La sécurité informatique

Les arnaques

1. L'ingénierie sociale

Le terme d'« ingénierie sociale » (en anglais «social engineering ») désigne l'art de manipuler des personnes afin de contourner des dispositifs de sécurité (le facteur humain pouvant être considéré comme le maillon faible de tout système de sécurité). Il s'agit ainsi d'une technique consistant à obtenir des informations de la part des utilisateurs par téléphone, courrier électronique, courrier traditionnel ou contact direct. L'ingénierie sociale est basée sur l'utilisation de la force de persuasion et l'exploitation de la naïveté des utilisateurs en se faisant passer pour une personne de la maison, un technicien, un administrateur, etc.

La meilleure façon de se protéger des techniques d'ingénierie sociale est d'utiliser son bon sens pour ne pas divulguer à n'importe qui des informations pouvant nuire à la sécurité de l'entreprise. Il est ainsi conseillé, quel que soit le type de renseignement demandé :

de se renseigner sur l'identité de son interlocuteur en lui demandant des informations précises (nom et prénom, société, numéro de téléphone) ; de vérifier éventuellement les renseignements fournis ; de s'interroger sur la criticité des informations demandées.

2. Scam ou nigerian scam

Le «scam» («ruse» en anglais), est une pratique frauduleuse d'origine africaine, consistant à extorquer des fonds à des internautes en les appâtant avec une grosse somme d'argent dont ils pourraient toucher un pourcentage. L'arnaque du scam est issue du Nigeria, ce qui lui vaut également l'appellation «419» en référence à l'article du code pénal nigérian réprimant ce type de pratique.

L'arnaque du scam est classique : vous recevez un courrier électronique de la part du seul descendant d'un riche africain décédé il y a peu. Ce dernier a déposé plusieurs millions de dollars dans une compagnie de sécurité financière et votre interlocuteur a besoin d'un associé à l'étranger pour l'aider à transférer les fonds. Il est d'ailleurs prêt à vous reverser un pourcentage non négligeable si vous acceptez de lui fournir un compte pour faire transiter les fonds.

En répondant à un message de ce type, l'internaute s'enferme dans un cercle vicieux pouvant lui coûter de quelques centaines d'euro s'il mord à l'hameçon et même la vie dans certains cas.

En effet, deux cas de figures se présentent : Soit les échanges avec l'escroc se font virtuellement auquel cas celui-ci va envoyer quelques "documents officiels" pour rassurer sa victime et petit à petit lui demander d'avancer des frais pour des honoraires d'avocats, puis des frais de douanes, des frais de banque, etc.

Soit la victime accepte, sous pression du cyberbandit, de se rendre dans le pays avec la somme en liquide auquel cas elle devra payer des frais pour pouvoir rester dans le pays, payer des frais de banque, soudoyer des hommes d'affaires, et ainsi de suite.

Dans le meilleur des cas la victime rentre chez elle en avion délestée d'une somme d'argent non négligeable, dans le pire scénario plus personne ne la revoit jamais...

3. Le phishing

Technique utilisée par les escrocs en ligne, visant à usurper l'identité d'une personne ou d'une entité connue.

Le principe est le suivant : un internaute reçoit un email non sollicité (spam) à l'habillage d'une entité connue (portail, banque, etc.). L'objectif est d'attirer l'internaute sur un faux site afin de mettre à jour ses informations personnelles (carte bancaire, numéro de téléphone...). Ces informations, saisies dans un faux formulaire, sont alors utilisées à mauvais escient par des escrocs.

Les loteries

Vous recevez un courrier électronique indiquant que vous êtes l'heureux gagnant du premier prix d'une grande loterie d'une valeur de plusieurs (centaines de) milliers d'euros. Pour empocher le pactole il suffit de répondre à ce courrier.

Après une mise en confiance et quelques échanges de courriers, éventuellement avec des pièces jointes représentant des papiers attestant que vous êtes bien le vainqueur, votre interlocuteur vous expliquera que pour pouvoir toucher ladite somme, il faut s'affranchir de frais administratifs, puis viennent des frais de douane, des taxes diverses et variées, etc.

C'est de cette façon que ces cybertruands arrivent à extorquer des milliers d'euros à des internautes dupes de cette supercherie.

Pour éviter tout problème, vérifier que la loterie ou le jeu concours possède un règlement auquel on est en droit d'accéder. Et comment expliquer qu'il faille engager des frais pour toucher une somme si importante ?

Bref, le mieux est de glisser directement ce type de message à la corbeille !

4. Les Hoax

On appelle hoax (en français canular) un courrier électronique propageant une fausse information et poussant le destinataire à diffuser la fausse nouvelle à tous ses proches ou collègues.

Ainsi, de plus en plus de personnes font suivre (anglicisé en forwardent) des informations reçues par courriel sans vérifier la véracité des propos qui y sont contenus. Le but des hoax est simple : provoquer la satisfaction de son concepteur d'avoir berné un grand nombre de personnes.

Les conséquences de ces canulars sont multiples :

L'engorgement des réseaux en provoquant une masse de données superflues circulant dans les infrastructures réseaux ;

Une désinformation, c'est-à-dire faire admettre à de nombreuses personnes de faux concepts ou véhiculer de fausses rumeurs (on parle de légendes urbaines) ;

L'encombrement des boites aux lettres électroniques déjà chargées ;

La perte de temps, tant pour ceux qui lisent l'information, que pour ceux qui la relayent ;

La dégradation de l'image d'une personne ou bien d'une entreprise ;

L'incrédulité : à force de recevoir de fausses alertes les usagers du réseau risquent de ne plus croire aux vraies.

Ainsi, il est essentiel de suivre certains principes avant de faire circuler une information sur Internet.

Afin de lutter efficacement contre la propagation de fausses informations par courrier électronique,

il suffit de retenir un seul concept :

Toute information reçue par courriel non accompagnée d'un lien hypertexte vers un site précisant sa véracité doit être considérée comme non valable !

Ainsi tout courrier contenant une information non accompagnée d'un pointeur vers un site d'information ne doit pas être transmis à d'autres personnes.

Lorsque vous transmettez une information à des destinataires, cherchez un site prouvant votre propos.