Prime

CCS-A

Engenharia Social

O que é Engenharia Social?

- Método de usar pessoas como parte de um processo de ataque cibernético.
- É uma das etapas do ataque. Normalmente a primeira.
- É um ponto de partida para o ataques contra os componentes do computador ou sistema.

Métodos de Engenharia Social

O que a Engenharia Social exige?

Interação social. Não precisa ser de conhecimento técnico de segurança

O que a Engenharia Social envolve?

Manipulação da própria natureza social das relações entre seres humanos.

Primeiro Método – Vontade de Ajudar

Uma característica que gostaríamos de ver em um ambiente de equipe;

Tendemos a recompensar com a ajuda!

Táticas sutis na Engenharia Social exploram:

- Cultura de colaboração;
- Trabalho em equipe;
  - Com as palavras certas;
  - Com informações corretas.
- Confiança das pessoas.

Segundo Método – Criando um Situação Hostil

- **O que envolve o segundo método da Engenharia Social?**

  Evitar a hostilidade e empatia com o atacante.

- **O que o engenheiro social utiliza?**

  Simpatia das pessoas;

  Desejo de compaixão.

Características Marcantes da Engenharia Social

- **Um bom engenheiro social usa:**
  - Linguagem corporal para influenciar os outros;
  - Estereótipos.
- **Melhor defesa contra engenharia social:**
  - Treinamento;
  - Conscientização.

Ferramentas da Engenharia Social

Qual é a principal ferramenta de um engenheiro social?

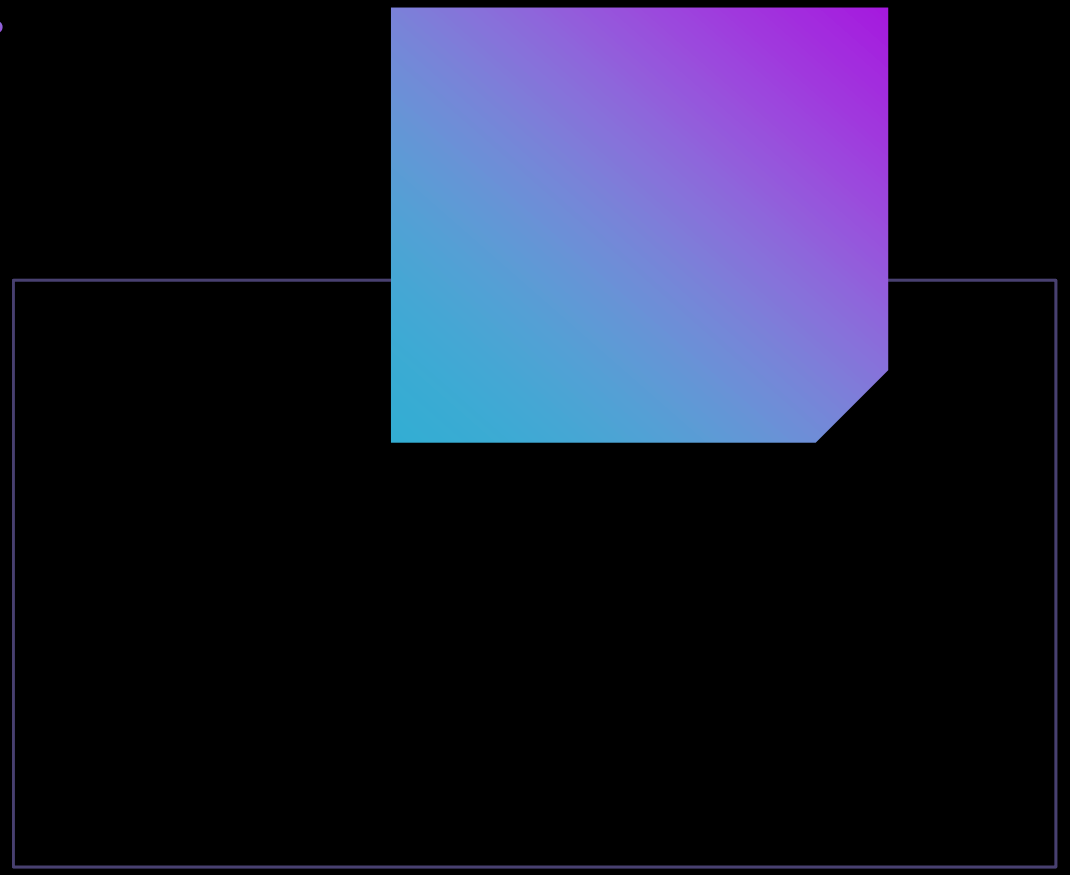
Ψ | Psicologia.

