ENGENHARIA SOCIAL

GUIA PARA PROTEÇÃO DE CONHECIMENTOS SENSÍVEIS

PNPC

PROGRAMA NACIONAL
DE PROTEÇÃO DO
CONHECIMENTO SENSÍVEL

Engenharia social

Guia para Proteção de Conhecimentos Sensíveis

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Produção
Departamento de Contrainteligência
Programa Nacional de Proteção do Conhecimento Sensível (PNPC)

Projeto Gráfico
Coordenação-Geral de Relações Institucionais e Comunicação
Divisão de Serviços Gráficos

Impressão
Divisão de Serviços Gráficos

2021

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).

Criado em 1997, o PNPC é uma assessoria de segurança que busca promover uma cultura de proteção de conhecimentos sensíveis em instituições nacionais com foco na prevenção de ameaças como espionagem, sabotagem e vazamento de informações.

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 de ataque sem violência física que busca fazer com que a vítima realize voluntariamente ações prejudiciais a si mesma, como divulgar informações sensíveis ou transferir dinheiro para desconhecidos.

Quando alguém convence uma pessoa a divulgar sua senha, está realizando uma ação de engenharia social. Se alguém obriga uma pessoa a dar sua senha sob ameaça de violência, isso não é engenharia social.

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 é uma técnica que tem se tornado cada vez mais comum e pode ser utilizada por qualquer pessoa que tenha interesse em suas informações. Desde **serviços de inteligência** de Estados nacionais até **hackers** amadores, todos utilizam com maior ou menor grau de sofisticação técnicas de engenharia social.

Um serviço de inteligência poderá conseguir mais informações prévias para que a ação seja mais efetiva, porém, talvez, um hacker com menos recursos atinja o mesmo objetivo enviando um e-mail com link malicioso, por exemplo.

Não é preciso ter anos de formação para realizar uma ação 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. Isso é chamado por psicólogos de **Sistema Rápido** ou **Sistema 1** de pensamento. Quando paramos para raciocinar a respeito do que fazemos, estamos acionando nosso **Sistema Lento** ou **Sistema 2**.

Se a situação que estamos enfrentando se encaixa em algo que estamos acostumados a fazer, dificilmente paramos para pensar a respeito. Porém, se há algum estranhamento, se desconfiamos de algo, então, engajamos nosso Sistema Lento para analisar melhor a situação.

Temos uma espécie de modelo mental de como as situações acontecem, principalmente as que ocorrem todos os dias. 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 pensar a respeito do que estamos fazendo.

Como assim?

Frequentemente, precisamos chamar o suporte de tecnologia para resolver problemas em nossas máquinas. Esperamos que eles se comportem de uma forma e que eles utilizem certa linguagem.

Se um engenheiro social se apresentar como técnico de TI e utilizar um padrão de linguagem fora dessa nossa

expectativa, vamos desconfiar de que se trata de um impostor. Mas, se o seu comportamento corresponder ao que esperamos de um profissional do suporte, provavelmente não vamos acionar nosso Sistema Lento. Assim, o falsário poderá pedir nossa senha e não iremos refletir se devemos fornecê-la ou não.

Quais fragilidades o engenheiro social pode explorar?

O engenheiro social sabe que, quando temos uma **pressão de tempo**, a probabilidade de utilizarmos nosso Sistema Lento 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. Ele pode criar uma narrativa para incentivar a vontade de auxiliá-lo. Ao mesmo tempo, ele manipulará a situação de forma que ajudar seja a resposta natural e que recusar nos cause um sentimento de culpa.

O engenheiro social pode, por exemplo, ressaltar como a falta daquela informação pode custar o emprego dele. Dessa forma, passar uma informação comentada cotidianamente entre funcionários da sua instituição não teria um custo psicológico alto para você, enquanto não a fornecer ocasionaria peso na consciência.

ENTREVISTA

O que é entrevista?

Entrevista é uma técnica da engenharia social que também busca informações que não estaríamos dispostos a fornecer. Diferentemente de outras técnicas de engenharia social, a entrevista não necessariamente envolve o desenvolvimento de uma narrativa falsa. Nós não precisamos ser enganados em uma ação de entrevista. Nós forneceremos as informações por nossa própria vontade.

O engenheiro social consegue isso **manipulando** o fluxo da conversa. Ele pode nos encontrar, por exemplo, em um congresso profissional e puxar papo sobre alguma amenidade. A partir daí, ele irá nos guiando de forma a levar a conversa para onde tem interesse. De um assunto, ele puxará outro, que usará como gancho para o próximo e assim por diante. Tudo de forma o mais natural possível, sem chamar nossa atenção. Sem perceber, provavelmente vamos passar a informação para o engenheiro social sem que ele nem ao menos tenha que perguntá-la.

