Opinião

Entenda como a IA transforma mentiras em "verdades" e previna-se dos malvertisings

Natália Santos (*)

O termo malvertising – uma combinação de malicious (malicioso) e advertising (publicidade) - não é novo, mas tem ganhado os holofotes da mídia por ser uma prática crescente entre hackers mal-intencionados para aplicar golpes.

Baseado no formato de anúncio publicitário, geralmente publicado em fonte confiável, como um site, uma mensagem eletrônica, ou no feed de uma rede social, os cibercriminosos se utilizam do recurso para disseminar malware, phishing e outras armadilhas digitais.

Para cumprir a missão de enganar os usuários, o malvertising é criado a partir de estratégias de engenharia social associadas a tecnologias como a Inteligência Artificial (IA) e o Machine Learning.

Os tipos mais comuns de malvertising estão no dia a dia de quem usa a internet. Eles divulgam produtos ou serviços legítimos por meio de links maliciosos (quase sempre com promoções imperdíveis), que levam a páginas falsas ao serem acessados. Uma modalidade mais sofisticada redireciona automaticamente os usuários para sites de phishing ou downloads de malware. Na pior das hipóteses, os anúncios já vêm com códigos embarcados capazes de explorar vulnerabilidades no navegador ou em plugins como Flash e Java.

Mas se nada disso é novo, por que ainda caímos em emboscadas? Posso responder facilmente a essa pergunta com uma simples análise: o cibercrime evoluiu a tal ponto, que ganhou recursos inteligentes, permitindo desde a criação ou adulteração de vídeos, áudios e fotos com a ajuda da IA (golpe conhecido como Deepfake), até o desenvolvimento de códigos maliciosos e fraudes mais sofisticadas.

No início deste ano, por exemplo, pesquisadores da Universidade Federal do Rio de Janeiro (UFRJ) identificaram mais de 4,3 mil anúncios em redes sociais, manipulados por IA com imagens de políticos brasileiros, convencendo as vítimas a acessarem páginas suspeitas atrás de uma falsa indenização.

A mesma técnica foi recentemente aplicada na criação de anúncios falsos envolvendo indevidamente a imagem de influencers e celebridades em propagandas de jogos de azar na internet, como o "Tigrinho" e o "Subway Money". Não por acaso, a IA entrou no foco do FBI (Departamento Federal de Investigação Norte-americano), que em meados do ano passado já alertava sobre a utilização de ferramentas de inteligência artificial generativas para o desenvolvimento de golpes digitais. Hoje, a maioria dos países, inclusive o Brasil, está estabelecendo suas regulamentações para o uso da IA.

Dicas para não cair em golpes

Combater o Malvertising hoje envolve a adoção de boas práticas de segurança por usuários individuais, administradores de sites, redes de publicidade e corporativas. É importante garantir que o sistema operacional, navegadores e plugins estejam sempre atualizados com as últimas correções de segurança. Além disso, é fundamental utilizar softwares de segurança, como antivírus e antimalware, além de soluções que identifiquem sites maliciosos antes que eles sejam carregados.

Aos administradores de sites, recomendo escolher redes de publicidade confiáveis, com regras rígidas de segurança e monitoramento. É importante implementar ferramentas que monitorem e filtrem anúncios em busca de atividades suspeitas e treinar suas equipes sobre os riscos de malvertising e como lidar com possíveis ameaças. Já as redes de publicidade precisam implementar processos rigorosos de verificação de dupla autenticidade para garantir que os anunciantes sejam legítimos. Devem também usar tecnologias avançadas para monitorar os anúncios em busca constante de atividades maliciosas e ter um plano de resposta rápido para remover anúncios maliciosos ou mitigar possíveis danos.

