factis®

Mantenha-se Alerta no Jogo

Mantenha-se em Segurança Durante o Mundial da FIFA de 2026

O maior evento de futebol do mundo é também uma das maiores oportunidades para ocorrerem burlas online.

factis®

Os Cibercriminosos Já Entraram em Campo

Os grandes eventos desportivos atraem consistentemente campanhas de phishing, burlas com bilhetes falsos, apps maliciosas e burlas nas redes sociais.

Domínios Falsos do Mundial

Os investigadores já identificaram websites suspeitos que imitam plataformas de bilhetes e de streaming.

Burlas nas Redes Sociais

Os passatempos falsos e as contas falsificadas disseminam-se rapidamente durante os grandes torneios.

Os Adeptos São Alvos Preferenciais

Os burlões tiram partido da urgência, do entusiasmo e do medo de perder a oportunidade.

factis®

Burlas com Bilhetes Falsos: O Truque Mais Antigo

Os websites fraudulentos de bilhetes estão a multiplicar-se a um ritmo alarmante - muitos não se conseguem distinguir da plataforma oficial da FIFA. Milhares de adeptos já reportaram ter pago centenas a milhares de dólares por bilhetes que nunca chegaram às suas mãos. Os burlões clonam a marca oficial, usam nomes de domínio convincentes e desaparecem após o pagamento.

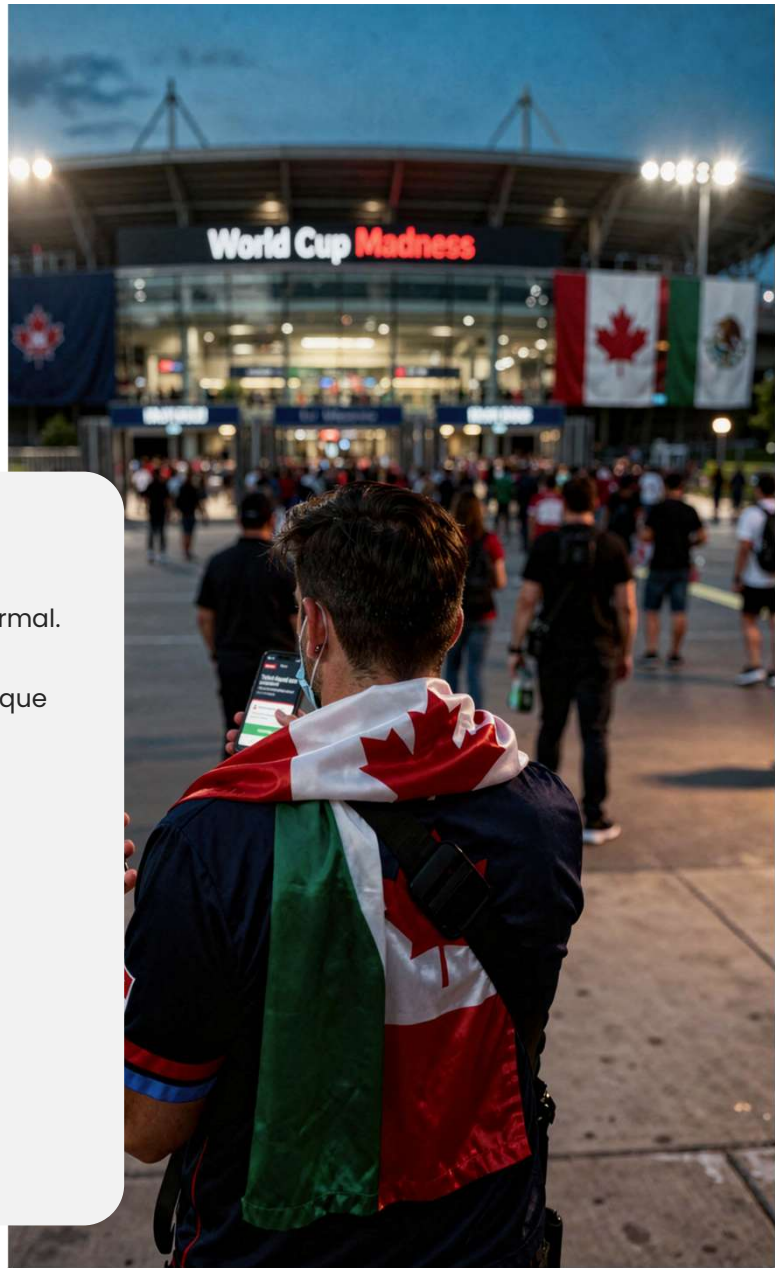
Verificação da Fonte
Adquira bilhetes apenas através do site **FIFA.com** ou de revendedores oficialmente autorizados. Guarde o site oficial nos favoritos.

