



# Phishing

# PHISHING, O QUE É?



O phishing é uma técnica de fraude online que visa roubar informações pessoais. Geralmente, os golpistas se passam por entidades confiáveis e solicitam dados sigilosos. E-mails, mensagens e sites falsos são comuns nesse tipo de ataque.

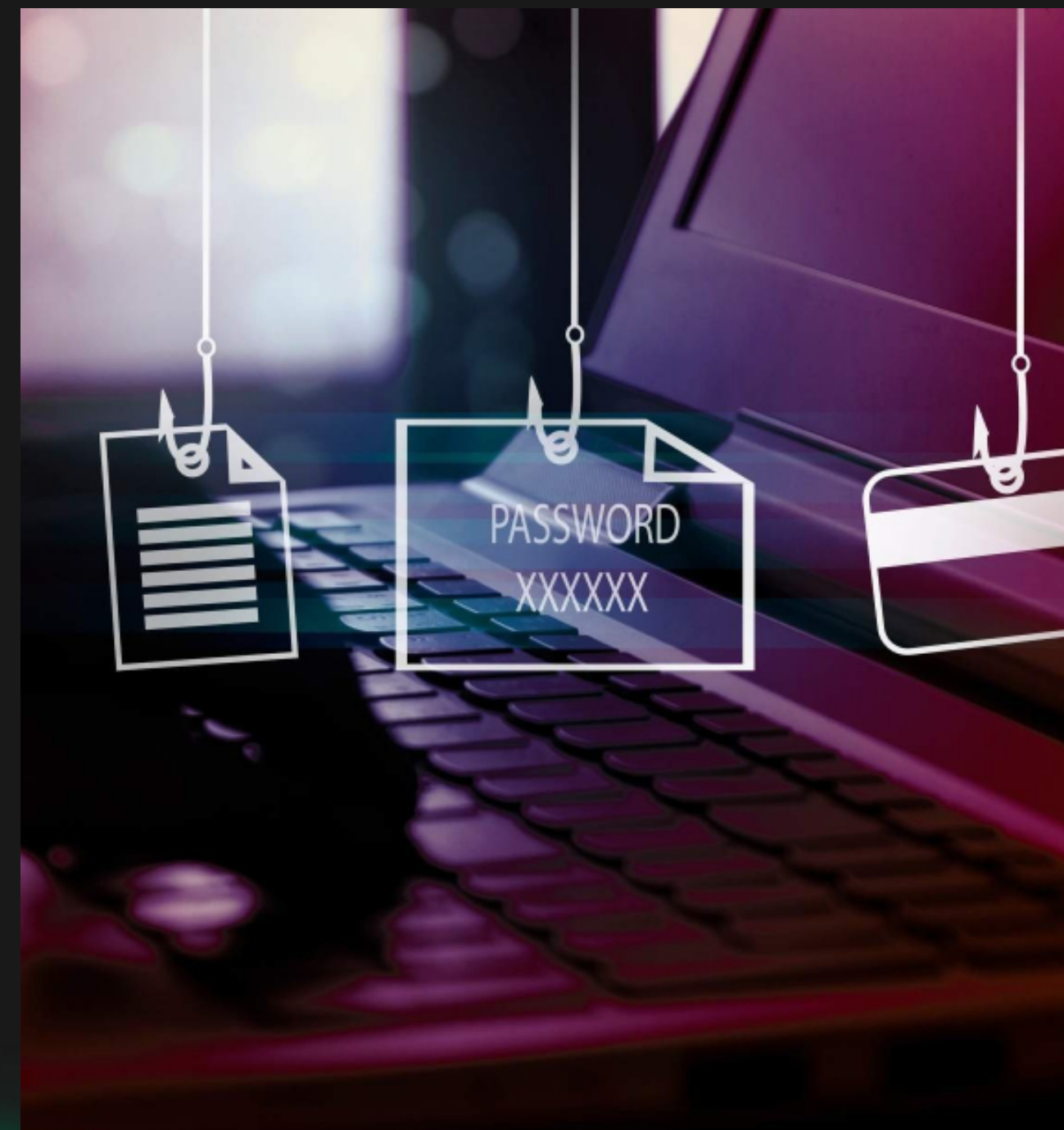




# COMO O PHISHING FUNCIONA



1. **Preparação:** Cria uma mensagem se passando por uma empresa legítima;
2. **Envio:** Envia a mensagem para um grande número de pessoas por e-mail ou outros meios de comunicação;
3. **Engano:** A mensagem é projetada para enganar a vítima;
4. **Obtenção de Informação:** Se a vítima cair no golpe e fornecer suas informações pessoais, o hacker pode usá-las para varias atividades maliciosas.



# PRINCIPAIS TÉCNICAS UTILIZADAS



- Blind Phishing;
- Smishing;
- Clone Phishing;
- Vishing;
- Spear Phishing;
- Whaling.





# COMO EVITAR O PHISHING?

1. Desconfie de e-mails de remetentes desconhecidos;
2. Verifique cuidadosamente os URLs antes de fornecer informações;
3. Nunca compartilhe informações pessoais ou financeiras por e-mail ou telefone, a menos  
que você tenha certeza da identidade do solicitante;
4. Mantenha seu software atualizado para proteger contra vulnerabilidades;
5. Use a autenticação de dois fatores sempre que possível;
6. Esteja atento a mensagens que tentam criar urgência;
7. Verifique a segurança do site antes de inserir informações confidenciais;



# PROPRIEDADES AFEDATAS

Ao cair em um golpe de phishing, as vítimas podem imprudentemente divulgar Dados confidenciais comprometendo sua confidencialidade. Além disso, os hackers podem modificar dados ou realizar atividades fraudulentas, comprometendo a integridade das informações. E em casos mais avançados, o phishing pode resultar na instalação de malware nos sistemas das vítimas, afetando sua disponibilidade e tornando-os inacessíveis ou comprometidos.

