Prime

CCS-A

Engenharia Social

Hoax

- Um *hoax* pode ser muito prejudicial como uma fraude que estimula a propagação ou não afetar a segurança em si.
- Treinamento contra notícias alarmarntes deve conter:

Aprender a suspeitar de e-mails e histórias incomuns;

Saber quem contatar para confirmar as suspeitas sobre um *hoax*.

- Outras formas de *hoax*:

Aconselhar o usuário a enviá-lo para seus amigos para que eles também saibam sobre o problema.

Watering Hole

- O caçador fica aguardando sua preza, ele vem por vontade própria.
- Os invasores podem plantar malware em sites que usuários visitam.

Watering Hole
Infecção estratégica de um site alvo com malware.

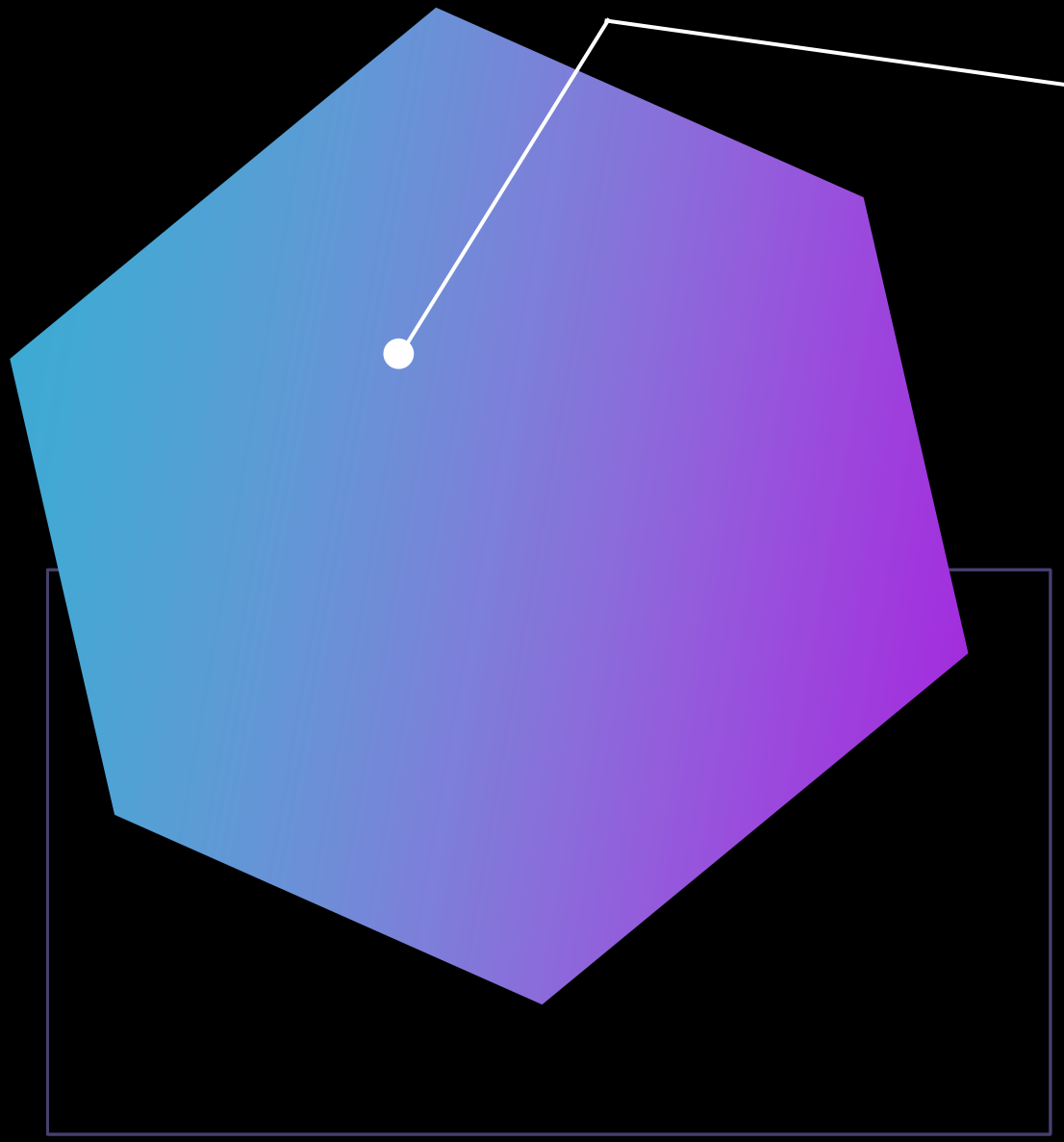
- Podem ser:
  - Muito eficazes na entrega de malware a grupos específicos;
  - Apoiados por estados-nação e outros invasores de alto recurso;
  - Sofisticado e normalmente é um ataque Dia Zero.

