

# Redes Sociais ou Redes de Burlas?

---

 [digitalinside.sapo.pt/redes-sociais-ou-redes-de-burlas](https://digitalinside.sapo.pt/redes-sociais-ou-redes-de-burlas)

Bruno Castro

O quotidiano de milhões de pessoas passa inevitavelmente pelas redes sociais, e é cada vez mais impossível ignorar o crescimento alarmante de burlas online. O que começou com esquemas ocasionais e mal elaborados tornou-se hoje numa teia complexa e persistente de perfis falsos, mensagens enganosas e tentativas de fraude cada vez mais convincentes. No Facebook, por exemplo, grupos de “comércio local” estão inundados por contas fictícias que prometem produtos a preços baixos, muitas vezes acompanhados por fotografias falsas e descrições genéricas. O mesmo fenómeno repete-se em grupos de arrendamento de imóveis, onde supostos senhorios exigem pagamentos adiantados por casas que nem sequer existem.

Mas as burlas não se limitam aos grupos de comércio nas redes sociais. Chegam por mensagens privadas, por e-mail, ou até por SMS, sempre com um tom de urgência envolvido. Alguém finge ser dos CTT a pedir o pagamento de uma taxa, outro faz-se passar por um banco ou por uma entidade pública, como a Autoridade Tributária, a informar que há uma coima por liquidar ou um processo em curso. Tudo isto com links duvidosos que abrem a porta ao roubo de dados, fraudes monetárias, acesso a contas bancárias, ou, pior, na instalação de software de espionagem para roubo de credenciais como os famosos “infostealers”. A realidade é que, a manipulação se torna cada vez mais sofisticada e as pessoas, como fator humano, continuam a ser o principal alvo de ataques de engenharia social.

Perante esta avalanche de tentativas de burla, é inevitável questionar o papel das plataformas digitais. Facebook, Instagram, TikTok, entre outras, têm à disposição ferramentas tecnológicas avançadas e acesso a equipas de moderação que poderiam, em teoria, travar este tipo de comportamentos, de forma eficiente. Contudo, na prática, continua a ser demasiado fácil criar uma conta falsa, infiltrar-se em grupos e começar a semear armadilhas. Os mecanismos de denúncia existem, mas raramente resultam numa resposta rápida ou eficaz. Os utilizadores sentem-se desprotegidos, e a inação das plataformas reforça a sensação de impunidade entre os burlões.

No entanto, quando falamos de redes sociais, as empresas operam muitas vezes de forma reativa e a correr atrás do prejuízo uma vez que estão condicionadas. Além disso, e como em muitos outros setores, falta uma cooperação mais estreita entre a comunidade de cibersegurança e os donos das redes sociais, que, na realidade, continuam a privilegiar o crescimento e a retenção de utilizadores em detrimento da segurança.

O problema dos scams online é que já ultrapassaram a esfera do incómodo ocasional. Tornaram-se uma ameaça real, com impacto financeiro, emocional, e até legal para quem é apanhado desprevenido. Exige-se agora um esforço coletivo: das plataformas,

que devem investir realmente em mecanismos de detecção e reação a ações maliciosas como tentativas de fraudes ou desinformação (por exemplo); da comunidade de cibersegurança, para que continuem a inovar e a pressionar por maior colaboração; e dos próprios utilizadores, que têm de se contextualizar do que é realmente o ciberespaço e dos riscos que acarreta, e por inerência, de se protegerem a si e aos seus. Estamos, todos, a viver numa nova era digital onde a confiança já não pode ser dada por garantida.

Apesar de tudo isto, talvez o elemento mais crucial desta equação seja o próprio utilizador. A verdade é que, por mais tecnologia que exista, nenhuma ferramenta substitui o sentido crítico e de alerta. A literacia digital é hoje uma das competências mais importantes que qualquer cidadão pode desenvolver. Desconfiar de mensagens suspeitas, verificar perfis antes de iniciar qualquer tipo de transação, nunca partilhar dados pessoais por impulso, ativar a autenticação de dois fatores e estar atento às tendências de fraude são atitudes fundamentais. A cibersegurança é uma responsabilidade social, mas também, é individual, pertencente a cada um de nós. Temos também de ser responsáveis, conscientes do risco e estar atentos na nossa vivência neste novo mundo (perigoso) digital. A nossa primeira defesa será sempre a consciência e a vigilância ativa.