Especialista alerta para o aumento de perfis falsos, campanhas fraudulentas e sequestros de contas durante a Black Friday e explica como empresas podem fortalecer sua governança digital

A Black Friday, antes símbolo de oportunidades, tornou-se também um dos períodos mais vulneráveis para ataques cibernéticos e fraudes em redes sociais. O aumento do tráfego digital, a correria por promoções e o alto volume de campanhas patrocinadas criam um ambiente fértil para golpes que exploram tanto consumidores quanto marcas.

De acordo com o Panorama de Ameaças para a América Latina 2024, o Brasil é hoje o segundo país com mais fraudes digitais do mundo, e o prejuízo vai muito além do financeiro. “Quando um perfil falso replica a identidade de uma marca ou influenciador, há também um dano reputacional e jurídico. É o tipo de golpe que contamina a confiança, e a confiança é o principal ativo de uma empresa”, destaca o advogado Lucas Ruiz Balconi, Doutor em Direito pela USP e especialista em Direito Digital.

Segundo ele, o recente entendimento do Supremo Tribunal Federal (STF) sobre o Marco Civil da Internet, ao estabelecer o “dever de cuidado” das plataformas digitais, muda o cenário de responsabilidade, exigindo que as empresas estejam mais preparadas para agir rápido diante de fraudes. “O silêncio diante de um golpe pode ser interpretado como omissão. As empresas precisam ter protocolos preventivos e reativos para lidar com esses riscos”, reforça.

A seguir, o especialista elenca medidas estratégicas para proteger marcas, criadores e consumidores em um ambiente cada vez mais suscetível a manipulações digitais.

1. Crie uma política de governança digital com protocolos de resposta

“Mais do que proteger senhas, é preciso criar governança digital interna, com papéis e fluxos claros para lidar com incidentes. Empresas que dependem de redes sociais para vender ou comunicar precisam ter um plano de resposta: quem aciona o jurídico, quem comunica à plataforma e quem fala com o público. Esse tempo de reação pode ser a diferença entre conter o dano em horas ou perder a reputação em dias. É preciso que as empresas tratem o gerenciamento de contas e acessos com o mesmo nível de rigor que tratam dados financeiros, inclusive prevendo planos de contingência em caso de perda de acesso”, explica Balconi.

2. Faça auditorias periódicas e use ferramentas de monitoramento inteligente

“Monitorar menções e perfis similares à marca é essencial, mas o especialista defende o uso de ferramentas de escuta digital e IA para mapear padrões de comportamento suspeitos. Golpistas sofisticados replicam não só a identidade visual, mas também o tom de voz da marca e os horários de postagem. A auditoria contínua e o uso de alertas automatizados permitem reagir antes que o golpe escale”, diz.

3. Estruture contratos e políticas de uso com cláusulas de segurança digital

“Empresas que trabalham com influenciadores, afiliados ou representantes comerciais devem incluir cláusulas contratuais de proteção de marca e uso de imagem. Muitos golpes surgem quando terceiros divulgam campanhas sem critérios ou usam links encurtados que redirecionam para páginas falsas. Cláusulas contratuais claras sobre divulgação e monitoramento mitigam esse risco jurídico e reputacional”, orienta o advogado.

4. Invista em autenticação, rastreabilidade e backups independentes

“A autenticação de dois fatores é o mínimo mas não o suficiente, eu recomendo infraestruturas redundantes e controle descentralizado de acessos. Contas comerciais devem ter responsáveis

designados, acesso via gerenciadores oficiais e backup das credenciais fora da plataforma. Em caso de bloqueio ou invasão, isso garante rastreabilidade e prova de titularidade. A comprovação da titularidade da conta é frequentemente o fator que define a velocidade com que o acesso é recuperado", afirma Balconi.

5. Se comunique com transparência e antecipe-se ao golpe

"Acredito muito que a comunicação é uma ferramenta de defesa cibernética. Ao informar o público sobre canais oficiais, formatos de campanha e meios de pagamento legítimos, a marca desarma parte da estratégia dos fraudadores. Além disso, ele recomenda que, em casos de fraude, a empresa publique posicionamentos rápidos e técnicos, sem alarmismo, mas com clareza sobre as medidas adotadas. Transparência não é fragilidade, é maturidade digital. Uma marca que assume o controle da narrativa reduz danos e reforça a confiança", complementa.

Com o avanço das fraudes e a pressão por maior responsabilização jurídica das plataformas, a segurança digital deve ser tratada como pilar de ESG corporativo. "Proteção de dados e confiança digital são questões de governança. Em 2026, empresas que não tiverem políticas sólidas nesse campo não estarão apenas vulneráveis a golpes, estarão fora das melhores práticas de compliance e reputação", conclui Lucas Ruiz Balconi.

Fonte: Comunica PR, em 05.01.2026