Typosquatting

- É uma forma de ataque que envolve a capitalização de erros de digitação.
- Como acontece:
  - Se um invasor tiver registrado a URL digitada errada, o usuário chega até a página do invasor.
- Conhecido também como **URL *Hijacking*.**
- Existem várias razões pelas quais um invasor irá buscar essa via de ataque:
  - *Phishing* para coletar credenciais;
  - Plantar malware.

Pretexting

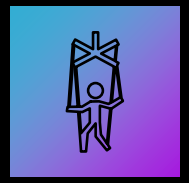
- O que o engenheiro social utiliza:
  - Uma narrativa (o pretexto) para influenciar a vítima a fornecer alguma informação.
- O pretexto não precisa ser verdadeiro, mas apenas crível.
- Principal objetivo:
  - Ganhar a confiança do alvo e explorá-lo.
- Pode ocorrer via:
  - E-mail;
  - Telefone;
  - Qualquer outra forma de comunicação.



Campanhas de Influência

- As campanhas de influência envolvem:
  - Uso de informações coletadas;
  - Publicação de material direcionado para indivíduos-chave;
  - Tentativa de alterar opiniões e mudar a mente das pessoas sobre um assunto.
- São ainda mais poderosas quando usadas em conjunto com as mídias sociais e *influencers*.
- Guerra híbrida:
  - Informação é usada para influenciar as pessoas a uma posição favorecida por aqueles que a divulgam;
  - Efeito psicológico (*bandwagon*) movendo crenças da massa.

Princípios (Razões Para a Eficácia)



A **engenharia social** é muito bem-sucedida por duas razões gerais:

- Desejo básico de ser útil: Uma resposta é dada por quem tem o conhecimento;
- Procuram evitar confrontos e problemas: Intimidação e ameaça em chamar o supervisor.

Por que a engenharia social é eficaz?

- Utiliza gatilhos psicológicos + ferramentas técnicas.

Autoridade

- O uso da **autoridade** em situações sociais pode levar a um ambiente em que uma parte se sente em risco ao questionar a outra sobre algo.
- Se você agir como um chefe ao solicitar algo, as pessoas estarão menos propensas a retê-lo.
- Melhor defesa contra ataques de engenharia social:

Políticas;

Conscientização.

Intimidação

- A intimidação geralmente é sutil;
- Forma de comunicação que cria uma expectativa de superioridade;
- Como ser intimidador:
  - Usar as credenciais ou títulos que criem autoridade;
  - Títulos extravagantes: Assessor Líder de Serviços Especiais.

Consenso

Consenso
Decisão homogênea de um grupo.

- Não vem de um campeão, mas de rodadas de negociação em grupo;
- Como o consenso é usado na engenharia social:
  - O engenheiro social simplesmente motiva os outros a alcançar um resultado consensual.

Escassez

Como a percepção de escassez atua:

- Motivando um alvo a tomar uma decisão rapidamente sem deliberação.

OBJETIVO:
Motivar um alvo a tomar uma decisão rapidamente, sem pensar;

Chegar com algo que é escasso e valorizado.

Familiaridade

- Construir um senso de familiaridade pode levar a uma confiança valiosa e equivocada;
- Como a engenharia social usa o senso de familiaridade:
  - Conversando sobre um tópico em comum;
  - O engenheiro social persuade e transmite uma sensação de familiaridade.

Confiança

Confiança
Compreensão de como algo vai agir sob determinadas condições.

Como a confiança é usada na Engenharia Social:
Engenheiros sociais podem moldar as percepções para induzir a conclusões falsas.

Objetivo:
Oferecer um caminho que leve o alvo a sentir que está fazendo a coisa certa.

Urgência

- Por que o tempo de urgência é manipulado na engenharia social:

Gera-se atalhos que podem acarretar no atropelamento dos processos.

- Chave para isso:

Percepção.

- Chave em todos os ataques de engenharia social:

Manipulação.

Reconhecimento

- Termo militar usado para descrever as ações de levantamento de um campo de batalha para obter informações antes das hostilidades;
- Métodos fora do alcance da vítima:
  - Pesquisas no Google e redes sociais;
  - Pesquisas em registros públicos e imprensa.
- Por que utilizam esse ataque?
  - Saber as fraquezas do alvo torna mais fácil um possível ataque.

