**Centro Paula Souza**

**ETEC Professor Camargo Aranha**

Caique

**Atividade Pratica Segurança de Informaçoes**

**Desenvolvimento de sistemas**

**São Paulo**

**2025**

Sumário

[**Tipos de Golpes na Internet e Exemplos Reais** 3](#_Toc191405860)

[1. Golpe de Cartão de Crédito Falso (Clonagem de Cartão) 3](#_Toc191405861)

[2. Golpe de Comércio Eletrônico Falso (Falsa loja online) 3](#_Toc191405862)

[3. Golpe de Clonagem de WhatsApp 3](#_Toc191405863)

[**Tipos de Ataques na Internet e Exemplos Reais** 4](#_Toc191405864)

[1. DDoS (Ataque de Negação de Serviço Distribuída) 4](#_Toc191405865)

[2. SQL Injection 4](#_Toc191405866)

[3. XSS (Cross-Site Scripting) 4](#_Toc191405867)

[Ferramentas para Causar Esses Ataques 5](#_Toc191405868)

# **Tipos de Golpes na Internet e Exemplos Reais**

### ****Golpe de Cartão de Crédito Falso (Clonagem de Cartão)****

* **O que é?**: Criminosos clonam os dados do cartão de crédito da vítima para fazer compras online ou até em lojas físicas sem que a pessoa saiba.
* **Exemplo Real**:
  + **Ano**: 2019
  + **Golpe**: Clonagem de Cartão de Crédito
  + **Empresa**: Vários bancos e vítimas individuais
  + **Prejuízo**: Estimado em **US$ 1,5 bilhão** globalmente (em 2019, considerando o valor de fraudes com cartões).
  + **Como aconteceu?**: Hackers conseguiram acessar os dados de cartões de crédito através de lojas online vulneráveis, usando técnicas como **skimming** (captura de dados via dispositivos) e **malware** (programas maliciosos). Usaram esses dados para fazer compras sem o consentimento dos donos dos cartões, resultando em perdas financeiras para as vítimas e as instituições financeiras.

### 2. ****Golpe de Comércio Eletrônico Falso (Falsa loja online)****

* **O que é?**: São lojas online falsas que parecem legítimas, oferecendo produtos baratos. Quando a pessoa paga, nunca recebe o que comprou.
* **Exemplo Real**:
  + **Ano**: 2020
  + **Golpe**: Loja online falsa
  + **Empresa**: Vários consumidores, sem uma empresa específica
  + **Prejuízo**: Milhões de dólares
  + **Como aconteceu?**: Muitos sites falsos, que pareciam lojas confiáveis, venderam produtos como smartphones e roupas a preços muito baixos. Depois, as pessoas fizeram a compra, pagaram, mas nunca receberam os produtos. Esses sites desapareciam depois de um tempo, e ninguém conseguia recuperar o dinheiro.

### 3. ****Golpe de Clonagem de WhatsApp****

1. **O que é?**: Os criminosos clonavam o número de WhatsApp da vítima e passavam a se comunicar com os contatos dela, pedindo dinheiro ou favores.
2. **Exemplo Real**:
   * **Ano**: 2021
   * **Golpe**: Clonagem de WhatsApp
   * **Empresa**: Vários casos individuais, sem uma empresa específica
   * **Prejuízo**: Varia por caso, mas muitas pessoas perderam quantias de dinheiro significativas.
   * **Como aconteceu?**: O criminoso usava uma técnica para clonar o número de WhatsApp da vítima e, depois, se passava pela pessoa, pedindo dinheiro a amigos ou familiares com histórias falsas de emergência. Muitas pessoas caíram nesse golpe, transferindo grandes quantias de dinheiro.