Além dessas medidas, redes corporativas com muitos terminais de acesso conectados podem se beneficiar de ferramentas de cibersegurança que ajudam a inibir a entrada de malwares e a bloquear o acesso de hackers por meio de vulnerabilidades abertas por malvertising acessado inadvertidamente. Um exemplo dessas ferramentas é o webshield, que atua como uma barreira entre o navegador do usuário e a internet, bloqueando conteúdos potencialmente perigosos antes que possam causar problemas

É preciso considerar, no entanto, que os erros humanos ainda são a porta de entrada para a maioria dos ataques cibernéticos. Não adianta adquirir a melhor tecnologia do mundo se os usuários não forem treinados para entender os perigos associados a comportamentos imprudentes. Afinal, é para ludibriar pessoas que os cibercriminosos se aperfeiçoam para fazerem mentiras parecerem verdades. Nesse sentido, a conscientização e a proatividade ainda são as peças-chave para proteger usuários e infraestruturas digitais contra os efeitos prejudiciais do malvertising.

(*) Head de Marketing da VaultOne, empresa de cibersegurança especializada em tecnologias de Gerenciamento de Acesso Privilegiado (PAM) e proteção de identidades.

Nvidia acusada da práticas monopolísticas

Uma coalizão de grupos progressistas está pressionando o Departamento de Justiça dos Estados Unidos (DOJ) a investigar a Nvidia por possíveis práticas ilegais.

Vivaldo José Breternitz (*)

corelens_CANVA

A gigante da tecnologia alcançou um quase monopólio no mercado de chips de alto desempenho e Unidades de Processamento Gráfico (GPUs), componentes fundamentais para inteligência artificial. Críticos argumentam que o domínio da Nvidia está sufocando a competição.

Os grupos afirmam que a participação da Nvidia no mercado, superior a 80% globalmente e 98% em alguns produtos utilizados pelos grandes data centers, está possibilitando práticas anticompetitivas como vendas cruzadas, fixação de preços em altos patamares e atraso na entrega de produtos adquiridos por empresas que também são clientes de concorrentes da Nvidia.

Eles também expressam preocupações com o potencial controle da empresa sobre infraestruturas críticas e seu suposto desrespeito aos controles de exportação, especialmente no que diz respeito às vendas para a China.

Enquanto os principais concorrentes da Nvidia, AMD e Intel, tem perdido mercado a Nvidia cresce de forma explosiva, sendo atualmente uma das três empresas mais valorizadas do mundo. A França já está investigando as práticas da Nvidia, mas outras grandes economias têm sido mais lentas em agir.

Jonathan Kanter, executivo do DOJ, já expressou preocupação com a concentração de poder na indústria de tecnologia, o que leva a se acreditar em uma possível investigação das práticas da Nvidia.

O resultado dessas investigações pode impactar significativamente o futuro da inteligência artificial e o cenário competitivo da indústria de tecnologia da informação.

(*) Doutor em Ciências pela Universidade de São Paulo, é professor da FATEC SP, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjnitz@gmail.com.

IA no atendimento? Especialista explica como usar a tecnologia para melhorar a experiência do cliente

Um relatório apresentado pela PwC indica que 73% dos consumidores consideram a experiência do cliente um fator importante na sua decisão de compra.

O estudo revela também que 32% dos consumidores abandonariam uma marca após uma única experiência ruim, o que mostra a importância das empresas terem uma boa experiência de compra para seus usuários.

Com a evolução do atendimento ao cliente, os consumidores hoje esperam uma resposta instantânea e uma experiência aprimorada, independentemente do setor, produto, preço ou canal de comunicação. No entanto, apesar dos benefícios da adoção de tecnologias e ferramentas baseadas em inteligência artificial (IA), ainda há um longo caminho a percorrer em termos de atendimento ao cliente e fidelização do consumidor.

Neste contexto, Willian Pimentel, Diretor Geral da Freshworks na América Latina, acredita que o futuro do atendimento ao cliente será mais brilhante do que nunca, mas exige que os líderes do setor pensem sistematicamente sobre como, quando e onde aplicar IA para melhorar a experiência.

"O aumento das expectativas dos clientes, que esperam um serviço eficiente e permanente, semelhante ao oferecido por empresas como a Amazon, reduziu a qualidade do CX em um momento de grande melhoria tecnológica. Os clientes querem tudo ao seu alcance e esperam um contato mínimo, por isso as empresas devem adotar novas ferramentas para atender a essas expectativas", diz Pimentel.

