TEMA 06
Engenharia Social

Habilidades:

- Entender a importância da integridade e confidencialidade dos dados.
- Aprender a elaborar e decifrar armadilhas digitais e falsificações.
- Compreender e elaborar perfis para evitar golpes de engenharia social.

Até aqui você já pôde ter noção de que os ataques cibernéticos são extremamente perigosos e se tornam mais desafiadores a cada dia. A Engenharia Social, muitas vezes, faz parte deles e é uma das principais artimanhas que definem o sucesso do crime virtual.
A **Engenharia Social irá abordar a manipulação psicológica das vítimas** (pessoas envolvidas que sofrem o ataque), **com o objetivo de adquirir informações confidenciais através do abuso da confiança, ignorância perante determinado assunto e até mesmo da ingenuidade da pessoa**.
Por diversas vezes, a vítima mal percebe que está sob ataque ou seus dados se encontram em perigo. O atacante que usa da Engenharia social irá explorar o que o usuário tem de mais vulnerável e atacar esses pontos de diversas maneiras. Costuma ser alguém que se apresenta longe de qualquer suspeita, extremamente comunicativo e persuasivo. Estuda o comportamento da(s) vítima(s) e aplica técnicas psicológicas, sociais e ambientais para conseguir exatamente o que precisa.

Contexto Histórico

A Engenharia Social é uma prática utilizada para manipular e enganar as pessoas, geralmente, com foco em obter informações confidenciais, acesso a sistemas ou influenciar comportamentos. Sua história remonta a séculos atrás, e evolui conforme a sociedade e a tecnologia avançam.
No passado, a Engenharia Social era praticada principalmente em ambientes offline, e envolvia técnicas de persuasão e manipulação pessoal. Por exemplo, vigaristas e golpistas utilizavam truques, histórias inventadas e falsas identidades para obter a confiança das pessoas e, assim, realizar fraudes financeiras ou outros tipos de crimes.
Com o avanço da tecnologia da informação e a popularização da internet, a **Engenharia Social migrou para o ambiente digital**. Através de e-mails fraudulentos, chamados de *phishing*, ou de mensagens em redes sociais, os cibercriminosos tentam enganar os usuários, levando-os a revelar informações pessoais, senhas ou a executar ações prejudiciais.
A história da Engenharia Social está repleta de exemplos marcantes. Um caso famoso é o **"Ataque do Cavalo de Troia" da Guerra de Troia**, descrito na mitologia grega. Os gregos conseguiram entrar na cidade de Troia enviando um grande cavalo de madeira como um presente, enquanto estavam soldados em seu interior.
Atualmente, a Engenharia Social continua a evoluir e se adaptar às circunstâncias. Os cibercriminosos usam técnicas cada vez mais sofisticadas, como Engenharia Social baseada em informações obtidas de mídias sociais, Engenharia Social reversa em que eles estudam os padrões de comportamento de uma pessoa ou organização antes de lançar um ataque, e **Engenharia Social de voz**, na qual se utilizam técnicas de manipulação vocal em chamadas telefônicas.

A defesa contra a Engenharia Social envolve a conscientização e o treinamento dos usuários, bem como a implementação de medidas de segurança, como autenticação em dois fatores e políticas de privacidade e segurança rigorosas. Em resumo, tem uma longa história e se adaptou ao longo do tempo, enquanto se adaptava aos avanços tecnológicos. A conscientização sobre as técnicas utilizadas pelos engenheiros sociais e a adoção de medidas de segurança adequadas são fundamentais para se proteger contra esses ataques.

Geralmente, a pessoa que sofre o ataque se sente tão à vontade que, sem perceber, rompe o sigilo e confidencialidade anteriormente confiadas e entrega diversas informações sigilosas ou deixa a "porta aberta" para este indivíduo.
Abaixo, você verá um **simples exemplo do uso da Engenharia Social** que, provavelmente, você já deve ter presenciado algo parecido no seu dia a dia.

Exemplo:
Um número desconhecido liga para a vítima. Do outro lado da linha, um simpático atendente a parabeniza com a notícia que foi premiada com carro 0km, e que para resgatar, precisa "confirmar" alguns dados como CPF, RG, endereço e, por fim, solicita ao ganhador um depósito de determinado valor em uma conta bancária. A pessoa, ingênua e acreditando em suas palavras, passa todos os seus dados pessoais e ainda realiza a transferência.