Verificação do URL com Atenção
Procure erros ortográficos subtis como"f1fa.com" ou"fifa-tickets2026.net" - sinais inequívocos de burla.

Nunca Pague por Transferência Bancária
Os burlões preferem métodos de pagamento não rastreáveis. Por isso, utilize somente cartões de crédito com proteção contra burlas.

Sinais de Alerta

- Preços muito abaixo do valor normal.
- Pressão para “comprar já antes que se esgotem”.
- Sem conexão segura HTTPS.
- Pagamento por criptomoeda ou transferência bancária.
- Sem informações de contacto verificáveis de vendedor.
- Erros gramaticais ou marca inconsistente.



factis®

Quem São os Alvos?

Os cibercriminosos lançam uma rede ampla durante o Mundial de 2026 - explorando o entusiasmo dos adeptos, viajantes e colaboradores. Ninguém está imune.

Adeptos em Viagem

Reservam bilhetes, hotéis e experiências online - são alvos preferenciais de sites falsos, e-mails de phishing e burlas de viagem.

Espectadores em Casa

Procuram transmissões, resumos e apps de apostas - vulneráveis a transferências maliciosas, portais de streaming falsos e roubo de credenciais.

Colaboradores Empresariais

Acedem a conteúdos de adeptos em dispositivos de trabalho - criando pontos de entrada para malware, fugas de dados e comprometimento da rede da sua empresa.

Burlas de Streaming e Apps Falsas

Com os direitos de streaming legítimos protegidos por assinaturas pagas, milhões de adeptos procuram transmissões “gratuitas” do Mundial - caindo diretamente nas armadilhas dos cibercriminosos. As apps falsas e sites de streaming fraudulentos distribuem malware, roubam credenciais e esvaziam contas bancárias.

Apps Maliciosas

Apps falsas “FIFA 2026 Live” recheadas de spyware surgem em lojas de apps de terceiros e em anúncios nas redes sociais. Após a sua instalação, acedem aos seus contactos, câmara e apps bancárias.

Sites de Streaming Falsos

Sites que prometem “transmissões grátis em HD” redirecionam para páginas maliciosas, desencadeiam transferências automáticos ou forçam falsos avisos de atualização de software para instalar ransomware.

Recolha de Dados de Pagamento

Muitas plataformas falsas solicitam pagamento para “acesso Hd” ou “visualização sem anúncios” - apanhado os dados do seu cartão sem qualquer intenção de prestar tal serviço.

Assista só a transmissões de emissoras oficiais como Fox Sports, TSN, Televisa e FIFA+, ou outras que estejam disponíveis no seu país. Descarregue apps exclusivamente da Apple App Store ou do Google Play.

Burlas em Apostas e Fantasy Leagues

As apps falsas de apostas, fantasy leagues e burlas de “vitórias garantidas” tornam-se cada vez mais comuns durante grandes jogos.

