**Trabalho: Guerra de Informação – OSINT e Engenharia Social**

**Objetivo**

O objetivo deste trabalho é demonstrar como informações podem ser coletadas através de técnicas de **OSINT (Inteligência de Fontes Abertas)** e **Engenharia Social**. Os alunos aprenderão a importância da privacidade e da proteção de dados pessoais.

**Divisão das Equipes**

* A turma será dividida em **trios**.
* Cada trio será um **"Time de Investigação"** e terá outro trio como **"Alvo"**.
* Os pares de trios serão sorteados pelo professor.

**Fase 1: Coleta de Informações (OSINT & Engenharia Social)**

Cada **Time de Investigação** terá **5 dias** para coletar o máximo de informações possíveis sobre seu trio-alvo. As fontes permitidas incluem:  
✅ Redes sociais (Facebook, Instagram, LinkedIn, Twitter, etc.)  
✅ Buscas no Google (e técnicas avançadas)  
✅ Informações públicas (sites de registro de domínios, etc.)  
✅ Qualquer outra fonte aberta disponível na internet

🚫 **O que NÃO é permitido**:  
❌ Contato direto com o trio-alvo (exemplo: enviar mensagens se passando por outra pessoa)  
❌ Acessar informações privadas sem permissão  
❌ Uso de phishing ou engenharia social fora do ambiente do trabalho

**Entrega:**  
Cada trio deve preparar um relatório detalhado com:

1. **Lista de informações descobertas** (nomes, cidade, profissão, hobbies, etc.)
2. **Fontes utilizadas para cada informação**
3. **Métodos utilizados na busca** (como encontraram as informações)
4. **Sugestões de como o trio-alvo poderia se proteger melhor**

**Critérios de Avaliação (Nota de 0 a 10)**

✔ **Coleta de informações (4 pontos)** – Quantidade e qualidade das informações coletadas pelo Time de Investigação  
✔ **Relatório (3 pontos)** – Clareza na apresentação dos dados coletados e nas explicações  
✔ **Defesa e resposta (3 pontos)** – Capacidade do trio-alvo de avaliar os riscos e sugerir boas práticas de proteção

**Fase 2: Defesa e Proteção**

Após a entrega dos relatórios, cada trio terá acesso ao relatório produzido sobre eles e deverá:

1. **Avaliar as informações descobertas** (quais são realmente verdadeiras?)
2. **Explicar como poderiam ter protegido melhor esses dados**
3. **Criar um plano de defesa** para evitar exposição futura

**Entrega:**  
Cada trio escreverá uma resposta explicando:

* Quais informações eram verdadeiras
* Como poderiam ter evitado que essas informações fossem descobertas
* Estratégias de proteção para o futuro

**Reflexão Final**

Após o trabalho, faremos um debate em sala sobre:

* Como informações pessoais podem ser expostas sem percebermos
* O impacto da engenharia social em ataques reais
* Boas práticas de segurança digital para o dia a dia

**Ranking de "Nível de Exposição"**

**Como funciona?**

* Se um trio conseguiu descobrir **mais de 10 informações relevantes** sobre o outro, o alvo recebe uma **classificação de exposição alta**.
* Se descobriram **5 a 10 informações**, a exposição é **moderada**.
* Se encontraram **menos de 5**, a exposição é **baixa**.
* O trio com **melhor proteção** ganha um bônus na nota!

**Objetivo:** Estimular os alunos a revisarem suas configurações de privacidade e a serem mais conscientes sobre o que compartilham.