Percebeu que a Engenharia Social não é algo novo? Esta técnica possui várias vertentes e na grande maioria das vezes, é feita de maneira imperceptível.

Partindo para o contexto da Segurança da Informação e os ataques cibernéticos, a Engenharia Social é empregada em vários crimes digitais, e sempre com os mesmos atributos: ter o poder da persuasão e garantir a confiança do usuário. A diferença para os ataques que não se utilizam da Engenharia social, é que estes atingem o objetivo criminoso sem a necessidade da interação humana, enquanto os ataques que envolvem esta técnica persuadem a vítima para que passe os dados e informações por livre e espontânea vontade.

Emoções
Todo ser humano apresenta "gatilhos" psicológicos que são acionados em determinadas situações e podem deixá-lo vulnerável e aberto para expor algo confidencial. São estes gatilhos que os atacantes se aproveitam para conseguir o que querem. Conforme dito anteriormente, as vítimas demoram para desconfiar da situação de perigo que está inserida. O atacante, capacitado em Engenharia Social, utiliza do emocional das pessoas e pode criar cenários baseados neles para garantir o sucesso.

Tipos de ataques cibernéticos envolvendo Engenharia Social

Phishing
É um dos ataques mais populares hoje em dia. A tradução remete a "**pescaria**", ou seja, é arquitetado um ambiente para que **as vítimas "comam a isca" e se sintam confiantes**. O *phishing* apresenta diversas variações que veremos a seguir. A mais comum é aplicada pelo envio em massa de e-mails, com mensagens fortes e que chamam a atenção da vítima, normalmente para resolução imediata. De modo geral, os *phishings* tem como objetivo usar as métricas da Engenharia Social para persuadir e conseguir a confiança da vítima através de um contato que é ambientado para parecer autêntico. Normalmente, neste contato haverá **formulários, confirmação de dados cadastrais, links, solicitações de instalação de softwares entre outros**. A inocência, falta de atenção aos detalhes e a confiança são as metas que a Engenharia Social almeja para ter sucesso no ataque.

Smishing
O ***smishing*** é uma variante do *phishing*, que utiliza **aplicativos mensageiros e SMS** para se propagarem. De modo geral, são baseados em **mensagens de texto impactantes com um link malicioso encurtado**. A recomendação é de não clicar em nenhum tipo de link vindo de SMS de números desconhecidos e checar a veracidade da mensagem por outros meios.

Phishing de sites

Neste tipo de *phishing*, o ambiente malicioso está caracterizado como um site de bancos, escolas e até mesmo de redes sociais, no qual, o usuário realmente acredita estar em um ambiente seguro.

Veja abaixo este exemplo:

Aparentemente é a página inicial da rede social Facebook, não é mesmo? Agora, observe bem na url do site. O que é para ser https://www.facebook.com, é outro link completamente diferente e que mal utiliza o domínio. Esta é uma amostra do *phishing* de sites. Uma cópia muito fiel a página original, pronta para roubar seu usuário e senha.

Pretexting

O ***pretexting*, ou pretexto**, é um tipo de ataque que prepara uma relação com a vítima para que se sinta à vontade com ele. Essas relações, via de regra, são criadas no momento do golpe, no qual o **atacante finge ser alguém do ciclo social dessa vítima ou alguém que denota uma superioridade**.
O criminoso pode vestir várias "carapuças". Isso pode acontecer tanto pessoalmente, quanto por telefonemas e e-mails. Exemplificando, o atacante pode fingir ser um novo colega de trabalho e pedir ajuda em algum procedimento de acesso ao computador, se passar por um superior na empresa, solicitar dados confidenciais e até mesmo se vestir como um agente público, como um policial ou bombeiro e exigir entrar em algum setor, pressionando a vítima a aceitar imediatamente.

Quid Pro Quo

Partindo da tradução livre "**algo por algo**", o método *Quid Pro Quo* é baseado em uma premissa: "**Se você fizer algo por mim, farei algo para você**". Basicamente, o atacante virá com a pretensão de ajudar ou dar algum tipo de assistência à vítima e tudo o que ele precisa são de alguns dados ou informações para que isso seja feito.

