**Fraudes eletrônicas: estudo revela que 60% das empresas são responsabilizadas por golpes, mesmo não tendo conhecimento dos crimes**

*Golpes de engenharia social utilizam marcas de grandes corporações para atraírem as vítimas; especialista alerta sobre o impacto dessas ações para o jurídico das empresas*

Com o aumento da demanda digital nos últimos anos, influenciada principalmente pela pandemia de Covid-19, os casos envolvendo fraudes eletrônicas estão cada vez mais presentes no dia a dia da população. Segundo pesquisa realizada pela Federação Brasileira dos Bancos (Febraban), somente no primeiro semestre de 2021, os golpes de engenharia social (nos quais os dados das vítimas são usados por estelionatários digitais) aumentaram 165% no Brasil, em comparação com o segundo semestre de 2020. Um levantamento realizado pela Deep Legal, Lawtech de inteligência e gestão preditiva, aponta que apesar dos clientes serem os principais responsáveis pelo compartilhamento das informações pessoais e bancárias, em mais de 60% dos casos judicializados, as instituições são condenadas, ainda que parcialmente.

Entre as fraudes de engenharia social mais comuns estão o ‘golpe do motoboy’, golpes no WhatsApp e o *phishing* (que teve crescimento de 26% nos seis primeiros meses de 2021, segundo a Febraban). Nesta modalidade, a pessoa recebe um link em nome de uma empresa com a qual mantém relacionamento ou com ofertas sedutoras e acaba fornecendo os dados pessoais e bancários sem perceber que se trata de um site falso. De acordo com Vanessa Louzada, CEO da Deep Legal, “a cada ocorrência, um novo processo jurídico é criado, pois muitas vezes a pessoa que foi lesada recorre à Justiça para ter a compensação dos prejuízos, o que gera uma demanda ao jurídico da empresa”, explica.

O estudo feito pela Deep Legal coletou informações de diferentes bancos de dados do judiciário brasileiro, em cerca de mil processos em curso envolvendo fraudes eletrônicas. Em mais de 60% das decisões judiciais, as empresas foram condenadas de alguma forma a ressarcir os clientes. “Apesar do investimento das instituições e empresas de varejo em campanhas de orientação e na detecção do uso irregular de seus nomes e logomarcas, neste tipo de prática, o que está na mira do estelionatário digital é a desatenção do público que é levado pelo impulso em uma oferta tentadora, por isso é importante conhecer as modalidades de fraudes e a tendência de resultado das ações”, destaca Vanessa Louzada.

Ainda segundo o levantamento da Deep Legal, as instituições financeiras e de pagamento (de diferentes portes) são as mais demandadas na Justiça por casos de fraudes eletrônicas, seguidas por empresas de telefonia e do varejo.

Com o volume de golpes em ascensão e cada vez mais sofisticados, a especialista defende a necessidade de as empresas investirem em orientação e campanhas educativas, alertando continuamente seus clientes sobre os cuidados com operações eletrônicas. “O uso de Legal Analytics apoia o jurídico das empresas a conhecerem com amplitude e profundidade as ações em andamento e, com isso, preparar a defesa adequada, além de implementar melhorias internas, a fim de evitar condenações futuras e o surgimento de antigas e novas modalidades entre seus clientes”, afirma.

**Sobre a Deep Legal**

A Deep Legal é uma Lawtech de inteligência e gestão preditiva. Utiliza sofisticadas técnicas estatísticas e avançadas tecnologias como ferramentas de Big Data, Machine Learning e Inteligência Artificial para coletar dados, normalizá-los e transformá-los em informação consistente a fim de criar uma nova experiência aos profissionais jurídicos na otimização do seu trabalho de modo que possam informar, monitorar, comparar e predizer carteiras de ações judiciais.  São soluções direcionadas à gestão corporativa de empresas e escritórios jurídicos que possuem volume judicial. A Deep Legal ajuda a decodificar “dados” em insights estruturados e relevantes que se transformam em decisões estratégicas, inteligentes com geração de valor para o seu negócio.

<https://www.deeplegal.com.br/>