

GOLPES E VULNERABILIDADES		GOLPES E VULNERABILIDADES
O que é Engenharia Social ?		Engenharia Social: é o ato de trabalhar a mente de uma pessoa para manipulá-la. Alguns Crackers utilizam desse método, onde eles nem mesmo precisam usar grandes habilidades tecnológicas, somente com a sua lábia, mentiras e manipulações, eles conseguem explorar o emocional da vítima para conseguir aquilo que querem. Pessoas que fazem isso usam de Engenharia Social.
O que seria o SCAM ?		SCAM: literalmente significa " Golpe " em inglês, são golpes utilizados por pessoas que aparentam trazer algum benefício com o objetivo de tirar vantagem de uma pessoa, como roubar dados ou dinheiro mesmo. Geralmente nesse método nem é preciso usar tecnologia, esse tipo de criminoso usa somente a manipulação e lábia para enganar os usuários - ou seja, usa Engenharia Social. Existem várias técnicas para o uso de SCAMs, que são: <div><div>- Furto de Identidade; - Phishing; - Pharming; - Advance Fee Fraud; - Hoax (Boatos);</div><div>- SQL Injection; - Man-In-The-Middle; - IP Spoofing</div></div> A melhor forma de impedir essa ameaça é não se deixar levar por promoções que parecem ser "boas demais para ser verdade".
- reservado para a questão acima -		
Como funciona o método de SCAM denominado Furto de Identidade ?		Furto de Identidade: são os famosos " fakes ", pessoas que criam um perfil falso para se relacionar com outros, em busca de brechas emocionais, necessidades físicas, monetárias e etc. A melhor arma que a pessoa pode usar para se proteger desse estilo de fraude é pesquisar bem as pessoas com que está se relacionando.
Como funciona o método de SCAM denominado Phishing ?		Phishing: é o ato de pescar dados de uma vítima por através de uma isca, geralmente os criminosos usam um aplicativo ou página de uma entidade que realmente parece ser legítima , como um banco, órgãos públicos e etc, fazendo as vítimas preencherem seus dados nela, talvez até passando informações de alta privacidade como contas de banco e senhas. Mas na verdade é tudo falso, quando a vítima percebe já é tarde demais, seus dados já foram passados para o criminoso. O que deve ser feito para não cair nesta armadilha é prestar atenção no URL do site, ou se o aplicativo realmente é legítimo, não cair na armadilha de arquivos que redirecionam para uma página duvidosa, sem o cadeado HTTPS.
Como funciona o método de SCAM denominado Pharming ?		Pharming: o Pharming é um Phising mais sofisticado , pois o Phishing imita um site real, mas ele não consegue alterar o endereço DNS do site, no URL podemos ver que não é o mesmo usado pela instituição original, já no Pharming o criminoso conseguiu invadir o servidor da Entidade e consegue fazer com que o URL original aponte para um servidor a sua escolha, onde ele captura os dados das pessoas desavisadas que tentarem usar os serviços do site. Essa é uma técnica muito mais complicada e difícil de detectar, porém é mais difícil de acontecer, por que exige um trabalho maior. O Pharming também é conhecido como DNS Poisoning (Envenenamento de DNS) .
Como funciona o método de SCAM denominado Advance Fee Fraud ?		Advance Fee Fraud: Do Inglês " Fraude de Taxa Antecipada ", são pessoas que prometem um benefício as vítimas sobre as circunstâncias de que para receber esse benefício a vítima teria que pagar uma "pequena taxa antecipada". Essas fraudes podem ir desde golpes que aparentam ser reais, como um empréstimo, até histórias mirabolantes, como um milhorário que promete passar parte da herança dele para a vítima sobre a circunstância de receber uma pequena quantia para fazer a transação.
Como funciona o método de SCAM denominado Hoax ?		Hoax: Do inglês " Boatos ", que são mentiras repassadas em massa para denegrir a integridade de uma pessoa ou instituição. Além disso, os Hoax podem gerar muitos outros problemas como: - Auto consumo de Tráfego sobre a entidade atacada - Espalhar Malwares junto aos boatos, pessoas podem repassar arquivos aparentam ser inofensivos mas estão levando malwares para outras pessoas; - Deixar as pessoas desinformadas e gerar caos geral; A melhor forma de se proteger contra Hoaxes é não espalhar boatos, histórias sem uma fonte fiel, e pior ainda, compartilhar arquivos falsos.
Como as empresas podem ser proteger de Ataques por através de Engenharia Social ?		A empresa que deseja se proteger de ataques por através de engenharia social deve: - Investir em Treinamento Anti-Engenharia Social: treinando os funcionários a identificar perguntas e conversas que poderiam levar as pessoas a serem enganadas; - Investir em equipamentos de leitura biométrica: para evitar que pessoas que tentam se passar por funcionários adentrem a empresa sem serem detectados; - Acompanhamento visual de serviços técnicos e treinamentos: pessoas que se apresentam como prestadores de serviço, treinadores e etc, devem ser acompanhadas por um colaborador de confiança (que não tenha intimidade com o prestador de serviço), ou então, eles deverão ser vigiados por câmera enquanto executam seus serviços; - Tomar cuidado com o descarte de informações no lixo: papeladas que contém informações relevantes da empresa devem ser picotadas antes de serem descartadas; - Adoção da Mesa Limpa: treinar os funcionários para não deixar papeladas na mesa ou computadores logados com a tela aberta;
- reservado para a questão acima -		