Essa abordagem muitas vezes resulta em experiências ruins para os clientes,

Freshworks

Willian Pimentel é Diretor Geral da Freshworks na América Latina.

segundo o Diretor da Freshworks. "Um exemplo é que, quando a IA é aplicada indiscriminadamente, ela pode lidar bem com as chamadas iniciais, mas não resolver problemas mais complexos. Os clientes acabam frustrados quando seus problemas são direcionados incorretamente ou quando as soluções de IA são insuficientes."

Para Willian Pimentel, é fundamental aplicar a IA de forma sistemática, começando pelos problemas mais simples e abordando gradualmente os mais complexos. O especialista explica que a IA pode realizar análises excelentes e compreender rapidamente os problemas dos clientes, mas quando erra, pode errar muito. "Portanto, a supervisão humana é necessária para garantir que as soluções de IA sejam precisas e emocionalmente inteligentes. Isso significa permitir que a IA lide com problemas simples e cotidianos, enquanto os agentes humanos lidam com os problemas mais complexos", comentou.

Como alternativa para empresas que estão atrasadas no atendimento ao cliente e desejam atualizar rapidamente, o executivo da Freshworks destaca que elas devem primeiro entender seus desafios específicos. "As novas empresas de SaaS podem enfrentar problemas complexos que exigem uma gestão cuidadosa. A IA generativa pode ajudar a construir rapidamente um repositório robusto de conhecimentos e estabelecer um sistema de classificação eficaz utilizando IA. Isto significa categorizar os problemas com base na sua complexidade e garantir que os problemas mais simples sejam resolvidos rapidamente, enquanto os mais complexos são sinalizados para intervenção humana".

Pimentel também enfatiza que devem ser implementadas políticas e procedimentos claros: "Em um ambiente B2C, isso é essencial para que os sistemas de IA forneçam suporte eficaz. Por exemplo, a IA pode lidar com problemas simples seguindo protocolos predefinidos, mas os agentes humanos devem intervir quando a IA encontra problemas que demandem maior raciocínio", finalizou.

News @TI

ricardosouza@netjen.com.br

Solução que reconhece clientes em até 1 segundo

@Visando autenticar clientes de parceiros de forma ágil e segura, a Minds Digital, primeira Voice IDTech do Brasil e criadora do FraudShield, acaba de lançar o MindsID, solução que tem como objetivo reconhecer clientes em um segundo. Por meio de Inteligência Artificial, associada da biometria de voz da empresa e análise de dados comportamentais, como o cruzamento de telefones, CPFs e dados biométricos, a Voice IDTech tem como meta reduzir em até 30% o tempo médio de atendimento. "Um dos grandes desafios dos diretores e gerentes de Atendimento ao cliente é o tempo gasto para validar a identidade dos clientes. Com o MindsID, agora os nossos parceiros vão poder autenticar seus consumidores de forma mais eficaz, reduzindo custos e entregando uma melhor experiência, garantindo confiabilidade e proteção de dados." explica Marcelo Peixoto, CEO da Minds Digital (https://minds.digital/).

Empresas & Negócios **José Hamilton Mancuso (1936/2017)** **Laurinda Machado Lobato (1941-2021)** Responsável: **Lilian Mancuso**

Editorias
Economia/Política: J. L. Lobato (lobato@netjen.com.br); *Ciência/Tecnologia:* Ricardo Souza (ricardosouza@netjen.com.br); *Livros:* Ralph Peter (ralphpeter@agenteliterarioralph.com.br);
Comercial: comercial@netjen.com.br
Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; *Editoração Eletrônica:* Ricardo Souza.
Revisão: Maria Cecília Camargo; *Serviço informativo:* Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

Colaboradores: Claudia Lazzarotto, Eduardo Moisés, Geraldo Nunes e Heródoto Barbeiro.

ISSN 2595-8410

Jornal Empresas & Negócios Ltda
Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080
Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br)
Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90
JUCESP, Nire 35218211731 (6/6/2003)
Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.