



>> Fraudes e a Inteligência Artificial

Tenho acompanhado a evolução das fraudes cibernéticas e ficando cada vez mais preocupado com sua evolução. São inúmeras variáveis que tornam sua incidência cada vez mais presente e podemos citar neste aspecto a desinformação das vítimas, a falta de comunicação as autoridades competentes por vergonha de ter sido enganado, as ferramentas aplicadas pelos fraudadores, combinado com a lentidão na predição novos casos.

Vi recentemente uma notícia que “Fraude online engana poucas pessoas mas chega a 7 milhões de euros” (<https://zap.aeiou.pt/fraude-online-milhoes-580028>). Neste contexto, as vítimas mulheres, são abordadas por homens que se passam por milionários, que fazem todo um jogo de sedução prometendo encontros pessoais, contudo, solicitam ajuda financeira para ir encontrá-las, alegando algum tipo imprevisto.

Faço uma reflexão sobre este tema: será mesmo que são poucas pessoas? Será que todas as vítimas reportaram sua perda financeira? Tal fato causa um abalo emocional muito forte e é possível que a falta de relato aconteça neste caso. E fica outra pergunta: quantas vítimas foram feitas ao redor do mundo?

Percebe-se que este tipo de crime cibernético que em um primeiro momento teria uma pessoa enganando outra, pode ter tido o contributo da inteligência artificial. Primeiro, porque o autor do delito busca informações sobre a vítima, como por exemplo o status de seu relacionamento atual, comportamentos e logicamente informações sobre a vida financeira da vítima. Segundo pelo motivo de poder ser utilizados recursos de alteração de imagem (*DeepFake*) e voz para tornar o autor do crime mais atraente e colocá-lo em cenas que corroborem a história narrada e claro, evitar de ser identificado. Isso também facilita a comunicação, pois a língua deixa de ser uma barreira.

Essa só é uma das situações em que as pessoas naturais podem ser vítimas de fraudes com o apoio da Inteligência Artificial. Ainda esta semana, recebemos em um grupo de WhatsApp o relato de uma pessoa que relatou ter sua imagem e voz “clonada” em uma ligação de vídeo para sua mãe, onde o criminoso pediu o repasse de valores, mas por sorte acabou não sendo feito, pois houve a desconfiança e feitas algumas perguntas que levaram a conclusão não ser uma ligação real.

E cada vez mais os criminosos utilizaram este tipo de tecnologia para atacar pessoas com maior incidência sobre os que atacaram as organizações. A previsão é tenebrosa, porém é real. As organizações serão atacadas, sem dúvida e a Inteligência Artificial será utilizada principalmente para conseguir acessos privilegiados aos sistemas informáticos, com intuito de capturar os dados existentes e solicitar a extorsão para que estes não sejam divulgados.

Isso pelo motivo de ser possível maior efetividade na automação de fraudes (casos de *Phishing*, por exemplo), conseguir enganar as barreiras de proteção de acessos e o aumento da capacidade de coleta de dados. Sem contar nos casos de *Deepfake*, como já mencionamos anteriormente.

Mas quando falamos em conseguir valores com golpes, os fraudadores terão como alvos as pessoas, pois por intermédio delas, conseguiram os acessos as instituições, como banca, por exemplo e assim fazer as transações desejadas pelo fraudador. Neste caso há os dados de acesso coletados da pessoa, juntamente com ferramentas que podem simular acessos indevidos a conta bancária e fazendo o desvio dos valores.

Também é fato de que as pessoas vão ser induzidas a fazerem transferência de numerários, pois serão enganadas por fraudadores com uso da tecnologia de Inteligência Artificial. É muito mais fácil enganar uma pessoa do que uma organização, que tem recursos apropriados para identificação de casos de fraude.

A falta de regulação da Inteligência Artificial e até mesmo da plataforma de internet contribuem para que tornem estes ambientes “terra de ninguém”. Nem desses administradores dessas plataformas se responsabiliza e, tão pouco tem interesse de identificar casos em que pessoas são vítimas de crimes, mas tem grande interesse nas audiências que essas mesmas pessoas trazem de audiência para elas.

E ainda veremos a imensa capacidade criativa dos fraudadores, aliadas ao uso de ferramentas tecnológicas de enorme potencial, para prejudicar pessoas e instituições.

Espero ter dado minha contribuição!