Verificação do Licenciamento

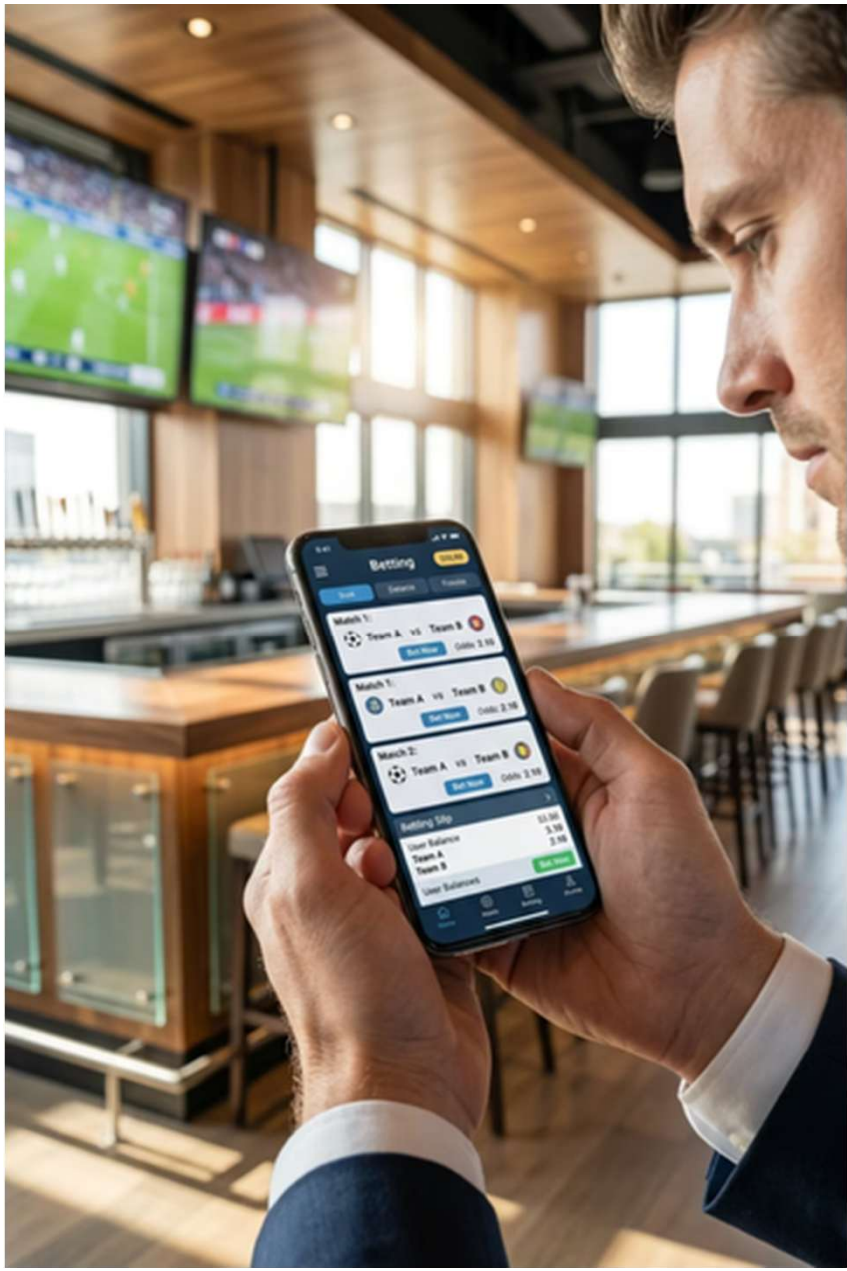
As plataformas de apostas legítimas apresentam números de licença regulamentares de autoridades de jogo reconhecidas. Sem licença? Saia imediatamente - o seu depósito corre sério risco de desaparecer.

Cuidado com “Vitórias Garantidas”

Nenhum serviço pode saber garantidamente qual é o resultado de algum jogo. Isto são burlas concebidas para obter taxas de subscrição e dados pessoais. Bloqueie e denuncie qualquer conta que faça tais alegações.

Seguir a Política da Empresa

Nunca aceda a plataformas de apostas ou fantasy leagues em dispositivos ou redes da empresa. Mantenha a sua vida digital pessoal e profissional completamente separadas.



Usurpação de Identidade e Phishing nas Redes Sociais

O Que Deve Ter em Atenção

Contas falsas que se fazem passar pela FIFA, jogadores, patrocinadores e federações de futebol são frequentemente utilizadas para difundir links de phishing, passatempos falsos e burlas durante grandes jogos.

- Falsos passatempos de “bilhetes VIP” que roubam credenciais de acesso.
- Contas falsas de jogadores a promover burlas e artigos contrafeitos.
- Mensagens de phishing e falsos passatempos de patrocinadores que recolhem dados pessoais.

