Engenharia Social: o golpe da persuasão

A internet em conjunto com as redes sociais foram e são até hoje consideradas um gigantesco avanço do século XXI, permitindo com que haja conexão entre pessoas, cidades e até países. Além disso, hoje é possível fazer praticamente tudo virtualmente, desde fazer compras a pagar contas.

Porém, neste meio digital de tanto avanço, existem pessoas de má fé que utilizam muitas vezes da ingenuidade de muitos e também da falta de conhecimento de outros a respeito dos meios virtuais, já que não é toda a população que possui domínio desse novo mundo. E, aproveitando-se destas questões, surgiram também inúmeros golpistas cibernéticos que utilizam redes sociais para extrair dinheiro, informações pessoais ou até sigilosas de empresas. Como é o caso da Engenharia Social, que surgiu nos meios físicos, mas migrou também para o meio digital.

Engenharia Social significa utilizar manipulação psicológica por meio da persuasão para conseguir acesso a tais informações confidenciais citadas anteriormente ou também a áreas importantes de uma instituição. Existem alguns exemplos mais conhecidos deste golpe, e são eles: *phishing, vishing e baiting, pretexting, squid pro quo* e muitos outros

O *phishing* pode ser considerado o tipo de golpe mais comum e o que mais ocorre nas redes sociais. Consiste em tentativas de adquirir ilicitamente senhas, números de documentos pessoais, dados bancários, número de cartão de crédito, etc. O golpista utiliza de e-mail, aplicativos, sites, anúncios e perfis nas redes sociais projetados para esses roubos; o criminoso se faz passar por uma pessoa ou empresa confiável enviando uma mensagem para conseguir atrair as vítimas.

Atualmente as redes sociais têm sido o principal alvo. Empresas nacionais ou multinacionais de várias marcas de roupas, eletrônicos e serviços possuem perfis oficiais e verificados no facebook, instagram, twitter e dentre outras mídias; e utilizam estas ferramentas para interagir com o consumidor e responder a comentários tanto positivos, quanto negativos. Utilizam também deste meio para ajudar o consumidor caso esteja tendo problemas com algum cadastro ou produto. E é desta interação que os infratores se aproveitam e criam falsos perfis de SAC ou suporte das empresas nas redes sociais e se passam por atendentes oferecendo ajuda e pedindo senhas, documentos ou número de celular; algumas pessoas distraídas, desesperadas para resolver sua situação ou até mesmo pessoas que não possuem muito conhecimento do meio virtual, nem percebem que o perfil não é verificado e acabam passando suas informações para o falso atendente que as convence com uma linguagem formal e acolhedora que promete ajuda.

A rede social mais afetada por esses golpes atualmente é o Instagram, com milhares de perfis falsos só esperando um comentário em alguma página oficial de empresas para fazerem suas vítimas.

É preciso sempre estar atento e desconfiar de e-mails não solicitados ou de perfis não verificados para evitar cair nesses golpes, pois uma vez passados informações restritas, os bandidos podem extrair altas quantias de dinheiro ou utilizar dados para fazer outros tipos de crimes.