Após conseguir a informação, o engenheiro social normalmente não finalizará a conversa de forma abrupta, para não levantar suspeita. Ao terminar, ele estará contente por ter conseguido a informação e nós por termos mantido uma agradável conversa, já que não desconfiamos do que realmente ocorreu.

Técnicas utilizadas na entrevista:

• **Pedir ajuda:** em vez de perguntar a informação diretamente, a pessoa pode pedir ajuda para resolver um problema no qual a informação 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, por exemplo.

• **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 confirmar a informação.

• **Contar algo parecido ou aparentemente sigiloso:** o engenheiro pode fornecer uma informação para que nós, inconscientemente, fiquemos mais propensos a também fornecer informações em troca. Essa técnica tem por objetivo despertar nossa tendência por reciprocidade.

Qual o objetivo do engenheiro social no ambiente virtual?

A engenharia social é uma técnica básica no arsenal dos hackers, mas também de atores mais sofisticados, como Estados nacionais, devido a sua eficiência. Utiliza-se a engenharia social 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 que permitirá um primeiro acesso ao sistema. Também pode nos fazer clicar em um **link** malicioso, permitindo que ele 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. Por isso, não podemos subestimar nossa probabilidade de ser alvo porque nossos acessos são limitados. Qualquer pessoa com acesso a um sistema de informação pode ser uma porta de entrada a ser explorada.

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

Phishing é aquela forma de engenharia social que todos nós já sofremos quando recebemos um e-mail **genérico** com alguma forma de golpe. Um ataque famoso é aquele do príncipe nigeriano que tem uma herança para receber e precisa justamente de nossa ajuda.

O *phishing* é como pescar com uma rede: a rede é jogada na maior área possível. No caso, 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, por outro lado, seria como uma pesca de arpão. É uma ação muito **bem direcionada**. Um e-mail de *spearphishing* utiliza os elementos da engenharia social já apresentados. Ele será direcionado a você. Utilizará um assunto que seja atrativo para você. Buscará informações específicas sobre você e sua instituição. Tentará se encaixar no seu esquema mental.

Se a eficiência do *phishing* normal é muito baixa, mas compensada pelo grande número de pessoas que recebem o e-mail, o *spearphiphing* é muito mais eficiente. Alguns ataques chegam a ter mais de 90% de sucesso.

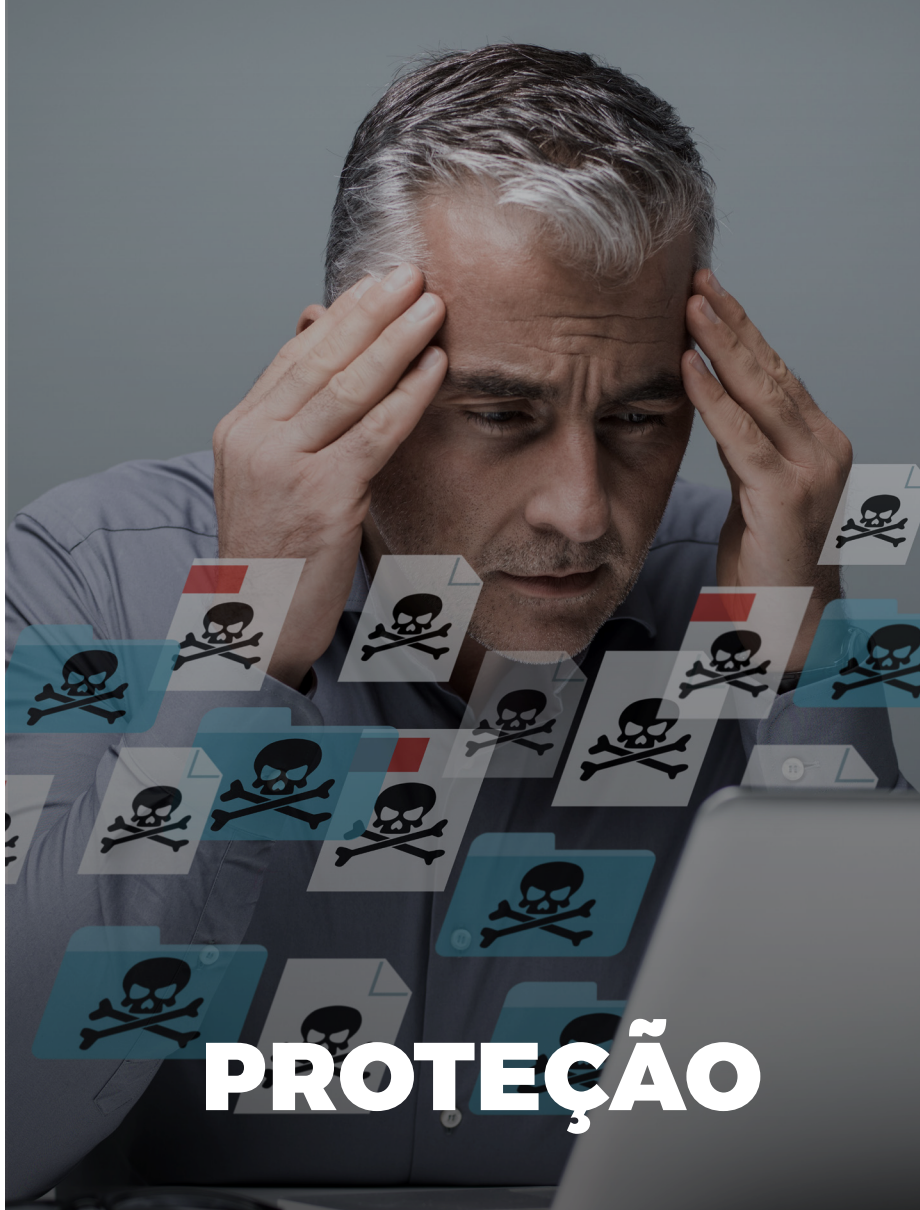
Imagine que você participará de um congresso em algumas semanas e que você receba um e-mail supostamente da organização do evento pedindo seus dados para agilizar o processo de credenciamento. Há mais chances de você acreditar na veracidade do e-mail do que em situações mais genéricas.