Representação

- A **representação** é uma técnica comum de engenharia social e pode ser empregada de várias maneiras;
- Ocorre por:
  - Telefone;
  - Online.
- Ocorre via:
  - Operadores de help desk;
  - Fornecedores;
  - Fontes on-line.

Autorização de Terceiros

Como funciona:
Usando informações obtidas, o invasor chega até a vítima com algo que ela está esperando ou acredita que seja normal.

Diferencial:
Não pede nada de anormal. Evita a verificação de referência.

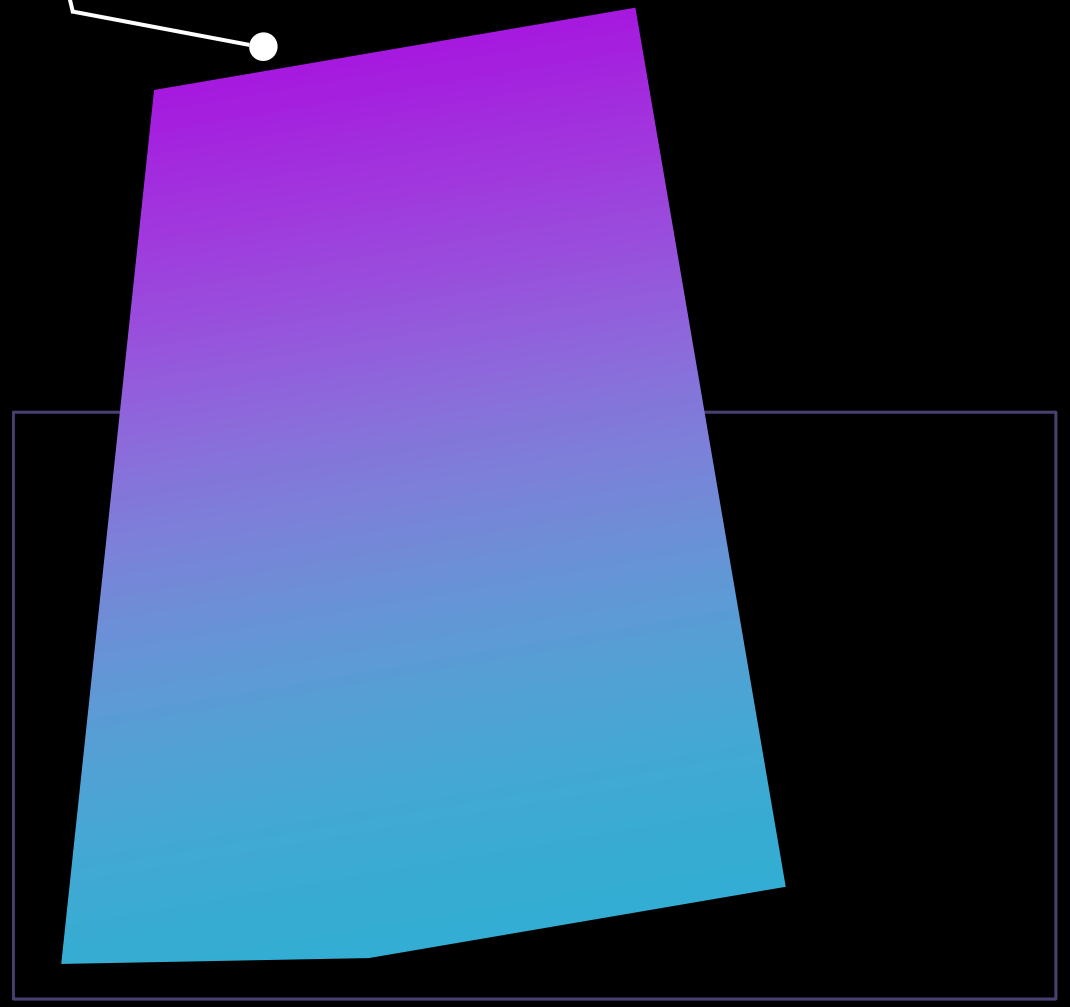
As ações geram:
Uma aparente autorização de terceiros, quando não há nenhuma.

Funcionários Terceirizados

- É comum em muitas organizações ter funcionários terceirizados;
- Como funciona um ataque como funcionário terceirizado:
  - Disfarce ou dizer que é troca de turno.
  - O invasor percorre os corredores despercebido, pois se mistura, coletando informações.

