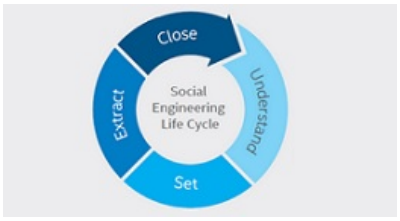
Les cybercriminels à la pointe de la psychologie | Le Net Expert Informatique



Les cybercriminels à la pointe de la psychologie

Les méthodes de substitution des données évoluent et se calquent de plus en plus sur des modèles de manipulation existant dans le monde réel tels que les techniques de ventes ou d'escroquerie. Nommé « piratage de l'OS humain », cette dernière publication soutenue par le Centre Européen de lutte contre la cybercriminalité d'Europol met en avant 6 leviers d'influence que les hackers utilisent pour rendre complices/acteurs les employés d'une société.

Ainsi, on parle de réciprocité des échanges pour décrire la tendance naturelle que l'homme a de répondre systématiquement aux courriels. Technique couramment utilisée dans le phishing, la rareté de l'offre motive les individus à obtenir une ressource qu'ils pensent être unique ou limitée dans le temps. Autre phénomène purement humain, la cohérence des engagements permet aux hackers de profiter de la victime qui souhaite simplement tenir ses promesses, par exemple, en suivant les processus de sécurité édictés par un pirate se présentant comme membre de l'équipe SI.
L'appréciation et l'amitié sont un facteur qui permet aux hackers d'augmenter la réussite de leur hameçonnage en gagnant la confiance d'une victime, la « charmer », en essayant notamment de rentrer directement en contact soit par le téléphone ou en ligne. Le respect de l'autorité est un autre levier. Par le biais d'un mail, le cybercriminel abuse de sa victime en se faisant passer pour le PDG de l'entreprise. Dernier levier discerné par Intel Security, un employé sous l'effet de masse a tendance à octroyer plus facilement sa confiance. Ainsi un mail malveillant aura plus d'impact s'il est envoyé à un groupe de collègues plutôt qu'à un seul destinataire.
Pour l'année 2014, McAfee Labs dénombre plus de 30 millions de liens suspects en relation avec l'augmentation des mails de phishing. Autre chiffre mis en avant dans ce rapport, 92% des employés contre 80% dans le monde se seraient déjà fait piéger par des menaces informatiques et le coût de cette cybercriminalité est estimé au total à 392 milliards d'euros par an. 2/3 des e-mails sont des spams et 18% des utilisateurs visés par mail de phishing cliquent sur ces liens malveillants, Intel Security rappelle l'importance que les entreprises doivent accorder à l'éducation de leurs collaborateurs concernant ces techniques de persuasion et d'escroquerie.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.itpro.fr/n/cybercriminels-pointe-psychologie-21105/
Par Tristan Karache