Como o engenheiro social planeja sua ação?

O engenheiro social planeja sua ação primeiro identificando sua vítima. Quem tem acesso à informação de que ele precisa? Quem pode ser a porta de entrada para um sistema?

Ele se comporta de forma a não levantar suspeitas, procurando, por exemplo, informações específicas sobra a instituição alvo, como siglas, nomes e cargos.

Depois, ele busca a forma mais simples de obter as informações que necessita. O que pode ocorrer pessoalmente, por e-mail, por telefone ou até pelas redes sociais.



Como evitar essas ações?

1. Desconfie
A principal forma de evitar é desconfiar. Se você não desconfiar, não irá parar para pensar no que está fazendo e não exigirá comprovação, clicará em anexos e links, 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. Uma forma simples é ligar de volta. Alguém que você não conhece está dizendo que é do setor de Recursos Humanos? Invente uma desculpa e retorne a ligação no ramal que você tem certeza que é do RH. Claro, não utilize o contato que o próprio interlocutor lhe passou. 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 de uma mensagem? Muitas vezes, apenas por hábito, abrimos documentos desnecessariamente. Aquele e-mail com uma nota fiscal de um estacionamento que você utilizou ontem, você realmente precisa abrir?

Um anexo em um e-mail de um potencial cliente com quem você nunca teve contato: você precisa abrir neste momento?

Tenha consciência de que todos os anexos são potenciais fontes de contaminação de seu sistema de informações. Acione seu Sistema Lento sempre que precisar decidir entre abrir ou não um anexo.

4. Evite links
Isso também vale para links recebidos por e-mail ou por redes sociais. Você precisa entrar naquela página por meio do link? Você não consegue chegar à mesma página diretamente, navegando pelo site? Todo link é um risco.

5. Limite informações
Você poderá dificultar o planejamento do engenheiro social limitando as informações disponíveis. O engenheiro social pode descobrir no LinkedIn que você é o chefe do setor de Recursos Humanos e, no Instagram, que você está viajando atualmente em um resort.

Com essas informações, ele pode ligar para o RH na sua ausência e citar que havia falado com você antes de sua partida e que deveria enviar um currículo em um anexo de e-mail para determinada pessoa da empresa. Você acha que o destinatário da men-

sagem abriria o anexo nesse caso?

6. Saiba o que pode ser compartilhado

Delimite de antemão quais são as informações sobre você ou sobre sua instituição que não podem ser compartilhadas. Tendo esse parâmetro, é possível perceber melhor quando uma conversa está sendo direcionada para assuntos mais sensíveis.

Nesse caso, pode-se tentar desviar o assunto ou negar explicitamente as informações solicitadas com respostas como "não tenho conhecimento" ou "isso eu não posso comentar".

7. 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. Outras pessoas também podem ter sido vítimas da mesma ação e podem não ter a mesma perspicácia que você. Afinal, basta que uma pessoa aja sem pensar para que o engenheiro social obtenha informações sensíveis de sua instituição.

Você também pode enviar um e-mail para **reporte@abin.gov.br** se desconfiar que você ou sua empresa/instituição foram alvos de engenheiros sociais.

PNPC

PROTEGER COM INTELIGÊNCIA

pnpc@abin.gov.br
www.gov.br/abin/pnpc

GABINETE DE
SEGURANÇA INSTITUCIONAL

PÁTRIA AMADA
BRASIL
GOVERNO FEDERAL