diffuseront les images compromettantes sur Internet (notamment Youtube) ou les enverront aux amis de la victime sur Facebook.

Recommandations

Il est recommandé à toute personne se trouvant dans une telle situation d'interrompre immédiatement le contact avec l'auteur de l'arnaque et de ne céder en aucun cas au chantage. En effet, les criminels continuent généralement d'exiger de l'argent après un premier paiement. Par ailleurs, il arrive souvent que les images soient publiées en ligne malgré le paiement.

Dans ce cas, la seule solution est de faire supprimer la vidéo ou la photo de la plate-forme en question. Sur Facebook et Youtube, par exemple, les contenus pornographiques sont interdits et peuvent être effacés relativement rapidement si la personne visée en fait la demande.