Mais de 4.300 sites falsos já exploram a Copa de 2026

Com o uso da tecnologia já presente em 83% dos ataques de phishing, este será o primeiro grande evento esportivo global sob a nova geração de golpes hiperpersonalizados

A Copa do Mundo de 2026 promete ser não apenas um marco esportivo, mas também o primeiro grande evento global da era dos golpes impulsionados por inteligência artificial. Nas últimas semanas, o FBI alertou para a proliferação de sites falsos que se passam por canais oficiais da FIFA, enquanto pesquisadores da Group-IB identificaram mais de 4.300 domínios fraudulentos usados em golpes envolvendo ingressos, produtos oficiais e transmissões do torneio.


Yuri_Arcurs_CANVA

O cenário chama atenção não apenas pelo volume das fraudes, mas pelo fato da tecnologia estar mudando radicalmente a forma como criminosos planejam, personalizam e executam ataques.

"A diferença em relação às Copas anteriores é que os criminosos agora contam com inteligência artificial para automatizar tarefas que antes exigiam equipes inteiras. Eles conseguem produzir campanhas falsas mais rapidamente, em maior volume e com um nível de personalização sem precedentes", afirma Rodolfo Almeida, COO da ViperX.

Os números ajudam a explicar essa mudança. Segundo levantamento da Kaseya divulgado em 2026, 83% das campanhas de phishing, golpe em que criminosos se passam por empresas ou pessoas confiáveis, já utilizam recursos de IA. O estudo mostra ainda que mensagens produzidas por inteligência artificial alcançam taxas de interação significativamente superiores às dos modelos tradicionais.

Como a IA transforma torcedores em alvos

Se antes os criminosos dependiam de disparos genéricos de e-mails e mensagens em massa, hoje a estratégia é muito mais sofisticada. A preparação dos golpes começa meses antes do torneio, acompanhando o comportamento dos torcedores em redes sociais, mecanismos de busca, grupos de discussão, plataformas de apostas e páginas relacionadas ao futebol.

A partir dessas informações públicas, ferramentas baseadas em IA conseguem criar mensagens personalizadas com referências específicas a seleções, jogadores, cidades-sede, promoções e até preferências individuais do usuário.

"Estamos entrando em uma fase em que o golpe deixa de ser genérico e passa a ser contextual. O criminoso sabe qual seleção você acompanha, qual conteúdo consome e quais produtos procura. A IA transforma essas informações em ataques extremamente convincentes", explica Almeida.

O resultado é uma redução significativa dos sinais tradicionais que costumavam ajudar as vítimas a identificar uma fraude, como erros de ortografia, textos mal escritos ou comunicações genéricas.

Deepfakes ampliam o potencial de manipulação

Outro fator que preocupa especialistas é o avanço dos deepfakes. Ferramentas de inteligência artificial já permitem criar vídeos, áudios e imagens falsas com alto grau de realismo, reproduzindo vozes, rostos e expressões de atletas, influenciadores, jornalistas e marcas patrocinadoras.

Na prática, isso permite que criminosos criem vídeos falsos de jogadores, influenciadores e até patrocinadores promovendo sorteios inexistentes, cupons fraudulentos e campanhas enganosas ligadas ao torneio.

"Antes era mais fácil. Muita fraude entregava sinais claros de que tinha algo errado. Agora com inteligência artificial, o golpe pode ser muito bem escrito, bem contextualizado e tecnicamente convincente. O desafio deixou de ser achar o erro óbvio e passou a ser identificar uma fraude que parece legítima", alerta o executivo.

Países sede já registram aumento das ameaças

Dados da Check Point mostram que Estados Unidos, México e Canadá, países que sediarão o Mundial de 2026, vêm registrando aumento no volume de ataques cibernéticos direcionados a organizações. Apenas no México, a média semanal ultrapassou 3.500 tentativas de ataque por organização monitorada.

Embora parte dessas ofensivas tenha como alvo empresas, fornecedores e infraestruturas ligadas ao evento, especialistas destacam que os consumidores continuam sendo um dos elos mais explorados pelos criminosos.

Entre as principais ameaças estão: sites falsos de venda de ingressos, promoções fraudulentas envolvendo patrocinadores oficiais, golpes relacionados a apostas esportivas, aplicativos falsos de acompanhamento da Copa, phishing por WhatsApp, SMS e e-mail, deepfakes utilizados para promover campanhas falsas e roubo de credenciais de pagamento e carteiras digitais.

Como reduzir os riscos

Para Almeida, a principal defesa continua sendo a combinação entre informação e cautela.

"A Copa de 2026 será provavelmente o maior laboratório já visto para o uso de inteligência artificial em golpes digitais. O torcedor precisa entender que os ataques estão ficando mais convincentes justamente porque são construídos para parecer legítimos. A desconfiança continua sendo uma das ferramentas de segurança mais importantes."

Entre as recomendações estão acessar apenas canais oficiais da FIFA e dos patrocinadores, verificar URLs antes de realizar pagamentos, desconfiar de promoções e ingressos com preços muito abaixo do mercado, evitar clicar em links recebidos por mensagens e ativar autenticação multifator em contas digitais.

Performance, integração e continuidade: o legado tecnológico da Copa do Mundo

José Roberto Rodrigues (*)

A Copa do Mundo é um dos maiores exemplos de alta performance sob pressão

Durante algumas semanas, bilhões de pessoas acompanham partidas em tempo real ao redor do mundo, analisam estatísticas, interagem em plataformas digitais e consomem conteúdo em múltiplas telas, enquanto atletas e equipes técnicas operam em um ambiente onde qualquer falha pode custar caro. Embora o olhar do público esteja voltado para o campo, existe uma engrenagem complexa e invisível garantindo que tudo funcione de forma sincronizada.