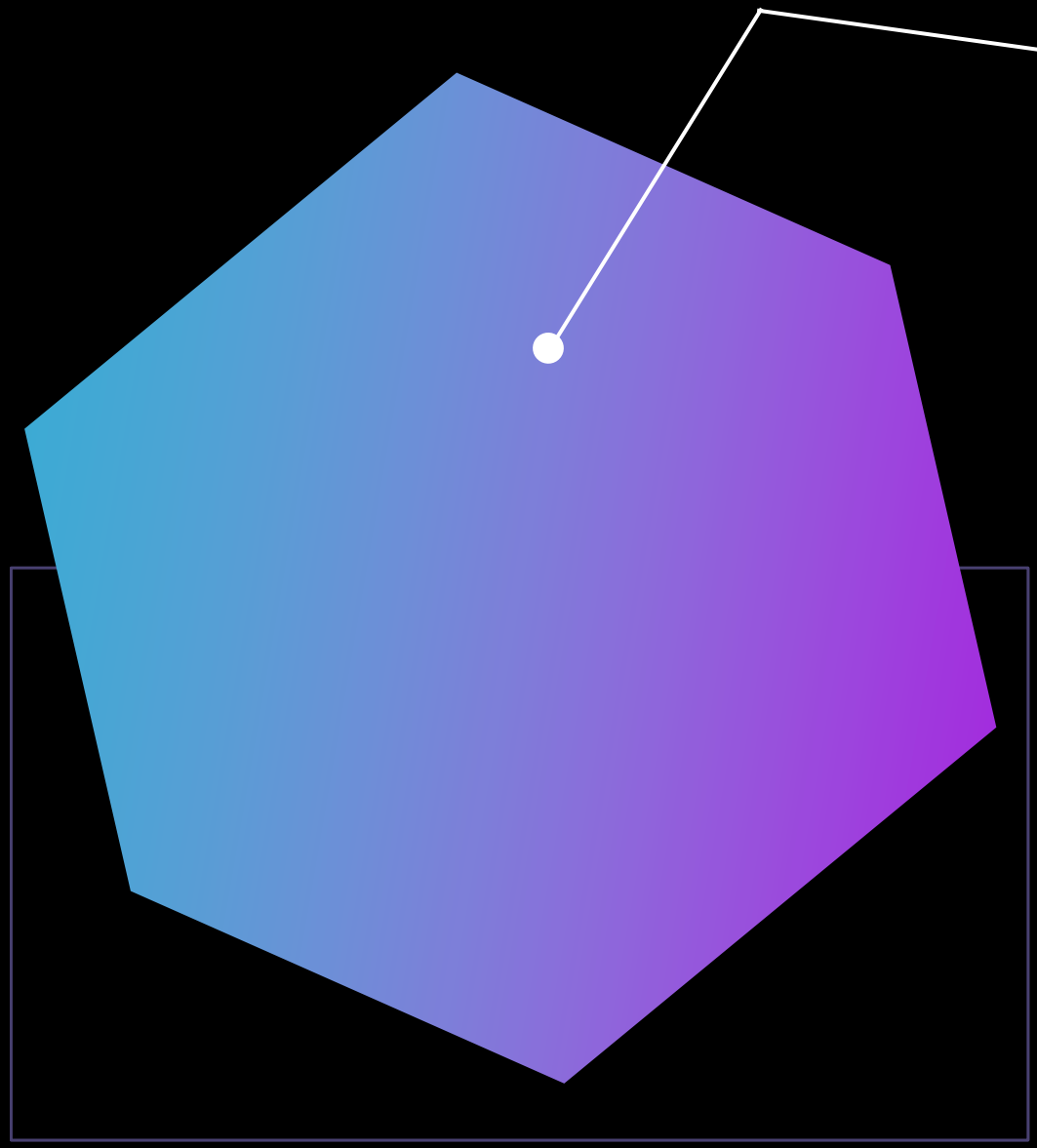
Personificação

- A personificação pode ser empregada em ataques online.
- Como a tecnologia atua:
  - Papel intermediário na comunicação.
- Principais meios de ataques online:
  - Falsificação de identidade (*phishing* via e-mail);
  - Golpes por meio das redes sociais que parecem pessoas confiáveis.