Qual é a importância de saber empregar as ferramentas para um engenheiro social?

Um bom engenheiro social sabe como ativar e desativar essas ferramentas.

É possível enxergar essas ferramentas?

Sim, no momento em que vemos os engenheiros sociais atuando.



Phishing

- Invasor que tenta obter informações confidenciais de usuários.
- Como o engenheiro social faz isso?
  - Disfarçando-se de alguém confiável em uma mensagem enviada a um grande grupo de usuários geralmente aleatórios.
- O invasor tenta obter informações como:

Nomes do usuário;

Senhas;

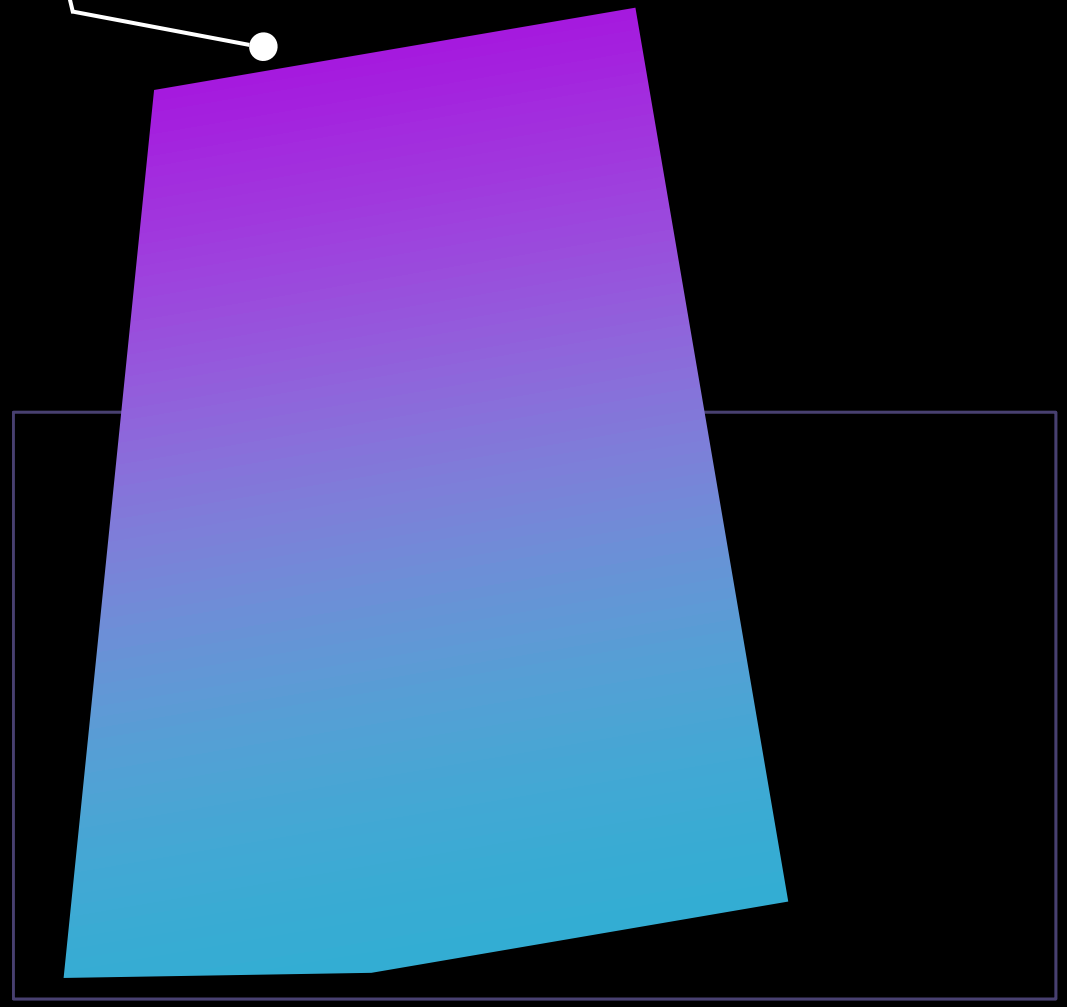
Números de cartão de crédito;