Para ilustrar, em nosso cotidiano, você já pode ter presenciado algum suposto técnico de alguma operadora ou colega de trabalho que **pede acesso remoto ao seu computador ou desativar o antivírus**, na premissa de realizar algum tipo de reparo. Pode acontecer também do criminoso **pedir algum tipo de credencial de recursos crítico**s que, em mãos erradas, pode comprometer todo o ambiente pelo roubo ou exclusão de dados.

Baiting

Esta técnica de "isca" vai abusar da curiosidade da vítima. Um dos exemplos mais comuns para exemplificar o *baiting* é a **pessoa mal-intencionada deixar um dispositivo de mídia, como um pendrive, CD, ou HD propositalmente em algum local**, seja público ou privado. Uma hora ou outra, alguém verá aquele dispositivo no chão e se sentirá atraída a pegá-lo e **ver o que tem dentro**. Nestas mídias, haverá softwares maliciosos como malwares só esperando o "curioso" inserir o dispositivo em sua máquina ou no computador da empresa para infectar a rede ou conceder acesso total a seus arquivos e documentos confidenciais.

Como evitar ataques envolvendo Engenharia Social?

Para evitar ataques envolvendo engenharia social, é importante adotar algumas práticas e medidas de segurança.

Aqui estão algumas orientações:

- **Conscientização e treinamento**: Eduque-se e conscientize-se sobre os diferentes tipos de ataques de Engenharia Social, suas técnicas e os sinais de alerta. Participe de treinamentos e workshops para entender melhor como identificar e lidar com esses ataques.
- **Desconfie de solicitações não solicitadas**: Esteja atento a solicitações de informações pessoais ou confidenciais, especialmente quando forem inesperadas ou originadas de fontes não confiáveis. Nunca forneça informações sensíveis por e-mail, telefone ou mídias sociais, a menos que possa verificar a autenticidade do solicitante.
- **Valide a identidade**: Sempre que receber uma solicitação de informações ou ação, cheque a identidade da pessoa ou organização envolvida. Entre em contato diretamente com a pessoa ou empresa, e use informações de contato confiáveis, para confirmar se a solicitação é legítima.
- **Esteja atento a redirecionamentos de URL**: Ao clicar em links recebidos por e-mail ou mídias sociais, apure cuidadosamente o URL antes de inserir informações confidenciais. Certifique-se de que o site seja legítimo e seguro. Evite clicar em links suspeitos ou desconhecidos.
- **Fortaleça as senhas**: Utilize senhas fortes e exclusivas para cada conta. Evite senhas óbvias ou fáceis de adivinhar. Considere o uso de gerenciadores de senhas para criar e armazenar senhas complexas de forma segura.
- **Mantenha os softwares atualizados**: Mantenha seu sistema operacional, aplicativos e programas antivírus atualizados. As atualizações geralmente incluem correções de segurança que ajudam a proteger contra ameaças conhecidas.
- **Cuidado com informações compartilhadas nas mídias sociais**: Seja cauteloso ao compartilhar informações pessoais ou detalhes sobre sua vida pessoal nas mídias sociais. As informações publicamente disponíveis podem ser usadas por atacantes para criar perfis falsos ou personalizar ataques de engenharia social.
- **Esteja atento a solicitações de ajuda financeira ou urgência**: Fique ligado a solicitações de transferências de dinheiro, doações ou pedidos de urgência que não possam ser verificados. Sempre confirme a autenticidade de tais solicitações antes de agir.
- **Mantenha um ambiente de trabalho seguro**: Em ambientes profissionais, seja cauteloso ao compartilhar informações sensíveis, especialmente com pessoas que não estão autorizadas a acessá-las. Não deixe dispositivos eletrônicos desbloqueados ou informações confidenciais à vista.

● **Relate incidentes suspeitos**: Se suspeitar de um ataque de Engenharia Social ou identificar atividades suspeitas, relate imediatamente ao departamento de segurança da informação ou equipe responsável pela segurança da sua organização.

Lembre-se de que a **Segurança da Informação é um esforço contínuo e envolve tanto aspectos técnicos quanto comportamentais**. Ficar atualizado sobre as últimas técnicas de engenharia social e adotar medidas de prevenção adequadas são essenciais para se proteger contra esses ataques.

RESUMO

A necessidade de permanecermos em constante estado de vigilância em relação a novas variantes de fraudes em Engenharia Social é incontestável. A **Engenharia Social refere-se a um conjunto de técnicas que se concentram na exploração de aspectos humanos para influenciar o comportamento de indivíduos, manipulando-os a realizar ações ou divulgar informações que não deveriam**. Em outras palavras, esses ataques têm como objetivo principal a alteração psicológica do alvo.