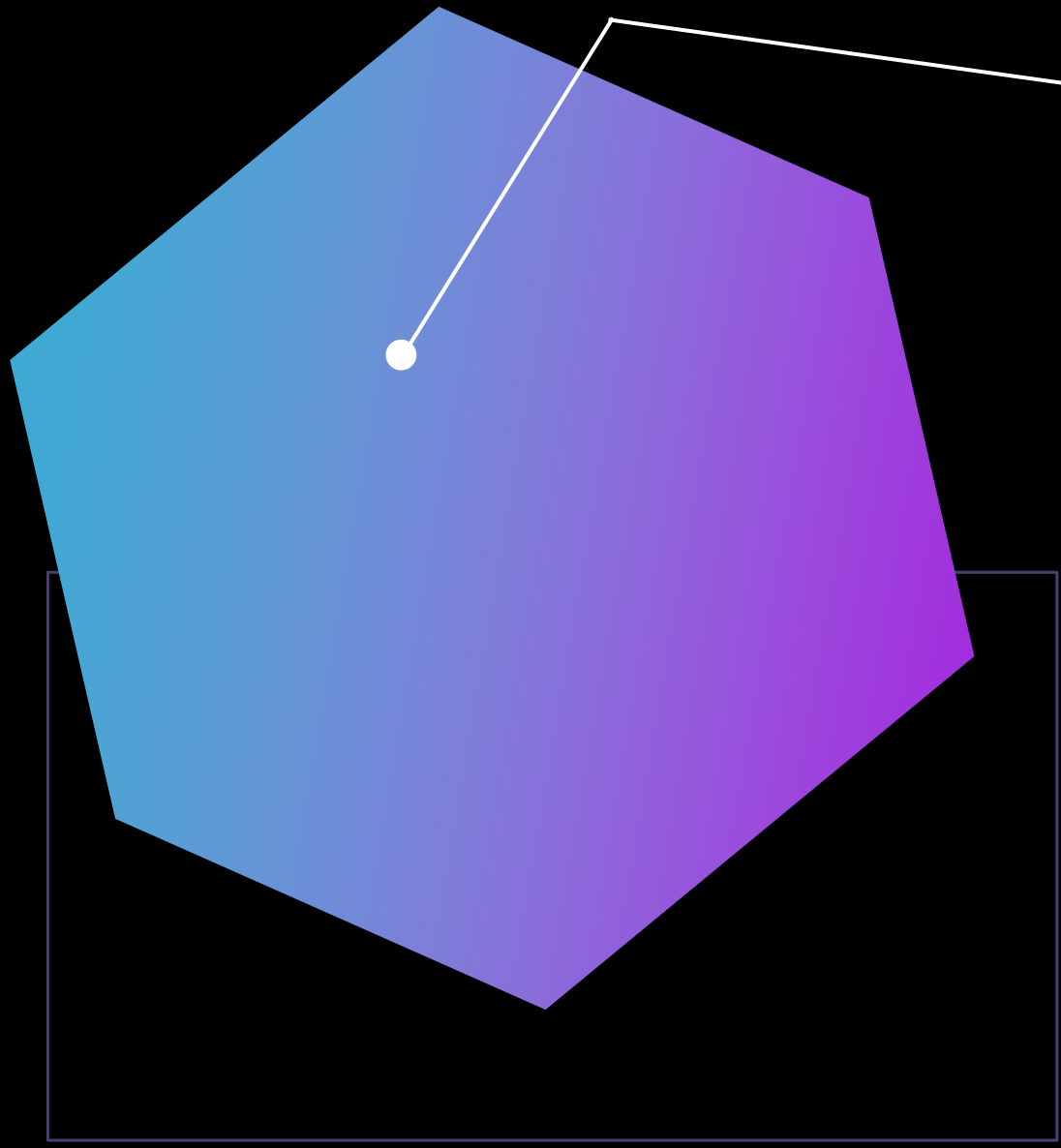
Defesas

- **Tenha processos em vigor que exijam:**
  - Solicitação da identidade.
- **Não deixe que ninguém entre sem verificar sua identidade.**
- **Aposte no:**
  - Treinamento;
  - Conscientização.
- **Realizar treinamentos regulares de acordo com o que está sendo vivenciado no momento, em vez de algo genérico.**



Lenda Urbana?

- Ataques de engenharia social funcionam: isso é um fato!
- Os elementos apresentados são usados o tempo inteiro por hackers.
- Defesas de engenharia social são mais fáceis de implementar do que de um ataque mais técnico.
- Defesa:
  - Políticas e procedimentos;
  - Treinamento de funcionários.



OBRIGADO!

MAIS FERRAMENTAS DE
ENGENHARIA SOCIAL