Detalhes sobre as contas bancárias.

- O *phishing* é muito adotado por engenheiros sociais?
  - Sim, esse é o tipo de ataque mais comum em Engenharia Social.

Smishing

- Ataque usando o **Short Message Service (SMS)** nos telefones celulares das vítimas.
- Como esse ataque ocorre?
  - Uso de urgência;
  - Ameaça (Se não cancelar o serviço XYZ, acarretará em uma cobrança X).



Vishing

- Variação do *phishing* que usa a tecnologia de comunicação de voz para obter as informações que o invasor está procurando.
- Essa tática é usada para:
  - Estabelecer uma relação de confiança e facilitar possíveis ataques.
  - Não há como confirmar se estão simulando a ligação.
- Em resumo, são ataques contra o estado cognitivo dos usuários (morder a isca):

Phishing;

Smishing;

Vishing.

Spam

- E-mail não solicitado, geralmente enviado em massa.
- O spam pode:
  - Ser legítimo;
  - Ter sido enviado por uma empresa para anunciar um produto.
- Cuidados com o spam:
  - Considerar a fonte antes de clicar em qualquer link ou responder diretamente.
- O spam altera o comportamento humano:
  - Convence usuários a clicarem em links suspeitos.

Spam Sobre Mensagens Instantâneas (SPIM)

- Uma variação do spam.
- Entregue por meio de um app de mensagens instantâneas.

OBJETIVOS:
Fazer com que um usuário desavisado clique em conteúdo ou links maliciosos, iniciando assim o ataque.

Spear Phishing

Tipo específico de *Phishing*, mais direcionado e não aleatório;

É um ataque bem-sucedido, pois parece mais plausível.

ALVOS:

- Uma pessoa ou grupo específico de pessoas com algo em comum;
- Executivos seniores.

Dumpster Diving

O processo de vasculhar o lixo.

- Busca encontrar:
  - Informações valiosas que possam ser usadas em uma tentativa de penetração.
- Por que vasculhar o lixo:
  - Lixos não são mais considerados propriedade privada e contém informações descartadas importantes.
- Medida de proteção:
  - As informações confidenciais devem ser trituradas e a organização deve considerar proteger a lixeira para que os indivíduos não possam mexer nela.

Shoulder Surfing

- Não envolve necessariamente contato direto com o alvo.
- O invasor observa diretamente o indivíduo inserindo informações confidenciais em um formulário ou teclado.
- O invasor pode tentar obter informações como:
  - Senha ou qualquer número de identificação pessoal (PIN) em um caixa eletrônico;
  - Código de acesso de entrada a uma porta segura;
  - Número de cartão de crédito.

