1.Introdução a Engenharia Social

A ***engenharia social*** é uma abordagem manipulativa que se concentra em explorar os aspectos psicológicos e sociais das pessoas para obter informações confidenciais, acesso a sistemas ou influenciar suas ações de maneira prejudicial. Engenharia social adota estratégia de manipulação psicológica que visa enganar, persuadir ou influenciar pessoas a tomarem ações específicas, divulgar informações confidenciais ou realizar tarefas que possam ser prejudiciais para a segurança da informação ou outros fins maliciosos.

Essa abordagem explora a confiança, ingenuidade, curiosidade ou outras características humanas para alcançar seus objetivos. Os engenheiros sociais frequentemente se fazem passar por alguém que eles não são, como um funcionário de uma empresa, um colega de trabalho, um amigo, um técnico de suporte ou uma autoridade legítima para obter acesso a informações confidenciais.

1.1 Princípios da engenharia social

Os **princípios da engenharia social** são fundamentais para entender como essa abordagem de manipulação psicológica opera. Eles são os alicerces sobre os quais os engenheiros sociais baseiam suas táticas para obter informações confidenciais ou influenciar o comportamento das pessoas. Ao reconhecer quando essas técnicas estão sendo usadas, as pessoas podem tomar medidas para verificar a autenticidade das solicitações e proteger suas informações confidenciais.

Engenheiros utilizam de várias táticas e as mais comuns são:

- **Autoridade:** As pessoas são mais propensas a cooperar quando instruídas por uma "autoridade"
- **Intimidação:** Os criminosos intimidam a vítima a realizar uma ação. A secretária de um executivo recebe um telefonema informando que seu chefe está prestes a fazer uma apresentação importante, mas seus arquivos estão corrompidos. Os criminosos virtuais pedem que os arquivos sejam enviados imediatamente para eles.
- **Consenso/prova social:** As pessoas realizarão essa ação que se acharem que as outras pessoas irão aprovar. Os criminosos criam sites com depoimentos falsos que promovem um produto, indicando que é seguro.
- **Escassez:** As pessoas irão realizar essa ação se acharem que existe uma quantidade limitada. Os criminosos oferecem uma oportunidade limitada por pouco tempo, na esperança de incitar a vítima a agir rapidamente.
- **Urgência:** As pessoas irão realizar essa ação se acharem que existe um tempo limitado.
- **Familiaridade/gosto:** Os criminosos criam empatia com a vítima para estabelecer um relacionamento. As pessoas são mais propensas a fazer o que outra pessoa pede se gostarem dela.
- **Confiança:** Os criminosos criam uma relação de confiança com a vítima, que pode precisar de mais tempo para ser estabelecida. Um "*especialista em segurança*" telefona para a vítima oferecendo conselhos e pede as credenciais para dar retorno. Ao mesmo

tempo que ajuda a vítima, o criminoso descobre um “erro grave” que precisa de atenção imediata. A solução é a oportunidade do criminoso.

A representação é o ato de fingir ser outra pessoa. Uma farsa é um ato com a finalidade de enganar ou ludibriar. Uma farsa virtual pode causar tanto problema quanto uma violação real. ***Piggybacking*** ocorre quando um criminoso se identifica juntamente com uma pessoa autorizada para entrar em um local protegido ou uma área restrita.

Os criminosos usam vários métodos de ***piggybacking*** como parecer escoltados pela pessoa autorizada, juntam-se a uma grande multidão. ***Tailgating*** descreve a mesma prática. Uma armadilha evita o piggybacking usando dois conjuntos de portas. Depois que os indivíduos entram pela porta externa, essa porta deve fechar antes que entrem pela porta interna.