# **Tipos de Ataques na Internet e Exemplos Reais**

### ****DDoS (Ataque de Negação de Serviço Distribuída)****

* + **O que é?**: Nesse ataque, os hackers sobrecarregam um site ou servidor com um monte de pedidos, fazendo com que ele fique lento ou até caia, deixando os usuários normais sem conseguir acessar.
  + **Exemplos Reais**:
    - **Ano**: 2016
      * **Ataque**: DDoS
      * **Empresa**: **Dyn**
      * **O que aconteceu?**: Hackers usaram vários dispositivos como câmeras e roteadores conectados à internet (botnet) para sobrecarregar o servidor da Dyn. Isso fez com que sites grandes como Twitter, Netflix e Reddit ficassem fora do ar por horas.
      * **Prejuízo**: **US$ 110 milhões**.
    - **Ano**: 2020
      * **Ataque**: DDoS
      * **Empresa**: **Cloudflare**
      * **O que aconteceu?**: Em 2020, a Cloudflare bloqueou o maior ataque DDoS de todos os tempos (2,3 terabits por segundo). Isso foi feito com uma botnet gigantesca e poderia ter derrubado muitos sites.
      * **Prejuízo**: Difícil calcular, mas foi um baita impacto na infraestrutura de internet global.

### ****SQL Injection****

* + **O que é?**: É quando o hacker injeta código malicioso dentro de um campo de um site (como um login ou uma busca). Esse código pode ser usado para acessar ou até roubar dados importantes do banco de dados do site.
  + **Exemplos Reais**:
    - **Ano**: 2013
      * **Ataque**: SQL Injection
      * **Empresa**: **Heartland Payment Systems**
      * **O que aconteceu?**: Hackers usaram SQL Injection para acessar e roubar dados de **134 milhões de cartões de crédito** de clientes. Foi um dos maiores vazamentos de dados da história.
      * **Prejuízo**: **US$ 150 milhões**.
    - **Ano**: 2017
      * **Ataque**: SQL Injection
      * **Empresa**: **Equifax**
      * **O que aconteceu?**: A Equifax, uma das maiores agências de crédito, foi hackeada através de uma falha de SQL Injection, expondo os dados pessoais de **147 milhões de pessoas**.
      * **Prejuízo**: **US$ 700 milhões**, incluindo multas e reparações.

### ****XSS (Cross-Site Scripting)****

* + **O que é?**: No XSS, o hacker injeta um script malicioso em um site. Esse script pode roubar informações da vítima, como senhas ou até fazer ações em nome dela.
  + **Exemplos Reais**:
    - **Ano**: 2014
      * **Ataque**: XSS
      * **Empresa**: **Yahoo**
      * **O que aconteceu?**: Um ataque XSS no Yahoo Mail permitiu que os hackers roubassem cookies de sessão e acessassem as contas de muitos usuários.
      * **Prejuízo**: Não tem um valor exato, mas a falha teve grande impacto na segurança do Yahoo.
    - **Ano**: 2018
      * **Ataque**: XSS
      * **Empresa**: **Facebook**
      * **O que aconteceu?**: Hackers usaram XSS para roubar dados de usuários do Facebook, como nomes e números de telefone, e depois conseguiram invadir mais contas.
      * **Prejuízo**: **US$ 3 milhões**.

## Ferramentas para Causar Esses Ataques

1. **LOIC (Low Orbit Ion Cannon)**
   * **O que é?**: LOIC é uma ferramenta usada para fazer ataques DDoS. Ela sobrecarrega os servidores com tráfego, fazendo o site cair ou ficar super lento.
   * **Como funciona?**: Você conecta o LOIC à internet e escolhe o site que quer atacar. O LOIC começa a mandar um monte de requisições para esse site, até ele não conseguir mais responder a usuários normais.
   * **Uso**: Foi muito usado pelo grupo **Anonymous** para realizar ataques a sites de governos e empresas.
2. **SQLmap**
   * **O que é?**: O SQLmap é uma ferramenta usada para testar e explorar falhas de **SQL Injection**. Com ela, você pode tentar acessar bancos de dados e roubar dados pessoais de um site.
   * **Como funciona?**: Ela envia comandos maliciosos para o site, testando se o banco de dados é vulnerável a SQL Injection. Se for, você pode acessar dados sensíveis, como senhas e e-mails.
   * **Uso**: Usado por hackers e profissionais de segurança para testar a segurança de sites, mas pode ser usado para roubar dados se não for controlado corretamente.