**Universidade São Judas Tadeu**

LUCAS TOSTA PIOLA - 825137169

**Projeto A3 - Sistemas Computacionais e Segurança**

**(SCC)**

Professor Calvetti

São Paulo

2025

**Autenticação em Duas Etapas**

A autenticação de dois fatores (2FA) é um método de segurança que adiciona uma camada extra de proteção ao acesso a contas e sistemas. Em vez de depender somente de uma senha, a 2FA exige um segundo tipo de autenticação, o que dificulta o acesso de invasores às informações privadas.

Esse segundo fator pode ser dividido em três categorias principais:

- Algo que você conhece, como uma senha ou PIN.

- Algo que você tem, como um código gerado por um aplicativo de autenticação.

- Algo que você é, como características biométricas (impressão digital, reconhecimento facial ou de voz).

O processo da autenticação em duas etapas normalmente segue os seguintes passos:

- O usuário insere seu nome de usuário e senha para acessar sua conta.

- O sistema solicita a confirmação de um segundo fator de autenticação.

- O usuário fornece esse segundo fator (como um código enviado por SMS ou gerado por um aplicativo).

Se ambos os fatores forem válidos, o acesso é liberado.

**Anti-Phishing**

O anti-phishing envolve um conjunto de ferramentas e práticas criadas para identificar e bloquear ataques de phishing antes que eles causem danos. As soluções anti-phishing utilizam uma variedade de técnicas para proteger os usuários, como:

**Filtros de URL:** Monitoram links suspeitos e bloqueiam sites fraudulentos antes que o usuário os acesse.

**Análise de Comportamento:** Identifica padrões de e-mails e mensagens fraudulentas.

**Listas Negras:** Mantêm um banco de dados com sites maliciosos conhecidos, impedindo o acesso a esses endereços.

**Autenticação de E-mails (SPF, DKIM, DMARC):** Ferramentas que verificam a autenticidade do remetente e ajudam a prevenir fraudes por e-mail.

**Monitoramento de Certificados SSL:** Detecta sites falsificados que tentam se passar por conexões seguras.

Essas tecnologias são frequentemente integradas a antivírus, navegadores e firewalls, criando uma camada adicional de proteção contra ameaças online.

**Principais Tecnologias Anti-Phishing**

Há diversas abordagens para combater os ataques de phishing. Algumas das mais utilizadas incluem:

**Filtros de Navegação Segura:** Ferramentas como o Google Safe Browsing e o Microsoft SmartScreen verificam URLs em tempo real e bloqueiam sites fraudulentos antes que o usuário os acesse.

**Soluções de Segurança de E-mail:** Provedores como Gmail, Outlook e Yahoo possuem sistemas de filtragem que movem mensagens de phishing para a pasta de spam.

**Extensões para Navegadores:** Ferramentas como Bitdefender TrafficLight e Avast Online Security adicionam proteção extra ao navegar na web.

**Autenticação de E-mails (SPF, DKIM, DMARC):** São protocolos que evitam que criminosos falsifiquem endereços de e-mail legítimos.

**Inteligência Artificial e Machine Learning:** Algumas soluções anti-phishing utilizam algoritmos para identificar padrões e prever novos ataques.

Embora o phishing continue a ser uma ameaça significativa, as soluções anti-phishing têm se mostrado cada vez mais eficazes na proteção contra esses golpes. Usar ferramentas apropriadas e adotar boas práticas de segurança pode reduzir bastante o risco de cair em fraudes online.

**VPN (Rede Virtual Privada)**

Uma VPN (Virtual Private Network) estabelece uma conexão criptografada e segura entre o seu dispositivo e a internet. Seu objetivo principal é proteger a sua privacidade, ocultando o seu IP real e usando um servidor em outro local do mundo, além de criptografar os dados, tornando-os ilegíveis para hackers.

**Anti-Cheat**

O sistema anti-cheat foi desenvolvido para detectar e prevenir trapaças em jogos online, buscando garantir uma experiência justa para todos os jogadores. Ele utiliza diversos métodos para identificar arquivos suspeitos ou alterados que possam indicar o uso de cheats, como:

**Verificação de arquivos do jogo:** O sistema verifica se os arquivos do jogo foram modificados ou substituídos por versões alteradas.

**Monitoramento de programas em execução:** O anti-cheat observa se há programas ou processos em segundo plano que possam estar interferindo no jogo.

**Análise comportamental:** Embora não seja o principal método em muitos sistemas anti-cheat, essa abordagem avalia o comportamento do jogador no jogo, como tempos de reação anormais, precisão excessiva, padrões de disparo, etc.

**Detecção de injeção de código:** Muitos cheats injetam códigos no jogo para alterar seu comportamento. O anti-cheat busca detectar e impedir essa injeção de código.

Apesar de todas essas técnicas, o anti-cheat ainda pode ser burlado, e por isso as empresas devem constantemente atualizar seus sistemas.

**Criptografia de Pagamentos**

A criptografia de pagamentos em lojas online protege transações ao codificar dados sensíveis, como as informações de cartões de crédito. Usando protocolos como SSL/TLS, ela garante que apenas o destinatário autorizado tenha acesso a esses dados, prevenindo fraudes e oferecendo maior segurança nas compras online.