Pharming

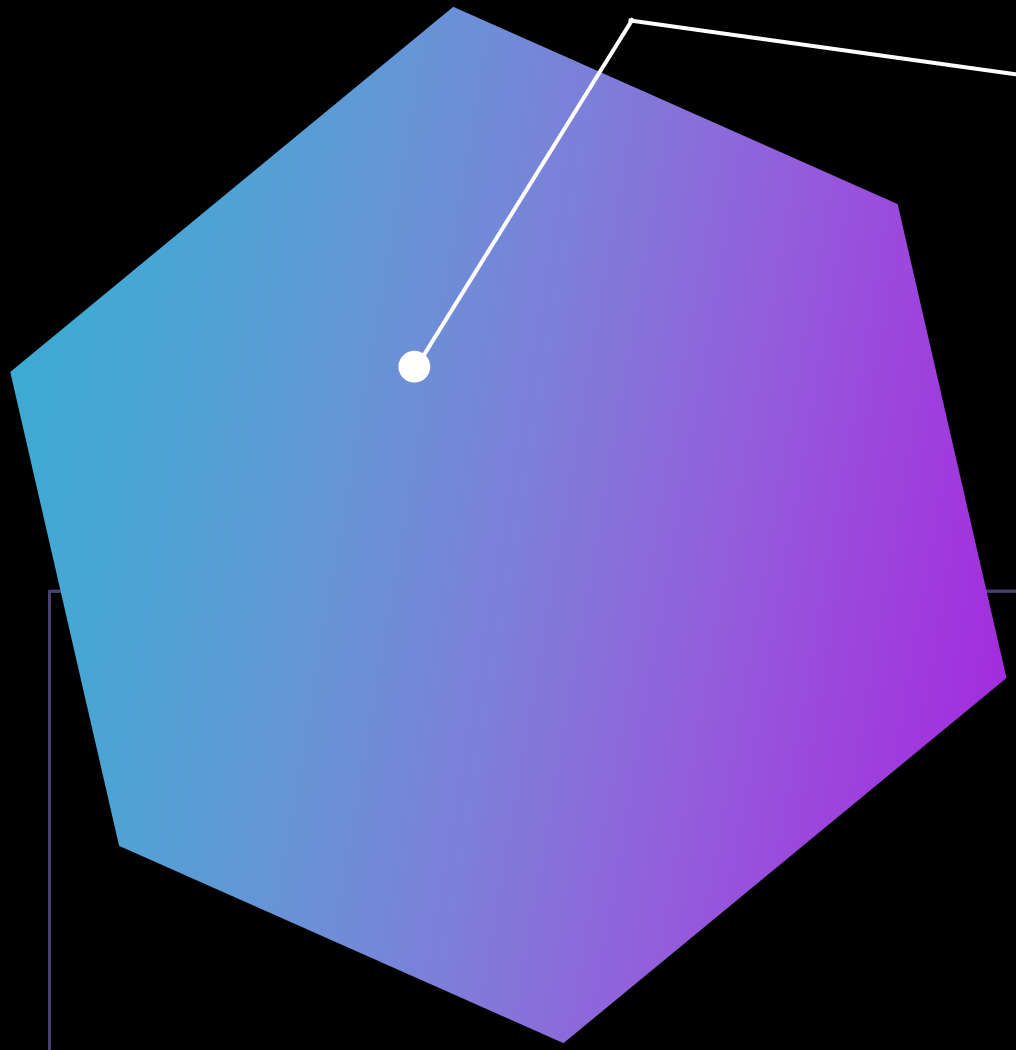
- Consiste em direcionar os usuários para sites falsos, que foram feitos para parecerem oficiais.
- No *pharming*, o usuário será direcionado ao site falso como resultado de atividades como:
  - Envenenamento de DNS (um ataque que altera URLs na tabela de nomes de domínio de um servidor);
  - Modificação de arquivos de host local (que são usados para converter URLs para o Endereço de IP).

Tailgating

- Tática simples de seguir de perto uma pessoa enquanto ela usa:
  - Próprio cartão de acesso ou PIN para obter acesso físico a uma sala ou prédio.
- É semelhante ao Shoulder Surfing, mas iniciado com uma conversa, por exemplo.
- Como geralmente acontece:
  - Tirando vantagem de um usuário autorizado que não está seguindo os procedimentos de segurança.
  - Desejo de ajudar alguém com conteúdo nas mãos.
- Controles:
  - Controle de acesso a portas duplas.
  - Boas práticas de segurança de um usuário autorizado.

