Entre a inovação do cibercrime e a responsabilidade da liderança

Todos os dias acordamos com uma nova notícia sobre burlas. Já quase fazemos 'scroll' automático, como se fosse um ruído inevitável do nosso tempo. 'Ransomware' mais agressivo e profissionalizado. Burlas em nome do SNS a prometer reembolsos fictícios. Esquemas que usam o nome da TAP para roubar dados bancários. Esquemas de 'phishing' que se fazem passar pela Autoridade Tributária. Até a já conhecida burla “Olá Pai/Olá Mãe” evoluiu para mensagens mais personalizadas.

Esta breve lista consiste apenas em algumas das mais recentes fraudes – uma lista que cresce, quer em números quer em vítimas, quer em sofisticação e sucesso destes ataques.

O que estes casos têm em comum não é apenas o prejuízo financeiro, mas acima de tudo, o sinal claro de que estamos perante um ecossistema criminoso altamente inovador, que aprende mais depressa do que muitas organizações legítimas conseguem reagir.

Durante demasiado tempo olhámos para a cibersegurança e para a prevenção da fraude como um problema técnico, contudo, o que estamos hoje a assistir é a uma corrida à inovação e, neste momento, em muitos contextos, os atacantes estão à frente. As burlas já não são mensagens mal escritas, com erros ortográficos ou emails caricatos. São comunicações bem desenhadas, com linguagem institucional, imagem corporativa alinhada, temporizações estudadas e gatilhos emocionais claros: urgência, medo, oportunidade, confiança numa marca (re)conhecida.

Quando alguém recebe uma SMS aparentemente enviada pelo SNS, pela TAP ou pelo seu banco, o ataque não é tecnológico, é psicológico. Explora confiança, autoridade e hábitos digitais, o que demonstra que os criminosos compreenderam algo essencial: as pessoas são o alvo direto. É redutor pensar que estamos apenas perante ‘novas formas de ataque’ – é muito mais que isso, já que, estamos perante modelos de negócio criminosos que evoluem como *startups*: testam, iteram, escalam e monetizam de forma acelerada.

Se os ataques são inovadores, a resposta também terá de o ser e, para isso, é preciso liderança. Liderança para reconhecer que a fraude e o cibercrime já são riscos estratégicos, ao nível de reputação, continuidade do negócio e confiança do cliente. Liderança para aceitar que investir em prevenção não é um custo, é sim, um fator de alta competitividade e resiliência. As organizações que continuam a reagir apenas após o incidente, com comunicados defensivos e medidas avulsas, estão a jogar um jogo antigo num terreno novo. A boa notícia é que a inovação não é exclusiva do crime, no entanto, exige mudança de mentalidade dentro das organizações.

Proteger hoje implica combinar tecnologia com cultura, dados com pessoas, inteligência artificial com literacia digital. Implica desenhar sistemas que antecipam comportamentos, não apenas que respondem a alertas. Implica ter monitorização 24/7, e não uma auditoria

ocasional. Implica formar colaboradores e consumidores como a sua primeira linha de defesa, não apenas como o elo mais fraco.

Mais do que perguntar «que ferramenta precisamos?», a pergunta deve ser «estamos a pensar a segurança de forma integrada, adaptativa e contínua?» Quando uma burla usa o nome de uma instituição pública ou de uma grande marca, o impacto vai muito além dos lesados diretos, vai acima de tudo, minar a confiança coletiva e colocar em causa a reputação e a fiabilidade da marca. E a confiança, uma vez perdida, é difícil de recuperar.

As notícias diárias sobre burlas não são apenas alertas isolados, devendo antes ser encarados como sinais de transformação profunda. O crime está a inovar e a pergunta é se a liderança, pública e privada, está a acompanhar essa velocidade. E sim, inovar é um ato de liderança. É escolher não reagir apenas quando o problema explode, e sobretudo, é criar mecanismos antes que ele exista.

A verdadeira liderança não se mede pela capacidade de controlar o risco, mede-se antes pela visão de o antecipar, transformar e aprender com ele. Num mundo em permanente mutação, temos de assumir claramente que, a mudança não é uma ameaça, é parte do processo e que a inovação nasce quando juntamos tecnologia, inteligência humana e um propósito claro. Quem lidera com visão não só está mais bem preparado como também constrói confiança, resiliência e futuro.