L'ingÃ©nierie sociale, l'outil prÃ©fÃ©rÃ© des escrocs

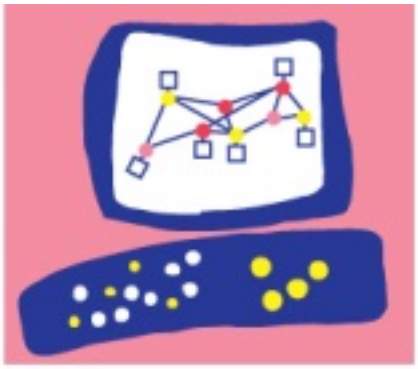
Internet

PostÃ© par : JulieM
PubliÃ©e le : 13/2/2014 13:30:00

L'ingÃ©nierie sociale est sournoise car elle exploite notre tendance naturelle Ã vouloir nous rendre utile. Les escrocs peuvent Ã©galement jouer sur les Ã©motions humaines, telles que la peur et la compassion. Voici quelques astuces employÃ©es par les escrocs pour soutirer des informations confidentielles, et comment vous en protÃ©ger.
Vous Ãªtes au bureau et un Ã©lectricien vient rÃ©soudre un problÃ¨me, ou votre tÃ©lÃ©phone sonne et c'est votre FAI qui vous informe d'un problÃ¨me avec votre compte.

C'est dans la nature humaine de coopÃ©rer, non ? Vous laissez l'Ã©lectricien entrer et le laissez faire ce qu'il doit faire. Vous rÃ©pondez aux questions posÃ©es par le reprÃ©sentant du service clientÃ¨le afin de vÃ©rifier votre identitÃ©. Malheureusement, au lieu de vous rendre utile, vous Ãªtes dÃ©sormais victime de l'ingÃ©nierie sociale. L'Ã©lectricien a installÃ© un routeur pirate ou des camÃ©ras de surveillance dans votre bureau. Le faux reprÃ©sentant du service clientÃ¨le connaÃ®t vos donnÃ©es personnelles, les informations de votre compte ou encore votre numÃ©ro de carte bancaire.

L'ingÃ©nierie sociale dÃ©signe les techniques utilisÃ©es par des individus pour conduire d'autres individus Ã effectuer certaines tÃ¢ches ou rÃ©vÃ©ler certains types d'information. Les cybercriminels et les voleurs profitent du dÃ©sir humain naturel de se rendre utile et de croire ce que les gens disent. Ces escrocs n'ont pas besoin d'employer de techniques de piratage sophistiquÃ©es ni de logiciels malveillants exploitant une vulnÃ©rabilitÃ© logicielle, quand il leur suffit simplement d'envoyer une piÃ¨ce jointe malveillante par email et demander au destinataire d'ouvrir le fichier.



Check Point®
SOFTWARE TECHNOLOGIES LTD.

L'ingÃ©nierie sociale n'est pas quelque chose de nouveau ; les escrocs et leurs escroqueries Ã©laborÃ©es ont existÃ© de tout temps. Ce qui est nouveau, c'est la quantitÃ© d'information que les escrocs peuvent recueillir sur leurs victimes ciblÃ©es avant mÃªme d'attaquer.

GrÃ¢ce aux rÃ©seaux sociaux, ils peuvent trouver toutes sortes d'information, par exemple le lieu de travail de leurs victimes ciblÃ©es, les noms de leurs collÃ¨gues, l'Ã©cole oÃ¹ elles ont

Ã©tudiÃ©, et mÃªme le dernier endroit oÃ¹ elles sont parties en vacances. Ils peuvent dÃ©terminer l'organigramme de l'entreprise ou les types de logiciels qu'elle utilise. Ils peuvent exploiter toutes ces informations pour convaincre une victime qu'ils disent la vÃ©ritÃ©.