Obtenção de Informações

- Chamadas de ou para help desk e unidades de suporte técnico podem ser usadas para obter informações.
- Um invasor pode obter:
  - ☑ Redefinição de senha;
  - ☑ Informações sobre algum sistema;
  - ☑ Outras informações úteis.



Whaling

- Ataque onde alvo é uma pessoa de alto valor, como um CEO ou CFO.
- Alvos do tipo são chamados de baleias.
- Não são realizados atacando vários alvos e esperando uma resposta.
- Como são construídos:
  - Sob medida para aumentar as chances de sucesso.
- Diferença das baleias para outros alvos:
  - Quase nenhuma, exceto que podem ser alvos de ataques sob medida.

Prepending

- Ato de adicionar algo ao início de uma relação, como um @nomedavitima.

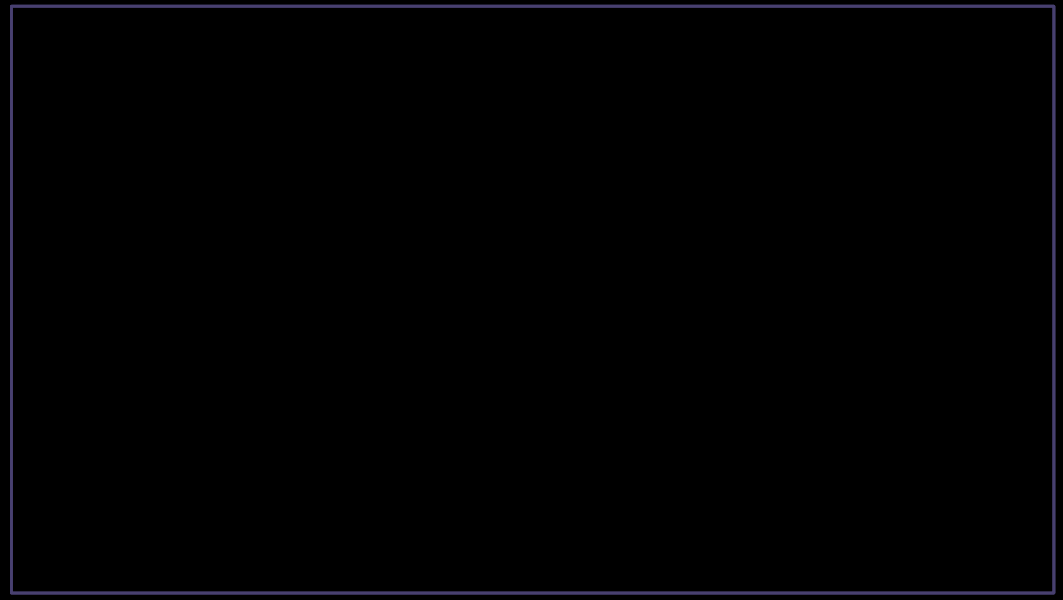
O QUE O ENGENHEIRO SOCIAL UTILIZA:

- Construções psicológicas sofisticada;
- *Prepender* gera engajamento e pode ser utilizado recursos de IA;

- Podem enganar com o nome e o e-mail do seu chefe;
- RE: ou FW: no e-mail;
- www.bradesco.com@192.168.2.1, onde o navegador ignoraria tudo à esquerda do @.

