ENGENHARIA SOCIAL

GUIA PARA PROTEÇÃO DE CONHECIMENTOS SENSÍVEIS

PNPC

PROGRAMA NACIONAL DE PROTEÇÃO DO CONHECIMENTO SENSÍVEL

APRESENTAÇÃO

Instituições nacionais, públicas ou privadas, são alvo constante de ações de engenharia social, método que busca acesso de forma dissimulada a informações sensíveis e não disponíveis.

Esta cartilha tem o objetivo de dificultar esse tipo de ação e foi elaborada pelo Programa Nacional de Proteção do Conhecimento Sensível (PNPC), desenvolvido pela Agência Brasileira de Inteligência (ABIN).


ENGENHARIA
SOCIAL

O que é engenharia social?

A **engenharia social** é um método usado para enganar, manipular ou explorar a confiança das pessoas. É uma forma não violenta de ataque que busca fazer com que a vítima realize voluntariamente ações prejudiciais a si mesma, como divulgar informações sensíveis ou transferir dinheiro para desconhecidos.

Uma ação de engenharia social pode se dar em um **contexto pessoal**, para obter informações sobre você, ou em um **contexto profissional**, para conseguir informações sobre sua instituição.

Quem é o engenheiro social?

A engenharia social pode ser utilizada por qualquer pessoa que tenha interesse em suas informações, como **serviços de inteligência** de Estados nacionais e **hackers** amadores, todos utilizam com maior ou menor grau de sofisticação técnicas de engenharia social.

Algumas pessoas fazem isso naturalmente: um vendedor de uma **empresa concorrente** pode conseguir muitas informações em um bate-papo com um fornecedor, sem que nunca tenha nem ouvido a expressão engenharia social.

Por quais canais a engenharia social pode ocorrer?

Qualquer forma de interação pode ser um canal para o engenheiro social realizar sua ação: pessoalmente, por telefone, por e-mail ou até por meio de redes sociais.

Por que a engenharia social funciona?

A engenharia social é uma técnica efetiva porque explora fragilidades do funcionamento da mente humana. No dia a dia, a maioria de nossas atividades é realizada de forma automática, rápida, sem que precisemos parar para raciocinar muito a respeito.

Temos uma espécie de modelo mental de como as situações acontecem. O engenheiro social sabe que, se ele conseguir manipular uma situação de forma que ela se enquadre no nosso modelo mental, provavelmente não vamos parar para refletir a respeito do que estamos fazendo.

Se um engenheiro social se apresentar como técnico de TI e utilizar um padrão de linguagem fora de nossa expectativa, vamos desconfiar de que se trata de um impostor. Mas, se o seu comportamento corresponder ao que esperamos, provavelmente não vamos parar para pensar a respeito.

Quais fragilidades o engenheiro social pode explorar?

O engenheiro social sabe que, quando temos uma **pressão de tempo**, a probabilidade de refletirmos é muito menor. Assim, é comum que ele explore supostas situações com prazos curtos ("tenho uma oferta de emprego, mas preciso que você complete a ficha ainda hoje") ou urgentes ("atualize seu aplicativo agora ou ficará sem acesso a sua conta bancária").

Ele também sabe que a **pressão de autoridade** é muito eficiente, principalmente em organizações mais hierarquizadas ("sou a secretária do Diretor Fulano e ele precisa de uma informação agora para tomar uma decisão").

Outra característica que ele pode explorar é nossa **empatia**, principalmente nossa disposição para ajudar, criando uma narrativa cuja recusa nos cause um sentimento de culpa. O engenheiro social pode, por exemplo, ressaltar como a falta daquela informação pode custar o emprego dele.


ENTREVISTA

O que é entrevista?

Entrevista é uma técnica da engenharia social que também busca informações que não estaríamos dispostos a fornecer. O engenheiro social consegue isso manipulando o fluxo da conversa. Sem perceber, podemos passar a informação para o engenheiro social sem que ele nem ao menos tenha que perguntá-la.

Técnicas de entrevista:

- **Pedir ajuda:** em vez de perguntar a informação, a pessoa pode pedir ajuda para resolver um problema no qual ela se encaixe.
- **Criticar para que você defenda algo:** a pessoa pode falar mal da sua instituição para receber as informações que você usará como argumento.
- **Errar para ser corrigido:** a pessoa pode compartilhar uma informação que sabe ser incorreta para que você a corrija com a informação que ela deseja.
- **Fingir que já sabe a informação:** a pessoa pode dar a entender que já sabe o que você está relutante em contar para que a conversa continue fluindo e você acabe por confirmá-lo.
- **Contar algo parecido ou aparentemente sigiloso:** o engenheiro pode fornecer uma informação para que nós fiquemos mais propensos a fornecer informações em troca, despertando nossa tendência por reciprocidade.

Qual o objetivo do engenheiro social no ambiente virtual?

A engenharia social é uma técnica básica no arsenal dos hackers e de Estados nacionais devido a sua eficiência, principalmente para se obter um ponto de entrada no sistema de informações de uma instituição.

O engenheiro social pode nos ludibriar, levando-nos a abrir um **anexo** contendo um malware ou nos fazendo clicar em um **link** malicioso, permitindo que invada um sistema.

Mesmo que não tenhamos os acessos internos que o hacker deseja, depois dessa primeira porta aberta, ele tentará aumentar seus privilégios e explorará novas vulnerabilidades.


PHISHING

Qual a diferença entre *Phishing* e *Spearphishing*?

Phishing ocorre quando recebemos um **e-mail genérico** com um golpe. O phishing é como pescar com uma rede: a mensagem é enviada para o maior número de pessoas possível. Mesmo que uma proporção pequena dos peixes caia na rede, o número de vítimas já será suficiente para que o criminoso atinja seu objetivo.

Spearphishing seria como uma pesca de arpão. É uma ação muito **bem direcionada**. Um e-mail de *spearphishing* utiliza os elementos da engenharia social, como um assunto que seja atrativo e informações específicas sobre você e sua instituição.


PROTEÇÃO

Como evitar essas ações?

1. Desconfie

Se você não desconfiar, não irá parar para pensar no que está fazendo e não exigirá comprovação, clicará em anexos e passará voluntariamente informações que não deveriam ser partilhadas.

2. Verifique

Como você sabe que alguém que está falando com você é realmente quem ele diz ser? Exija uma comprovação. Desconfie de todos os pedidos de informação de pessoas que você não conheça pessoalmente.

3. Desapegue do "abrir por hábito"

No caso de e-mails, você realmente precisa abrir o anexo ou link de uma mensagem? Muitas vezes, apenas por hábito, abrimos documentos desnecessariamente. Tenha consciência de que todos os anexos são potenciais fontes de contaminação de seu sistema de informações.

4. Limite informações

Você poderá dificultar o planejamento do engenheiro social limitando as informações disponíveis em suas redes sociais, como no LinkedIn e no Instagram.

5. Saiba o que pode ser compartilhado

Delimite de antemão quais são as informações sobre você ou sobre sua instituição que não podem ser compartilhadas. Assim, pode-se tentar desviar o assunto ou negar explicitamente as informações solicitadas com respostas como "não tenho conhecimento" ou "isso eu não posso comentar".

6. Alerte a segurança

Ao desconfiar de ter sido vítima de uma ação de engenharia social direcionada, alerte sua chefia e o setor de segurança de sua instituição.

Você também pode enviar um e-mail para **reporte@abin.gov.br** para informar sobre o caso.

PROTEGER COM INTELIGÊNCIA

pnpc@abin.gov.br

www.gov.br/abin/pnpc