LES PRINCIPES DE PERSUASION

et l'ingénierie sociale

L'ingénierie sociale consiste en un ensemble de techniques utilisées par les cybercriminels pour inciter des utilisateurs à leur envoyer des données confidentielles ou à ouvrir des liens vers des sites infectés ou bien encore, pour infecter leurs ordinateurs avec des programmes malveillants.

Cialdini a développé six principes de persuasion dans le domaine du marketing. Ces principes s'appuient sur l'idée selon laquelle la prise de décision nécessite des efforts, de sorte que les individus utilisent beaucoup de raccourcis de prise de décision pour décider quoi faire, comment se comporter ou quelle action entreprendre.

Ces principes peuvent également être utilisés par les cybercriminels lorsqu'ils veulent persuader leurs potentielles victimes d'entreprendre des actions spécifiques.

ENGAGEMENT & COHÉRENCE

L'engagement consiste à se comporter de la manière dont se dit être. La cohérence consiste à se comporter de manière cohérente selon nos opinions, croyances, etc.

Comment ça marche? Le fraudeur fait une petite requête à la victime et après que celle-ci s'y soit conformé, il fait des demandes plus importantes. La victime se sent obligé de se conformer à nouveau afin de rester cohérente avec elle-même

PREUVE SOCIALE

La preuve sociale consiste à reproduire ce que les autres font ou croient parce que l'on estime que si tout le monde le fait, alors l'action doit être légitime.

Comment ça marche? Le cybercriminel peut mentionner des noms d'amis de la victime ou bien mentionner qu'un certain nombre d'employés de l'organisation ont participé à l'action proposée par le cybercriminel.

RÉCIPROCITÉ

La réciprocité est une norme sociale très forte qui nous oblige à donner en retour aux autres ce que nous avons reçu d'eux.

Comment ça marche? Le cybercriminel offre des cadeaux ou des faveurs avant de commettre son attaque. Cela lui permet d'augmenter la probabilité que la victime va se conformer à ses demandes en raison du sentiment d'obligation.

AUTORITÉ

Les individus ont tendance à faire confiance aux personnes qu'ils perçoivent comme ayant une expertise ou autorité spécifique

Comment ça marche? Les fraudeurs peuvent se faire passer ou voler l'identité de personnes en position d'autorité (ex: le président d'une organisation) ou détenant une expertise (ex: un médecin)

RARETÉ

Les individus ont tendance à accorder plus d'importance aux opportunités, aux biens, aux services qui sont les moins disponibles ou qui sont rares.

Comment ça marche? Les fraudeurs peuvent promouvoir des services (ex: un logiciel en essai gratuit) ou biens à des potentielles victimes en mettant l'emphase sur le fait que l'offre se terminera bientôt afin d'augmenter la pression.

SYMPATHIE

Les individus ont tendance à se conformer aux demandes des personnes qu'ils apprécient soit parce qu'ils partagent des similarités ou parce qu'ils épouvent une attirance physique

Comment ça marche? Les fraudeurs utilisent des photos de profil de personnes attirantes afin de créer des connections avec les potentielles victimes et ainsi les faire plier aux demandes.