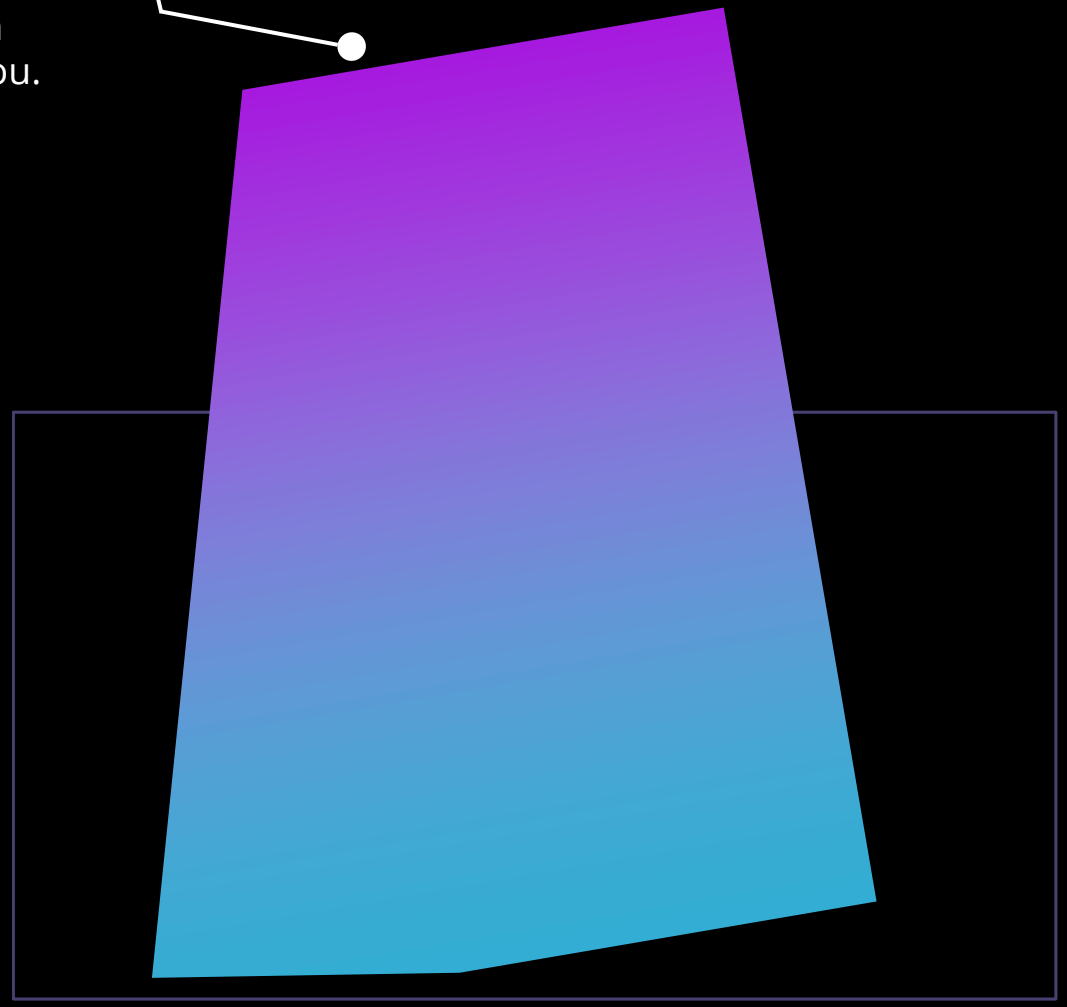
Fraude de Identidade

- Uso de credenciais falsas para atingir um fim.
- Entrar na empresa como um fornecedor.
- Pode ser feita:
  - Online, usando informações conhecidas sobre a pessoa que você está se passando e enganando a vítima que você está atacando.
- Formas de defesa:
  - Políticas;
  - Procedimentos fortes sem exceções.



Golpes de Fatura

- Golpes que usam uma fatura falsa na tentativa de fazer com que uma empresa pague por coisas que ela não encomendou.
- Envolve:
  - Se passar como fornecedor externou ou alguém de fora da contabilidade.
- Itens comuns desses golpes:
  - Produtos de escritório, como toner e materiais de escritório típicos;
  - Produtos de limpeza;
  - Associações organizacionais;
  - Serviços corporativos.



Coleta de Credenciais

- É mais do que Phishing, pois usa de várias outras técnias. Envolve **apenas** a coleta de informações de credenciais, como:

IDs de usuários;

Senhas.

- O que acontece depois?

Como o alvo não sabe que foi roubado, seus dados são redirecionados para a Dark Web para serem vendidos.

- Forma de combater esse ataque:

2FA

Autenticação de dois fatores.

OBRIGADO !

ENGENHARIA SOCIAL