Como Pode Manter-se em Segurança

A verificação é a sua primeira linha de defesa. Todas as campanhas legítimas do Mundial nas redes sociais provêm de contas verificadas com o selo azul. Em caso de dúvida - não clique.

- **Verificação dos selos de autenticação**
  As contas da FIFA, patrocinadores e federações têm de ter obrigatoriamente selos azuis - não é opcional.
- **Nunca dê credenciais via links de mensagens diretas**
  Uma organização legítima nunca pedirá a sua palavra-passe ou dados de pagamento através duma mensagem direta numa rede social.
- **Denúncia e bloqueio de contas suspeitas**
  Utilize imediatamente as ferramentas de denúncia da plataforma - para se proteger a si e a outros adeptos.

Segurança em Wi-Fi Público e a Viajar

Os estádios, zonas de adeptos, aeroportos, hotéis e centros urbanos em Nova Iorque, Los Angeles, Toronto, Cidade do México e Vancouver disponibilizarão redes Wi-Fi abertas durante o Mundial 2026. Muitas destas redes serão armadilhas maliciosas criadas por cibercriminosos para apanhar dados.

Usar Sempre uma VPN

Uma VPN aprovada pela empresa codifica o tráfego inteiro em redes públicas, tornando a sua intercetação praticamente impossível. Ative-a antes de se conectar - sempre, não abra exceções.

Evitar Redes Não Seguras

Nunca se conecte a redes com nomes como “FIFA_FanZone_Free” ou semelhantes - os atacantes utilizam deliberadamente nomes alusivos ao evento para atrairem vítimas. Utilize antes o hotspot de dados móveis do seu telemóvel.

Proteção dos Seus Dispositivos

Ative a encriptação total do disco, desative a conexão automática ao Wi-Fi, desligue o Bluetooth quando está no meio de multidões e mantenha o seu sistema operativo totalmente atualizado antes de ir para qualquer local no Mundial.

Atenção aos Códigos QR Maliciosos

Os códigos QR falsos em cartazes, menus e artigos para adeptos podem redirecioná-lo para sites de phishing. Utilize um leitor de QR que lhe permita pré-visualizar o URL antes de o abrir.

factis®

Proteja as Suas Contas com a MFA

A MFA bloqueia mais de 99% dos ataques automatizados de apropriação de contas. Ative-a em todas as plataformas - especialmente nos e-mails, contas bancárias e apps empresariais.

Boas Práticas de Palavras-passe

- ✓ Utilize uma palavra-passe única e complexa para cada conta.
- ✓ Deve ter no mínimo 16 caracteres com maiúsculas, minúsculas, números e símbolos.
- ✓ Use um gestor de palavras-passe - nunca confie na sua memória.
- ✓ Altere a sua palavra-passe imediatamente se suspeitar que ela foi comprometida.

Autenticação Multifator

Prefira apps de autenticação em vez de SMS - os ataques de SIM Swap estão a aumentar.

1. **Algo Que Sabe**
   A sua palavra-passe forte e única

2. **Algo Que Possui**
   A app de autenticação (Google, Microsoft)

3. **Algo Que Faz Parte de Si**
   Alternativamente pode usar a certificação biométrica

factis®

Esteja em Segurança - Dentro e Fora de Campo

O Mundial da FIFA de 2026 é um evento único numa geração. Não deixe que os cibercriminosos lhe roubem esta experiência - nem os seus dados. Você é a camada mais importante da nossa defesa de segurança. Mantenha-se alerta, em segurança e aproveite os jogos.

Verificação Total
Fontes oficiais: FIFA.com, transmissoras autorizadas, contas de redes sociais verificadas

Proteção das Suas Contas
Palavras-passe únicas + MFA em todas as plataformas, sempre, sem exceções

Proteção da Sua Conexão
VPN em Wi-Fi público, evite redes suspeitas, atualize os seus dispositivos antes de viajar

Reportar Atividade Suspeita
Se vir algo suspeito, comunique - contacte a Segurança Informática imediatamente

O jogo não acaba com o apito final. As ameaças também não.

Mantenha-se alerta - mantenha-se em segurança no mundo digital