**Universidade São Judas Tadeu**

EDUARDO CECILIO ALVES SANTOS

LUCAS PERES SIMÕES

PEDRO HENRIQUE GUIMARÃES RESTANI

RAFAEL HENRIQUE GARBELINI ALBERTO

**Projeto A3 - Sistemas Computacionais e Segurança**

**(SCC)**

Professor Calvetti

São Paulo

2025

**Autenticação por duas etapas**

A autenticação em duas etapas (2FA) é uma estratégia de segurança que oferece uma camada adicional de proteção para o acesso a contas e sistemas. Ao invés de depender exclusivamente de uma senha, a 2FA requer um segundo elemento de autenticação, dificultando assim a ação de invasores que queiram acessar informações confidenciais.

Esse segundo elemento pode ser classificado em três categorias principais:

- Algo que você sabe como uma senha ou um PIN.

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

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

O funcionamento da autenticação em duas etapas geralmente segue este procedimento:

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

- O sistema solicita um segundo elemento de autenticação.

- O usuário fornece esse segundo elemento (por exemplo, um código gerado por um aplicativo ou recebido por SMS).

- Se ambos os elementos estiverem corretos, o acesso é concedido.

**Anti-Phishing**

O anti-phishing é um conjunto de tecnologias e práticas desenvolvidas para identificar e bloquear ataques de phishing antes que eles causem danos. As soluções anti-phishing utilizam diferentes 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 – Detectam padrões suspeitos de e-mails e mensagens fraudulentas.

Listas Negras – Mantêm registros atualizados de sites maliciosos conhecidos, impedindo o acesso a esses endereços.

Autenticação de E-mails (SPF, DKIM, DMARC) – Ferramentas que verificam a autenticidade do remetente e evitam fraudes por e-mail.

Monitoramento de Certificados SSL – Identificam sites falsificados que tentam imitar conexões seguras.

Essas tecnologias são frequentemente integradas a antivírus, navegadores e firewalls, fornecendo uma camada extra de proteção contra ataques cibernéticos. Principais Tecnologias Anti-Phishing

Existem diversas abordagens utilizadas para impedir ataques de phishing. Algumas das mais comuns incluem:

Filtros de Navegação Segura – Ferramentas como o Google Safe Browsing e o Microsoft SmartScreen verificam URLs em tempo real e bloqueiam páginas fraudulentas antes que o usuário as acesse.

Soluções de Segurança de E-mail – Provedores como Gmail, Outlook e Yahoo possuem sistemas que filtram mensagens suspeitas e movem e-mails de phishing para a pasta de spam.

Extensões para Navegadores – Programas como Bitdefender TrafficLight e Avast Online Security adicionam camadas extras de proteção ao navegar na web.

Autenticação de E-mails (SPF, DKIM e DMARC) – São protocolos que impedem que criminosos falsifiquem endereços de e-mail legítimos para enganar vítimas.

Inteligência Artificial e Machine Learning – Algumas soluções anti-phishing usam algoritmos para identificar padrões suspeitos e prever novos ataques. O phishing é uma das maiores ameaças digitais da atualidade, mas as soluções anti-phishing têm se tornado cada vez mais eficazes na proteção contra esses golpes. Com o uso de ferramentas adequadas e boas práticas de segurança, é possível reduzir significativamente o risco de ser vítima de fraudes online.

**VPN**

O VPN (Rede Virtual Privada em português) cria uma conexão criptografada e segura entre o seu dispositivo e a internet. Um VPN tem como seu objetivo de proteger a sua privacidade, ocultando o seu IP real e utilizando um servidor em outro lugar do mundo, além de criptografar seus dados, tornando os ilegíveis contra crackers.

**Anti-cheat**

O Anti-cheat é um sistema desenvolvido para detectar e prevenir cheats (trapaças) em jogos online, com seu intuito em manter um espaço mais justo para os jogadores. Eles utilizam diversas formas de detectar arquivos suspeitos ou alterados que possam indicar um uso de hacks, tais como:

- Verificar os arquivos do jogo.

Para assegurar que nenhum deles foi alterado ou substituído por versões modificadas, o anti-cheat analisa esses arquivos e garante a autenticidade deles.

- Monitoramento de programas em execução.

O anti-cheat verifica se há processos ou programas ativos no sistema em segundo plano.

- Análise comportamental.

Embora não seja o método principal da maioria dos anti-cheats por conta de possíveis falsos positivos caso algum jogador seja extremamente habilidoso, ao invés de buscar por arquivos suspeitos, ele analisa o comportamento do jogador no jogo, como tempo de reação fora do normal, precisão irreal, padrões de disparo e etc.

- Detecção de injeção de código.

A maioria dos cheats injetam códigos dentro do jogo para modificar a maneira que ele se comporta, o trabalho do anti-cheat é detectar essa injeção e impedir a execução.

Mesmo com todos esses métodos, o anti-cheat ainda pode ser burlado, devido a isso, empresas precisam constantemente atualizar os seus sistemas.

**Criptografia de pagamentos**

A criptografia de pagamentos em lojas online protege as transações ao codificar dados sensivéis como informações de cartão de crédito. Usando protocolos como SSL/TLS, ela assegura que somente o destinatário autorizado acesse esses dados, evitando fraudes e aumentando a segurança nas compras.