1.2 Técnicas de engenharia social

- **Personificação:** Essa técnica envolve a capacidade de se fazer passar por alguém ou algo que você não é. Isso pode incluir fazer-se passar por um funcionário de uma empresa, um colega de trabalho, um amigo ou qualquer outra identidade confiável. A personificação é usada para ganhar a confiança da vítima, o que torna mais provável que ela divulgue informações confidenciais ou cumpra solicitações.
- **Confiabilidade:** A confiança é essencial na engenharia social. Os engenheiros sociais trabalham para construir uma relação de confiança com suas vítimas, muitas vezes construindo relacionamentos falsos ou fornecendo informações falsas com um ar de autenticidade. Quando as vítimas confiam no atacante, elas são mais propensas a cumprir suas solicitações.
- **Dumpster diving e utilização não autorizada:** Esse princípio se concentra na obtenção de informações a partir de fontes físicas, como lixeiras, contêineres de reciclagem ou documentos impressos deixados sem proteção. Além disso, envolve o acesso não autorizado a instalações físicas ou sistemas de computador para obter informações valiosas.
- **Engenharia social online:** Embora as técnicas mencionadas acima se apliquem principalmente a interações pessoais, a engenharia social também se estende ao mundo online. Isso pode envolver a criação de perfis falsos em mídias sociais, o envio de e-mails de phishing ou a criação de sites falsos para enganar as pessoas.

1.3 Coleta de credenciais

A **coleta de credenciais** envolve a tentativa de obter informações de login e senha de usuários por meio de técnicas enganosas. Isso pode ser parte de uma tentativa de phishing ou pode ser realizado em sites falsos que se passam por legítimos. Os atacantes criam páginas da web ou mensagens que imitam sites legítimos, como os de bancos, redes sociais ou serviços de e-mail. As vítimas são levadas a acreditar que estão inserindo suas credenciais em um site real. Uma vez que as informações de login são inseridas, os atacantes as coletam e as usam para acessar as contas das vítimas, realizar atividades maliciosas ou roubar informações pessoais.

1.4 Campanhas de influência

Campanha de influência é mais uma tática de engenharia social que se concentra em influenciar as opiniões, atitudes e ações das pessoas por meio de campanhas de desinformação, manipulação emocional, propaganda enganosa ou outros métodos destinados a alcançar um determinado objetivo. Essas campanhas podem ser usadas para influenciar a opinião pública, moldar percepções, promover agendas políticas, econômicas ou sociais e, em alguns casos, até mesmo incitar ações específicas. A educação em literacia midiática e a conscientização sobre desinformação são ferramentas importantes para identificar e combater essas influências.

1.5 Identificação de alvos

Os operadores por trás da campanha identificam grupos-alvo ou indivíduos específicos que desejam influenciar. Isso pode ser baseado em fatores demográficos, psicográficos, geográficos ou outros critérios.

1.6 Desenvolvimento de narrativa

Uma narrativa é criada para transmitir uma mensagem específica. Isso pode incluir informações falsas, propaganda, teorias da conspiração, apelos emocionais ou outros elementos destinados a persuadir o público-alvo.

1.7 Distribuição de conteúdo

A narrativa é distribuída por meio de uma variedade de canais, incluindo mídias sociais, sites de notícias falsas, blogs, redes de mensagens, anúncios pagos e outros meios de comunicação. A disseminação muitas vezes é mascarada como conteúdo legítimo.

1.8 Amplificação

Os operadores podem usar robôs (***bots***) ou contas falsas nas mídias sociais para amplificar o alcance da campanha. Isso cria a ilusão de apoio popular à narrativa.

1.9 Engajamento

Os operadores buscam envolver o público-alvo, incentivando discussões, compartilhamentos, comentários e ações específicas que estejam alinhadas com os objetivos da campanha.

1.10 Monitoramento e adaptação

Durante a execução da campanha, os operadores monitoram o progresso e ajustam suas táticas conforme necessário. Isso pode envolver a criação de novos conteúdos, segmentação mais precisa ou adaptações à narrativa.

1.11 Avaliação do sucesso

A campanha é avaliada com base em métricas específicas, como o alcance da mensagem, o engajamento do público-alvo e a eficácia na influência das opiniões e ações desejadas.