As táticas empregadas pelos fraudadores em engenharia social são sutis e engenhosas. Eles usam **várias estratégias de persuasão para convencer suas vítimas a revelar, de maneira voluntária, suas informações pessoais e sensíveis**. Isso pode incluir detalhes como senhas, informações bancárias, dados de cartões de crédito, entre outros. De fato, o mais alarmante é que muitas vítimas não percebem que suas informações foram comprometidas até que seja tarde demais.

Frequentemente, os ataques de Engenharia Social são tão bem orquestrados que a vítima, sem sequer perceber, acaba sendo conduzida a acreditar que a divulgação dessas informações confidenciais é de seu próprio interesse. Deste modo, muitas vezes, as vítimas nem sequer têm consciência de que estão caindo em uma armadilha.

Assim, é de **suma importância que continuemos vigilantes, educando-nos e a outros sobre a natureza desses ataques e como podemos nos proteger deles**. Em um mundo cada vez mais conectado, a emergência de novas estratégias de Engenharia Social é inevitável. Portanto, é crucial reconhecer as maneiras pelas quais esses golpes podem ocorrer, e tomar medidas proativas para se proteger contra esses tipos de fraudes.

ATIVIDADES

1. O que é Engenharia Social?

Engenharia Social é uma prática que envolve a manipulação psicológica de pessoas para obter informações confidenciais ou realizar ações que comprometam a segurança, geralmente por meio do abuso da confiança, ignorância, ou ingenuidade da vítima.

2. Qual é o objetivo principal da Engenharia Social?

O objetivo principal da Engenharia Social é obter informações confidenciais, como senhas, dados bancários, ou outros detalhes sensíveis, ou fazer com que a vítima realize ações que comprometam a segurança, como instalar um software malicioso ou fornecer acesso a sistemas protegidos.

3. Cite três exemplos comuns de técnicas de Engenharia Social.

- Phishing: Envio de e-mails falsos que parecem ser de fontes confiáveis para induzir a vítima a fornecer informações pessoais ou clicar em links maliciosos.
- Pretexting: O atacante cria um pretexto ou uma falsa identidade para enganar a vítima e obter informações confidenciais.

- Baiting: Uso de iscas, como pendrives ou CDs infectados deixados em locais públicos, para atrair a curiosidade da vítima e induzi-la a inserir o dispositivo em seu computador, espalhando malware.

4. Explique a importância da conscientização e treinamento dos usuários para prevenir ataques cibernéticos. Como essas práticas podem fortalecer a segurança da informação de uma organização?

Conscientização e treinamento são essenciais para capacitar os usuários a identificar e evitar ataques de Engenharia Social. Quando os funcionários são bem informados sobre as táticas que os cibercriminosos usam, eles estão mais preparados para reconhecer tentativas de fraude e evitar ações que possam comprometer a segurança da organização. Esses treinamentos também reforçam a importância de práticas seguras, como o uso de autenticação multifator, verificação de identidade, e a atenção aos sinais de phishing. Coletivamente, essas medidas ajudam a criar uma cultura de segurança dentro da organização, onde os funcionários se tornam a primeira linha de defesa contra ataques cibernéticos.

5. Discuta a importância de validar a identidade de um solicitante antes de fornecer informações confidenciais. Cite três métodos que podem ser usados para verificar a autenticidade de uma solicitação.

Validar a identidade de um solicitante é crucial para prevenir que informações confidenciais sejam entregues a cibercriminosos. Isso evita que atacantes, usando técnicas como pretexting ou phishing, enganem os funcionários e comprometam a segurança da organização.

Três métodos para verificar a autenticidade de uma solicitação incluem:

- Contato direto: Entre em contato diretamente com a pessoa ou organização, usando informações de contato confiáveis que você já possui, para confirmar se a solicitação é legítima.
- Autenticação em dois fatores: Exija que o solicitante passe por um processo de autenticação adicional, como um código enviado para o telefone ou e-mail, antes de fornecer qualquer informação.
- Verificação de credenciais: Peça ao solicitante para fornecer credenciais ou documentos que comprovem sua identidade e a validade da solicitação, especialmente se for alguém que você não conhece pessoalmente.