Il est dans la nature humaine d'aider

Defcon, la plus grande confÃ©rence de pirates, organise tous les ans une compÃ©tition de type Â« capture du drapeau Â» en s'aidant de l'ingÃ©nierie sociale. Les participants ont quelques semaines pour Ã©tudier une sociÃ©tÃ© ciblÃ©e. De grandes entreprises telles qu'Apple, Johnson & Johnson et d'autres, ont Ã©tÃ© ciblÃ©es les annÃ©es prÃ©cÃ©dentes.

Le jour de la compÃ©tition, les concurrents entrent dans une cabine, appellent une personne de la sociÃ©tÃ©, et tentent de lui faire rÃ©vÃ©ler des Â« drapeaux Â», tels que la version du navigateur utilisÃ© dans l'entreprise ou le type de logiciel installÃ© sur son ordinateur.

Les candidats prÃ©tendent gÃ©nÃ©ralement Ãªtre des collÃ¨gues d'un autre bureau essayant de recueillir des informations pour le PDG, et avoir vraiment besoin d'aide parce qu'ils sont complÃ¨tement dÃ©passÃ©s. La plupart du temps, les gens veulent aider et proposent librement des informations.

La peur est lucrative

Les escrocs sont passÃ©s maÃ®tres de l'alarmisme. Une escroquerie courante consiste Ã appeler de la part d'un service d'assistance technique ou similaire en raison d'un problÃ¨me sur l'ordinateur de l'utilisateur. L'appelant demande Ã l'utilisateur de taper quelques commandes standard sur l'ordinateur et explique que le rÃ©sultat obtenu tÃ©moigne de la prÃ©sence de programmes malveillants ou d'autres problÃ¨mes graves. Ã ce stade, l'utilisateur est convaincu que quelque chose ne va pas bien et communique son numÃ©ro de carte bancaire au Â« reprÃ©sentant Â» pour rÃ©soudre le problÃ¨me.

VÃ©rifiez vÃ©rifiez, et vÃ©rifiez encore

Si quelqu'un appelle en prÃ©tendant Ãªtre d'une qualitÃ© officielle, demandez des preuves. Demandez un numÃ©ro de poste afin de pouvoir rappeler cette personne. Si la personne prÃ©tend Ãªtre un employÃ© d'un autre bureau ou d'un fournisseur, demandez une information vous permettant de confirmer son identitÃ©. S'il s'agit d'un policier, demandez son numÃ©ro de badge. Si ces personnes sont lÃ©gitimes, elles vous fourniront les informations demandÃ©es sans hÃ©sitation.

Ne cÃ©dez pas Ã la pression Â« vous avez quelques minutes pour agir Â». Vous avez toujours le temps de rÃ©flÃ©chir et de vÃ©rifier.

MÃ©fiez-vous toujours des situations dans laquelle vous Ãªtes activement contactÃ© au sujet d'un problÃ¨me. Aucune entreprise lÃ©gitime ne vous demandera votre mot de passe, et le gouvernement enverra toujours une lettre pour les communications officielles. Et si vous recevez soudainement un appel d'un ami ou d'un parent prÃ©tendant Ãªtre bloquÃ© dans un pays Ã©tranger et ayant besoin que vous leur envoyez de l'argent au plus vite, ne leur faite pas simplement confiance parce qu'il ou elle connaÃ®t le nom de vos frÃ¨res et sÅurs ou le nom de votre chien.

Soyez conscient de ce que vous communiquez en ligne, et rÃ©glez les paramÃ¨tres de contrÃ´le de votre confidentialitÃ©. Il existe certaines informations que vous ne devriez jamais communiquer en ligne, telles que votre mot de passe, les rÃ©ponses aux questions de sÃ©curitÃ© (comme le nom de jeune fille de votre mÃ¨re) ou votre numÃ©ro de sÃ©curitÃ© sociale.

Vous pouvez toujours vous rendre utile, mais prenez le temps de douter et de tout Ã©valuer. Une petite dose de scepticisme n'a jamais fait de mal, et peut faire une Ã©norme diffÃ©rence lorsqu'il s'agit de cybercriminalitÃ©, conclue **Thierry Karsenti,** Directeur Technique Europe - Check Point Software Technologies

Â