CRÓNICA DO OBEGEF
Nº 135 /2026-01-29
http://www.obegef.pt

Aldo Andretta

> > *As Tendências de Fraude para 2026. Nada Animador!*

Já venho falando, em minhas crônicas, sobre a crescente preocupação com o tema das fraudes. Há muito tempo isso deixou de ser algo restrito a um garoto sentado em frente ao computador que, com algumas habilidades informáticas, comete pequenos delitos. Tampouco é necessário mergulhar na Deep ou na Dark Web para encontrar fraudadores e esquemas utilizados contra pessoas e empresas.

Muito pelo contrário. Eu diria — se não estivéssemos falando de internet — que esses crimes são praticados "à luz do dia", para quem quiser ver. Basta uma simples busca por termos relacionados a fraude no *Telegram*, por exemplo, para encontrar pessoas vendendo serviços ilícitos. E, por mais incrível que pareça, os fraudadores precisam investir muito pouco dinheiro, pois já existem serviços que oferecem ferramentas de fraude a custos acessíveis, cobrando por tempo de uso.

E a velocidade é impressionante. O uso da inteligência artificial potencializou enormemente a forma como os fraudadores atuam. Descobrir fragilidades de processos, vulnerabilidades, meios de burlar biometria facial, entre outras técnicas, ganhou contornos nunca antes vistos.

E, falando em inteligência artificial, é aqui que mora um dos grandes riscos para 2026, especialmente quando tratamos do desenvolvimento pelas empresas. A busca frenética por "desenvolver, desenvolver e desenvolver" agentes de IA para ganho de produtividade pode gerar falhas de concepção, problemas no desenvolvimento, na segregação de acessos aos dados e na forma de utilização da inteligência. Erros de concepção e falhas de desenvolvimento podem permitir a exploração de ambientes — e isso, infelizmente, tende a acontecer. A

atenção aos dados é tão importante quanto aos demais aspectos, pois o acesso indevido a informações pode causar prejuízos significativos aos negócios.

Voltando um pouco no tempo, quando falávamos de golpes eletrônicos, os fraudadores atuavam de maneira muito mais grosseira, com sites e mensagens cheios de erros ortográficos e gramaticais, além do uso equivocado de imagens de empresas. Mas, com a inteligência artificial, esse cenário muda radicalmente. Quem nunca escreveu um e-mail e utilizou o *ChatGPT* para aprimorá-lo?

Os fraudadores aprenderam a fazer exatamente o mesmo. E foram além: passaram a utilizar a hiperpersonalização das mensagens, tornando-as extremamente fiéis às marcas exploradas, aliadas a gatilhos emocionais que induzem a vítima a clicar em links ou realizar compras que, mais tarde, se revelam fraudulentas. Acredito que esse seja mais um dos grandes riscos que veremos se intensificar.

Além disso, é cada vez mais provável o uso de jornadas coordenadas de fraude, que combinam múltiplos canais de comunicação — SMS, WhatsApp, e-mail, sites, anúncios pagos em plataformas digitais, entre outros — tudo para criar a percepção de uma campanha legítima de marketing de alguma instituição.

Nesse contexto, surge outro risco relevante: o insider. Trata-se do funcionário que é cooptado por fraudadores, voluntária ou involuntariamente, ou daquele que ingressa na instituição já com a intenção de obter acessos privilegiados. Esse tipo de ameaça é silenciosa e extremamente perigosa. Exige atenção redobrada aos controles de cibersegurança e, principalmente, à identificação de mudanças comportamentais, que nem sempre são evidentes, mas podem resultar em acessos indevidos, desvios financeiros ou, no pior cenário, ataques de *ransomware*.

E tudo isso precisa ser convertido em dinheiro. Nesse sentido, infelizmente, o PIX continuará sendo explorado, justamente por ser um meio de pagamento rápido, instantâneo e de fácil transferência.

O que antes era uma preocupação restrita a CISOs (Chief Information Security Officers) ou a áreas especializadas em fraude passou a figurar no topo da agenda dos CEOs. Segundo o Global *Cybersecurity* Outlook 2026, do Fórum Econômico Mundial, em 2025 os principais riscos apontados eram *ransomware*, fraude por meios eletrônicos, *phishing* e fraude na cadeia de

suprimentos. Agora, a fraude eletrônica e o *phishing* ocupam o primeiro lugar, enquanto vulnerabilidades em inteligência artificial e exploração de falhas de software passam a integrar esse ranking.

A preocupação dos CEOs faz total sentido. O nível de sofisticação adotado e a facilidade de burlar sistemas e enganar pessoas são tão impressionantes que, em determinados contextos, pensar em controles adicionais para confirmação de transações de risco deixa de ser exagero — ainda que isso traga mais burocracia.

Tudo está mudando e evoluindo muito rapidamente, e a fraude acompanha esse movimento. É essencial, neste momento que a informação permeie cada vez mais entre as pessoas, pois a educação continua a ser uma arma importante na contenção das fraudes. Talvez o futuro da prevenção seja pessoas mais atentas!

E para você, quais riscos enxerga no horizonte?

Espero que tenham aproveitado a leitura.