Essa lógica não é muito diferente do que acontece no ambiente corporativo atual. Se antes infraestrutura era percebida como suporte operacional, hoje ela se tornou elemento estratégico para competitividade e continuidade dos negócios. Em um cenário marcado por inteligência artificial, workloads mais complexos e operações distribuídas, empresas passaram a depender de ambientes digitais capazes de responder rapidamente a picos de demanda, ameaças cibernéticas e falhas inesperadas.

No futebol, nenhum time chega a uma final confiando apenas no talento individual. Existe preparação física, análise tática, integração entre setores, banco de reservas e capacidade de adaptação ao inesperado. No ambiente digital, a lógica é semelhante. Não basta ter ferramentas isoladas; é necessário construir arquiteturas integradas, com visibilidade, redundância e governança capazes de sustentar operações críticas.

Redundância, aliás, é um conceito que se conecta diretamente com o esporte. Em um campeonato longo, contar com alternativas estratégicas não é luxo, mas necessidade. O mesmo vale para empresas que dependem de disponibilidade contínua. Ter planos de contingência, ambientes híbridos e políticas robustas de recuperação deixou de ser diferencial e passou a compor a própria lógica de sobrevivência operacional.

Além disso, performance hoje também está diretamente ligada à capacidade de resposta. Segundo o relatório Cost of a Data Breach 2025, da IBM, o custo médio global de uma violação de dados atingiu US$ 4,44 milhões. Já organizações que utilizam inteligência artificial e automação em segurança conseguiram economizar, em média, US$ 1,9 milhão por incidente, além de reduzir significativamente o tempo de contenção e resposta.

O dado reforça uma percepção cada vez mais relevante: resiliência não significa ausência de falhas. Significa capacidade de absorver impacto, responder rapidamente e manter continuidade mesmo em cenários adversos.

Assim como uma seleção campeã não é construída apenas com estrelas, mas com preparo, integração e estratégia, empresas também precisam olhar para sua infraestrutura como parte central da performance. Em um mercado cada vez mais digital e imprevisível, vencer não será privilégio de quem evita completamente erros, algo praticamente impossível, mas de quem consegue operar com inteligência mesmo diante deles.

No futebol, títulos raramente são conquistados apenas com talento individual ou improviso. As campanhas mais memoráveis costumam ser resultado de planejamento, leitura de cenário, entrosamento e capacidade de adaptação diante da pressão. No ambiente corporativo, a lógica é semelhante. Em um mercado cada vez mais digital e imprevisível, organizações resilientes não são necessariamente aquelas que nunca enfrentam falhas, mas as que se preparam para responder rapidamente, manter continuidade e seguir competitivas mesmo nos momentos mais desafiadores. Afinal, tanto em uma Copa do Mundo quanto na gestão da infraestrutura digital, vencer costuma ser consequência direta da preparação invisível que acontece muito antes do apito inicial.

(*) Country Manager e Alliances Manager LATAM da Adistec Brasil.

O papel da tecnologia fiscal integrada ao ERP na gestão e nos resultados das PMEs

No cotidiano de pequenas e médias empresas (PMEs), é comum que a atenção esteja voltada às áreas mais visíveis, como vendas, marketing e atendimento, responsáveis pelo crescimento. Nesse contexto, o fiscal costuma ser tratado apenas como uma obrigação burocrática, distante da estratégia.

Essa visão, no entanto, está cada vez mais superada. Em um ambiente de alta competitividade e margens pressionadas, a eficiência tributária deixou de ser um detalhe operacional e passou a ser central para a saúde financeira. Mais do que cumprir regras, trata-se de preservar rentabilidade, evitar perdas e garantir previsibilidade.

As organizações geram informações fiscais continuamente, mas, quando esses dados ficam dispersos entre planilhas e sistemas desconectados, surgem falhas, retrabalho e decisões baseadas em informações incompletas.

Os impactos são claros: aumento do risco de inconsistências em cálculos e classificações, recolhimentos indevidos, penalidades e uso de tempo em tarefas manuais. Além disso, a falta de visibilidade sobre a carga tributária compromete a formação de preços e reduz margens.

Nesse cenário, a automação fiscal integrada ao ERP assume papel decisivo. Mais do que organizar informações, conecta áreas e transforma complexidade em inteligência operacional, assegurando consistência e confiabilidade.

Com isso, o sistema apura tributos em tempo real, aplica a legislação vigente e se atualiza automaticamente, reduzindo riscos e liberando a equipe para atividades mais estratégicas. A integração entre compras, vendas e financeiro permite compreender o impacto dos tributos no caixa, antecipar obrigações, estruturar melhor o planejamento financeiro e eliminar imprevistos.

Outro ganho relevante está na identificação de oportunidades, como a recuperação estruturada de créditos fiscais. Assim, além de resguardar o caixa, contribui para seu fortalecimento sustentável.

À medida que o negócio evolui, essa base se torna ainda mais crítica. O aumento das operações sem o devido aprimoramento dos processos, especialmente na área fiscal, gera gargalos e amplia riscos.

Integrada ao ERP, essa capacidade sustenta o crescimento com controle, precisão e eficiência, permitindo a expansão sem comprometer a governança.

No fim, o papel do gestor não é dominar a legislação tributária, mas assegurar que haja estrutura e ferramentas adequadas para que as informações circulem de forma segura, confiável e estratégica.

Investir em um ERP que incorpora recursos fiscais como ferramenta de gestão é uma decisão de negócio, que protege margens, eleva a eficiência, qualifica a tomada de decisão e sustenta o crescimento. Para PMEs que buscam competitividade real, trata-se de um requisito.

(Fonte: Décio Krakauer é CEO da Ramo).